ASSOCIAÇÃO BRASILEIRA DE ANUNCIANTES

2030: O futuro passa por aqui.

VLK ADV

Guia de Boas Práticas para Uso de Dados e IA no Marketing

Este guia é uma entrega dos GTs Inteligência Artificial e Privacidade e Proteção de Dados da ABA. Elaborado em parceria com o VLK Advogados.

Lançado em 13/05/2026

Introdução

A comunicação e o marketing atravessam uma transformação profunda impulsionada pela convergência entre o mundo on e offline, onde a interconexão constante entre pessoas, plataformas e dispositivos gera informações e rastros digitais que alimentam ferramentas de inteligência artificial, revolucionando a comunicação entre marcas e consumidores e democratizando o acesso a recursos que permitem a criação de conteúdos altamente customizados e convincentes.

Nesse cenário, o uso intensivo de dados tornou-se o verdadeiro combustível para a aplicação de sistemas de IA (especialmente IA generativa) que já fazem parte das rotinas de criação, planejamento e compra de mídia, impactando diretamente campanhas de marketing cada vez mais personalizadas e relevantes, fortalecendo o relacionamento e a fidelização entre marcas e consumidores.

Atualmente, é praticamente impossível dissociar o tratamento de dados pessoais das atividades de marketing. Os algoritmos de IA dependem de grandes volumes de informações para treinar modelos, gerar insights e antecipar comportamentos com precisão. Dados viabilizam a compreensão de públicos, a mensuração e a personalização; a IA amplia a capacidade de criar, testar e otimizar em escala. Juntas, essas tecnologias estão redesenhando a cadeia publicitária, do briefing e produção de conteúdo à compra de mídia, atendimento e realização de pesquisas para geração de insights.

Essa sinergia traz ganhos claros para o mercado, como maior eficiência de tempo e custos por meio da automação de tarefas, maior capacidade analítica no tratamento de grandes volumes de informação e a possibilidade de oferecer experiências mais relevantes e personalizadas em grande escala, mantendo consistência e velocidade de execução.

Ao mesmo tempo, esse avanço tecnológico amplia responsabilidades e pontos de atenção que não podem ser tratados apenas como ‘detalhes técnicos’. O uso combinado de dados e IA aumenta a exposição a riscos jurídicos, reputacionais e éticos, com impacto direto na confiança do consumidor e na sustentabilidade do ecossistema publicitário. A adoção responsável exige governança com controles proporcionais ao risco do respectivo uso da tecnologia (definição de papéis e responsabilidades, transparência, explicabilidade, revisão e supervisão humana, rastreabilidade, gestão de dados, documentação e resposta a incidentes), sob pena

de ampliar riscos regulatórios e reputacionais – desde publicidade enganosa e discriminação algorítmica até violações de privacidade, direitos autorais e direitos de personalidade. No cenário jurídico brasileiro, em particular, a conformidade no uso dessas tecnologias demanda interpretação integrada de normas e boas práticas aplicáveis, como Lei Geral de Proteção de Dados (LGPD), Código de Defesa do Consumidor (CDC), Lei de Direitos Autorais, autorregulamentação publicitária, EU AI Act, Nist e normas ISO/IEC.

É diante desse cenário que a ABA, em parceria com o VLK Advogados, apresenta o Guia ABA de Boas Práticas para Uso de Dados e IA no Marketing. O objetivo é contribuir para que o próprio mercado se antecipe, organizando e estabelecendo padrões concretos, aplicáveis e verificáveis que orientem anunciantes, agências, plataformas e fornecedores no uso lícito, ético e seguro de dados pessoais e de IA, em plena sintonia com a autorregulamentação publicitária e legislação vigente.

“Ao liderar esse movimento, o setor eleva a segurança jurídica, consolida a proteção de direitos e fortalece a confiança do consumidor, atuando de forma estratégica na construção de um ambiente regulatório equilibrado, reduzindo incertezas, antecipando riscos e evitando interpretações que possam sufocar a inovação ou restringir a liberdade criativa”, enfatiza Nelcina Tropardi, Presidente da ABA e VP Jurídico, Corporate Affairs, Compliance, Inclusão e Diversidade, ESG, Gestão de Risco e Comunicação Corporativa do Carrefour.

“Na era marcada pela velocidade da inovação tecnológica em busca de eficiência e customização a partir do uso intenso e cada vez mais sofisticado de dados pessoais e IA, torna-se relevante que a construção de parâmetros regulatórios conte com a participação ativa do próprio mercado. Iniciativas de autorregulação e de consolidação de boas práticas permitem reduzir assimetrias de conhecimento entre Estado e sociedade, incorporando a experiência prática de negócios. Ao liderar essa pauta, a ABA contribui para fortalecer a segurança jurídica, equilibrando a proteção de direitos fundamentais com o desenvolvimento econômico e tecnológico. O Direito é um impulsionador da inovação, inclusive nas modernas formas de se regular a comunicação e o marketing, alavancando a economia criativa e fortalecendo a confiança do consumidor.”, ressaltam Rony Vainzof e Gisele Karassawa, sócios do VLK Advogados.

Introdução

“O guia foi estruturado para transformar preocupações regulatórias e tecnológicas em orientações práticas e aplicáveis ao dia a dia do setor. Ao reunir conceitos essenciais, bases legais, princípios e boas práticas operacionais dos dois pilares que hoje moldam o marketing contemporâneo, proteção de dados e uso de IA, buscamos apoiar decisões estratégicas, orientar contratações, qualificar processos internos, fortalecer estruturas de governança e elevar os padrões de transparência e responsabilidade na comunicação com o público”, comenta Paula Ercole Bauléo, Líder do GT Inteligência Artificial da ABA e Sr Legal Manager na General Mills.

“O documento constitui um referencial para a adoção de políticas, processos e governança alinhados à legislação aplicável, à autorregulamentação publicitária e às melhores práticas nacionais e internacionais, servindo também como parâmetro técnico para reguladores e Judiciário na interpretação de condutas, riscos e padrões de diligência do setor”, completa Rodrigo Borges, Líder do GT Privacidade e Proteção de Dados da ABA e Diretor de Privacidade | América Latina da Kenvue.

“O Guia preenche uma lacuna real. O mercado já usa IA na produção de conteúdo, na segmentação e na compra de mídia, mas a maioria das organizações ainda governa esse uso de forma fragmentada, sem conectar os requisitos da LGPD, as regras de autorregulamentação e as obrigações contratuais em uma arquitetura que funcione na prática. O que este documento faz é exatamente isso: traduzir um conjunto disperso de normas e boas práticas em orientações aplicáveis ao ciclo completo da operação. Para equipes jurídicas que trabalham no produto, esse é o tipo de insumo que permite construir governança antes do incidente, não depois”, afirma Lucas Gobbo, Co-líder do GT Privacidade e Proteção de Dados da ABA e Global Legal Manager & Product Counsel no BEES | AB InBev.

Nota sobre referências internacionais:
As referências a autoridades, normas e materiais estrangeiros ao longo deste Guia são utilizadas em caráter comparativo, técnico e informativo, como subsídios de boas práticas e tendências regulatórias. Tais referências não possuem efeito vinculante no Brasil, salvo quando houver incidência normativa específica sobre determinada operação, agente ou território.

Este Guia se apoia no que a ABA vem construindo com pioneirismo e consistência desde a criação dos Grupos de Trabalho de Privacidade e Proteção de Dados e de Inteligência Artificial, que vêm fazendo um esforço contínuo para promover o debate qualificado sobre tecnologia, inovação e responsabilidade no marketing, edificando entendimentos e disseminando conhecimento técnico e qualificado por meio de iniciativas que incluem materiais de orientação, ações de advocacy e agendas para fomentar o diálogo institucional com atores relevantes. Esse esforço coletivo foi reconhecido, inclusive, com o Prêmio Marketing Best 2025, categoria Tecnologia, pelo case “Boas práticas da ABA para o uso da inteligência artificial no marketing”, que refletiu um conjunto consistente de entregas ao longo dos últimos anos, incluindo publicações e iniciativas desenvolvidas também em parceria com o VLK.

Ao consolidar esse conhecimento em um guia de boas práticas, a entidade busca contribuir para um ambiente de inovação responsável, no qual o uso de dados e inteligência artificial seja acompanhado por princípios fundamentais da publicidade ética, como respeito ao consumidor, integridade da comunicação, proteção de dados e responsabilidade na adoção de novas tecnologias. Ao mesmo tempo, pretende servir como benchmark nacional e internacional, reforçando o papel do Brasil no debate global e valorizando a experiência concreta dos anunciantes.

Mais do que um documento estático, este Guia pretende ser uma referência viva para o mercado, passível de evolução e aprimoramentos e atualizações, e um convite para que todo o ecossistema publicitário avance de forma colaborativa na construção de um marketing cada vez mais inovador, transparente e responsável. Acreditamos que é possível, e necessário, avançar com tecnologia sem renunciar a princípios que orientam a publicidade ética, como respeito ao consumidor, integridade da comunicação, proteção de dados e responsabilidade na adoção de IA.

Sandra Martinelli
CEO da ABA – Associação Brasileira de Anunciantes
e Membro do Executive Committee da WFA

Sumário

I - Proteção de Dados Pessoais no Marketing 08

1. Por que proteção de dados é tema estratégico para o marketing 09
2. Cadeia publicitária e agentes de tratamento 10
3. Princípios da LGPD aplicados ao marketing na prática 14
    - 3.1. Finalidade 14
    - 3.2. Adequação & Necessidade 14
    - 3.3. Transparência 15
    - 3.4. Segurança & Prevenção 17
4. Bases legais no marketing digital 18
    - 4.1 Brasil x Europa 18
    - 4.2 Consentimento e legítimo interesse: quando usar cada um 19
    - 4.3 *Cookies* e *first-party* 22
    - 4.4 Dados sensíveis no marketing 24
    - 4.5 *Consent* or *Pay* e execução de contrato 25
5. Publicidade direcionada e perfilamento 27
6. Publicidade programática e ecossistema de adtech 30
7. Transferência internacional de dados no marketing 31
8. Crianças e adolescentes no marketing digital 33

II - Inteligência Artificial no Marketing 37

1. IA “tradicional” x IA generativa no marketing 38
2. Onde a IA entra na cadeia publicitária 38
    - 2.1 Atores da cadeia: quem faz o que e onde a IA costuma entrar 39
    - 2.2. IA como ferramenta, parceiro criativo e risco jurídico 40
    - 2.3 Responsabilidade na cadeia 41
3. Casos de uso reais de IA no marketing 43
    - 3.1 Criação de conteúdo (texto, imagem, vídeo, áudio e variações) 44
    - 3.2. Mídia e otimização (compra, segmentação, *bidding* e decisão em tempo real) 46
    - 3.3. Mensuração e atribuição 47
    - 3.4 Atendimento e pesquisa (*chatbots*, agentes e pesquisa de mercado) 48

4. Princípios que devem regrar a IA Responsável e Ética no Marketing 49
4.1. Finalidade legítima e alinhamento com o negócio 49
4.2. Transparência e explicabilidade proporcional ao risco 50
4.3. Centralidade e supervisão humana 51
4.4. Não discriminação, equidade e mitigação de vieses 52
4.5. Segurança, integridade e confiabilidade 53
4.6. Responsabilidade e prestação de contas *(accountability)* 54
4.7. Legalidade e conformidade regulatória 54
4.8. Proporcionalidade entre risco, controle e impacto 56
5. Riscos-chave e salvaguardas práticas 57
5.1. Publicidade enganosa/abusiva, *AI washing* e *claims* sobre IA 58
5.2. Conteúdo sintético e integridade 59
5.3 Personas sintéticas e dados sintéticos 60
5.4 Viés, discriminação e estereótipos 62
5.5 Propriedade intelectual e direitos de personalidade 63
5.6. Dados pessoais no treinamento 65
5.7. Segurança da Informação na IA 67
5.8. Crianças e grupos vulneráveis: cuidados reforçados (conteúdo, segmentação, persuasão) 71
5.9. Sustentabilidade e impactos sociais (energia, cadeia de fornecedores, reputação) 72
6. Governança de IA aplicada à publicidade (como implementar) 74
6.1 Transparência com o público: quando e como divulgar uso de IA 74
6.2 *Assessment* para contratação de agências 76
6.3 Políticas internas e capacitação 77
6.4 Seleção e homologação de ferramentas 77
6.5. *Gate* de governança antes do *go-live* 78
6.6 Fluxo operacional com IA *(end-to-end)* 79
6.7 Rastreabilidade e documentação 79
6.8 Gestão de incidentes e resposta rápida 80

Conclusão 82

CAPÍTULO I

Proteção de Dados Pessoais no Marketing

1. Por que proteção de dados é tema estratégico para o marketing

Os dados pessoais assumiram papel central no marketing, pois deixaram de ser apenas insumos operacionais para se tornarem verdadeiros ativos de negócio, capazes de orientar decisões, personalizar experiências e maximizar resultados.

Em paralelo, a consolidação de marcos regulatórios globais, como GDPR, LGPD e mais de 130 legislações similares, redefiniu novos parâmetros estruturantes para o tratamento de dados na atividade publicitária. Longe de inviabilizar a publicidade orientada a dados, essas normas criaram critérios objetivos para seu uso responsável, estruturando hipóteses legais, governança e mecanismos de *accountability*.

Esse movimento superou o modelo ineficiente de dependência quase absoluta do consentimento, abrindo espaço para abordagens mais sofisticadas, sustentáveis e juridicamente seguras. O resultado é um ambiente em que dados podem impulsionar inovação e resultados, desde que integrados a uma estratégia consistente de conformidade, ética e gestão de riscos.

Nesse cenário, a confiança do consumidor emerge como um diferencial competitivo decisivo. Marcas que demonstram transparência, responsabilidade e respeito à privacidade tendem a construir relações mais duradouras e valiosas com seus públicos, enquanto práticas opacas ou abusivas geram não apenas sanções legais, mas também danos reputacionais significativos.

O uso ético e transparente dos dados, portanto, fortalece a imagem da marca e evita que comunicações sejam percebidas como intrusivas ou manipuladoras. A publicidade eficaz depende de uma relação de confiança; o público precisa acreditar que as informações recebidas são confiáveis e que sua privacidade é respeitada.

Pesquisa promovida pela PWC em 2024, demonstrou que 90% dos consumidores brasileiros entendem que a proteção de seus dados é um dos fatores mais importantes para as empresas conquistarem a sua confiança[1].

Assim, a LGPD não é, tão pouco deve ser compreendida ou interpretada, como obstáculo às atividades de marketing e publicidade, mas como elemento estruturante da sua lógica real de funcionamento. Integrar a proteção de dados às estratégias de comunicação e relacionamento é, hoje, condição essencial para a sustentabilidade, a credibilidade e a eficácia das ações de mercado.

1 https://www.pwc.com.br/pt/sala-de-imprensa/release/90-dos-consumidores-brasileiros-afirma-que-a-protecao-dos-seus-dados-pessoais-e-um-dos-fatores-mais-importantes.html

2. Cadeia publicitária e agentes de tratamento

Os agentes de tratamento são os sujeitos aos quais a legislação atribui deveres e responsabilidades no âmbito da proteção de dados, definidos a partir do seu poder de decisão sobre as finalidades e os meios do tratamento ou de sua atuação na execução dessas atividades.

No contexto da cadeia publicitária, é essencial identificar com precisão quem são esses agentes, quais decisões efetivamente controlam e quais operações executam, pois é essa delimitação que estrutura a matriz de responsabilidades e a alocação de riscos.

Podemos distinguir os agentes de tratamento em duas categorias[2]:

Controlador	A quem competem as decisões essenciais referentes ao tratamento de dados pessoais, em especial a finalidade, a natureza dos dados pessoais, os próprios dados pessoais necessários e a duração do tratamento. O seu elemento distintivo é o poder de decisão.	Como regra, caberá ao Controlador garantir a licitude do tratamento, enquanto o Operador deverá observar as instruções lícitas do Controlador e garantir que a execução do tratamento a si confiado se opera de forma segura e apta a atender eventuais solicitações de direitos do titular.
Operador	Agente que executa a atividade de tratamento em nome do Controlador, seguindo suas orientações, podendo tomar decisões não essenciais. Como por exemplo, a respeito do software ou hardware a ser utilizado.	

2 https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-para-definicoes-dos-agentes-de-tratamento-de-dados-pessoais-e-do-encarregado e https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf

Essas categorias de agentes de tratamento podem se relacionar de quatro diferentes formas:

Controladores Independentes	As Partes executam suas próprias atividades de tratamento, decidindo independentemente seus elementos essenciais.
Controladores Conjuntos	Quando os elementos essenciais do tratamento são definidos de forma conjunta, seja por decisão comum (as partes se unem para a tomada de decisão), seja por decisão convergente (as partes tomam decisões apartadas que se complementam e são ambas necessárias aos elementos essenciais da atividade de tratamento).
Controlador-Operador	Uma parte (Operador) executa uma atividade de tratamento cujos elementos essenciais são definidos por outra (Controlador).
Operador-Suboperador	Um Operador subcontrata a execução da atividade de tratamento a um terceiro (Suboperador).

⚠ ATENÇÃO!

O operador pode equipara-se a controlador quando deixar de cumprir as instruções lícitas do controlador e determinar por decisão própria e indevida as finalidades e os meios do tratamento[3].

Agentes da cadeia publicitária e qual papel eles tipicamente desempenham.[4]

ANUNCIANTE

Quem são?	Papel (como regra)
Entidades que promovem seus produtos, serviços ou marcas por meio de estratégias de marketing e campanhas de publicidade.	Serão considerados controladores das atividades relacionadas à coleta, ao uso e ao eventual compartilhamento de dados pessoais sempre que houver definição das finalidades e dos meios empregados para o direcionamento de anúncios ao público, seja em sites ou plataformas específicas. Podem, ainda, ser caracterizados como controladores nas hipóteses em que, mesmo sem realizar diretamente o tratamento de dados pessoais, participam da determinação do tipo de informações que desejam receber e para qual finalidade, como ocorre, ex.: na contratação de empresa de pesquisa de mercado, mediante definição de características demográficas, comportamentais ou interesse do público pretendido[5].

3 Conforme a LGPD (Art. 42, §1º, I) - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador. Vide também ICO: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-are-controllers-and-processors/#4

4 https://iabbrasil.com.br/wp-content/uploads/2021/08/IAB-BRASIL_PARECER-JURIDICO_LGPD-E-PUBLICIDADE-PERSONALIZADA_MARCEL-LEONARDI.pdf; https://publya.com/blog/glossario-da-midia-programatica/; https://www.gdpr-impact.com/; https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

5 https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pt.pdf, página 20

VEÍCULOS

Quem são?	Papel (como regra)
Proprietários de sites, apps e outros espaços digitais que oferecem espaços para veiculação de anúncios, monetizando por meio de SSPs ou redes de anúncio.	Serão considerados controladores quanto ao às atividades de coleta e compartilhamento de dados de seus usuários, não possuindo controladoria em relação as atividades feitas com os dados compartilhados pelos demais agentes da cadeia.

REDES DE ANÚNCIOS

Quem são?	Papel (como regra)
Intermediários entre anunciantes e Veículos, agregando inventários de anúncios e facilitando a sua comercialização.	Serão considerados controladores considerando seu papel na coleta de dados pessoais de múltiplos Veículos, elaboração de perfilamentos comportamentais e seleção de qual anúncio exibir para cada usuário.

DEMAND-SIDE PLATFORMS (DSPS)

Quem são?	Papel (como regra)
São plataformas utilizadas pelos anunciantes para comprar inventários publicitários.	Sempre que não tomarem decisões sobre os dados e atuarem apenas em nome dos anunciantes para realizar os anúncios com o melhor custo-benefício, serão considerados operadores.

SUPPLY-SIDE PLATAFORMS (SSPS)

Quem são?	Papel (como regra)
São plataformas utilizadas pelos Veículos para vender inventários publicitários.	Sempre que não tomarem decisões sobre os dados e apenas agregarem os inventários de publicidade dos Veículos[6], serão considerados operadores.

PLATAFORMAS DE GESTÃO DE DADOS (DMPS)

Quem são?	Papel (como regra)
Plataformas para coletar, organizar e segmentar dados de audiência.	Sempre que apenas ofereçam infraestrutura tecnológica para a gestão de dados utilizados nos anúncios e não adotarem decisões sobre os elementos essenciais dos dados, serão considerados operadores.

6 https://www.jipitec.eu/jipitec/article/download/410/411/2152

ATENÇÃO!

DSPS, SSPS e DMPS: embora operadores de dados no cumprimento de suas funções e atuações mais estritas, eles podem ser enquadrados como controladores independentes ou controladores conjuntos dependendo do seu modelo de negócios e nível de decisão sobre coleta, matching, enriquecimento e eventual uso dos dados para fins próprios.

Para fins de mitigação de riscos, as responsabilidades atribuídas a cada um dos agentes envolvidos devem ser delimitadas de forma clara e inequívoca por meio da formalização dessas atribuições em instrumentos contratuais, os quais, com base na NBR ISO/IEC 27701, devem definir:

Para contratos entre controladores	Para contratos com operadores
• Finalidades do tratamento e compartilhamento de dados • Definição das categorias de dados pessoais objeto do tratamento • Descrição global das atividades de tratamento (ex.: como os dados devem ser utilizados) • Responsabilidades pela implementação de medidas técnicas e administrativas de segurança • Responsabilidades na hipótese de incidentes de segurança • Responsabilidades e prazos de retenção e descarte dos dados • Responsabilidades e pontos de contato para o atendimento de solicitações dos titulares de dados • Responsabilidades quanto a transparência da atividade para com os titulares	• Finalidade do Tratamento e vedação do tratamento para outro fim • Categorias de dados tratados e de titulares • Determinação de obrigações de segurança atinentes ao tratamento de dados pessoais • Comunicar incidentes de segurança ao controlador sem demora indevida • Cooperação na resposta a Incidentes, com prazos bem definidos • Assistência ao controlador na resposta a solicitações dos titulares e da ANPD • Subcontratação da atividade de tratamento (possibilidade, critérios de aprovação, necessidade de informação) • Registro e retenção de *logs* • Retenção e Descarte dos dados • Devolução e eliminação dos dados ao fim do contrato

3. Princípios da LGPD aplicados ao marketing na prática

Embora inexista hierarquia normativa entre os princípios da LGPD, quatro deles demandam atenção especial no contexto das atividades de marketing: finalidade, adequação, necessidade e transparência.

3.1 Finalidade

As atividades de tratamento devem possuir um propósito específico, lícito, explícito e informado ao titular.

No âmbito do marketing isso significa que, antes de tratar qualquer dado pessoal para a realização da comunicação de campanhas publicitárias, é preciso se perguntar: o que a campanha busca alcançar? Quem é o público-alvo?

Essas e outras informações precisam ser bem-definidas desde o *briefing* da campanha e devem guiar o ciclo de vida dos dados (da sua coleta até a sua eliminação) e durante toda as etapas da campanha publicitária (ex.: do desenho da campanha, até sua execução e pós-campanha).

3.2 Adequação & Necessidade

Os princípios da adequação e da necessidade, considerados de forma conjunta, exigem que o tratamento de dados pessoais constitua meio eficaz para o atendimento da finalidade pretendida e limitado ao mínimo necessário para tanto.

Isso implica que:

- os dados pessoais tratados e os canais utilizados sejam aptos a alcançar o objetivo legitimamente almejado
- seu uso se encontre dentro da razoável expectativa do titular
- e tanto os dados, quanto os canais utilizados sejam meios razoavelmente necessários para se atingir a finalidade pretendida

MAS O QUE É NECESSÁRIO?

- ✗ Necessário não significa “absolutamente essencial”
- ✗ Necessário não significa útil ou habitual
- ✓ Necessário significa ser um meio razoável e proporcional de atingir a finalidade pretendida[7]

7 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/principles-and-grounds-for-processing/

Recomendações práticas para observação dos princípios da Adequação & Necessidade:	
Ao escolher um canal	✅ Avalie a possibilidade de o titular razoavelmente esperar receber aquela publicidade pelo canal pretendido ✅ Verifique se o canal é adequado ao seu público-alvo
Ao selecionar os dados	✅ Avalie cuidadosamente como os dados a serem utilizados são úteis para a campanha ✅ Pondere se o titular pode razoavelmente esperar que seus dados sejam utilizados para a campanha em questão ✅ Avalie se os dados selecionados podem ser encarados como excessivamente intrusivos sob o aspecto de privacidade

⚠ **ATENÇÃO!**

Limitação temporal do tratamento: não se pode manter os dados pessoais indefinidamente e a sua manutenção, após o término da finalidade para a qual eles foram coletados, deve ser justificada.

- A publicidade é processo contínuo de análise de comportamento. Se você define a finalidade da coleta como "gestão de relacionamento com o cliente" ou "promoção de produtos da marca X", a retenção pode deixar de estar presa ao fim de uma peça publicitária específica e passar a cobrir a estratégia de marketing de longo prazo
- É relevante periodicamente verificar práticas de retenção e implementar planos de minimização de dados, descartando o que de fato se tornou obsoleto ou excessivo, documentando em seus Registros de Operações de Tratamento (RoPA), como o reuso informado beneficia o titular dos dados (ex.: ofertas mais relevantes) e como o prazo de retenção foi calculado para não ser abusivo

---

3.3 Transparência

O princípio da transparência requer que sejam fornecidas informações "claras, precisas e facilmente acessíveis" sobre o tratamento de dados pessoais. É também fundamento da confiança, pois, no marketing orientado por dados, ser transparente mitiga riscos reputacionais, evita a percepção de manipulação e pode melhorar performance de campanhas (menos rejeição, menos *opt-out)*.

Transparência bem executada não reduz performance. Pelo contrário: qualifica a base e fortalece o relacionamento de longo prazo.

O que deve ser informado?

O conteúdo mínimo das informações a serem prestadas são definidos no art. 9°, da LGPD:

- Finalidade específica do tratamento
- Forma e duração do tratamento, observados os segredos comercial e industrial
- Identificação do controlador
- Informações de contato do controlador
- Informações acerca do uso compartilhado de dados pelo controlador e a finalidade
- Responsabilidades dos agentes que realizarão o tratamento
- Direitos do titular

Observação: caso o tratamento envolva inteligência artificial, essa é uma importante informação a ser incluída ao descrever a "forma" do tratamento.

ATENÇÃO!

Caso a atividade envolva transferência internacional de dados, informações adicionais precisarão ser fornecidas:

- A forma, a duração e a finalidade específica da transferência internacional
- O país de destino dos dados transferidos
- A identificação e os contatos do controlador
- O uso compartilhado de dados pelo controlador e a finalidade
- As responsabilidades dos agentes que realizarão o tratamento e as medidas de segurança adotadas
- Os direitos do titular e os meios para o seu exercício, incluindo canal de fácil acesso e o direito de peticionar contra o controlador perante a ANPD

Interessante a comunicação tentar explicar de forma concreta para que os dados geram valor ao usuário; indicar se há uso para personalização de ofertas; segmentação comportamental; treinamento ou aprimoramento de modelos de IA; e enriquecimento com dados de terceiros.

Tão importante quanto "o que" informar, é "como" informar.

Isso significa transformar obrigações legais em arquitetura de comunicação eficiente. Considerando a natureza dinâmica e eminentemente visual do ecossistema publicitário, não é recomendável que as informações prestadas ao titular comprometam a experiência do usuário – sobretudo à luz do dever de que tais informações sejam facilmente acessíveis.

Nesse contexto, deve-se evitar o uso de linguagem excessivamente técnica ou jurídica (“juridiquês”), privilegiando-se a aplicação da linguagem simples, direta e objetiva, preferencialmente acompanhada de recursos visuais que favoreçam a clareza e a compreensão do conteúdo.

Em outras palavras, recomenda-se que o mesmo nível de atenção dedicado à experiência do usuário na elaboração de uma landing page, ex.: seja igualmente aplicado à apresentação das informações relativas à privacidade e à proteção de dados pessoais, trazendo consistência e encantamento do consumidor de ponta a ponta da comunicação da marca.

De acordo com o caso, pode-se adotar abordagem de “Avisos em Camadas” (*Layered Notices*) para equilibrar o dever de informar com a necessidade de manter uma jornada fluida:

- **Camada 1 (Interativa e Visual):** No primeiro contato (ex.: banner ou tela de cadastro), apenas as informações críticas de forma concisa e visual, utilizando ícones e linguagem direta. Foque na finalidade específica e no benefício para o usuário (ex.: “Usamos dados pessoais para sugerir as ofertas que mais combinam com você”)
- **Camada 2 (Detalhada):** Através de link de fácil acesso, disponibilize o conteúdo técnico completo exigido pelo Art. 9º da LGPD
- **Camada 3:** FAQ e exemplos práticos

5.4 Segurança & Prevenção

Os agentes da cadeia publicitária devem adotar medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6, VII, LGPD). A prevenção (art. 6, VIII) exige que medidas de mitigação sejam implementadas antes da materialização do risco, não apenas como resposta a incidentes.

4. Bases legais no marketing digital

As bases legais são hipóteses jurídicas que autorizam a atividade de tratamento de dados.

Bases Legais para tratamento de Dados Pessoais	Bases Legais para tratamento Dados Pessoais Sensíveis
• Consentimento • Cumprimento de obrigação legal ou regulatória pelo controlador • Execução de políticas públicas • Realização de estudos por órgão de pesquisa • Execução de contrato ou de procedimentos preliminares • Exercício regular de direitos • Proteção da vida ou da incolumidade física • Tutela da saúde • Legítimo Interesse • Proteção do crédito	• Consentimento específico e destacado • Cumprimento de obrigação legal ou regulatória pelo controlador • Execução de políticas públicas • Realização de estudos por órgão de pesquisa • Exercício regular de direitos • Proteção da vida ou da incolumidade física • Tutela da saúde • Garantia da prevenção à fraude e à segurança do titular

Não há hierarquia entre as bases legais previstas na LGPD – isto é, o Controlador possui discricionariedade para eleger a base legal que melhor se adeque à atividade de tratamento, desde que efetivamente aplicável ao caso concreto.

No contexto das atividades de marketing, duas bases legais tendem a ser mais comumente aplicáveis: o consentimento e o legítimo interesse. Em razão disso, este guia concentra-se especificamente na análise dessas duas hipóteses legais.

4.1 Brasil x Europa

Embora a legislação nacional tenha sido inspirada no modelo europeu, os respectivos ecossistemas normativos não são idênticos. O sistema europeu, ex.: contempla normas específicas que impactam restritivamente a atividade publicitária, especialmente a Diretiva *ePrivacy* e suas transposições para as legislações nacionais, as quais impõem o consentimento como requisito para diversas atividades publicitárias[8]. Inclusive, o Digital Omnibus propõe alterar tais regras tentando diminuir o fenômeno da "Fadiga de Consentimento".

8 https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-on-the-use-of-storage-and-access-technologies/what-are-storage-and-access-technologies/#what_technologies_does_PECR_apply_to

No Brasil, o legítimo interesse pode ser juridicamente aplicável a determinadas atividades de marketing, desde que sua adequação seja avaliada caso a caso e devidamente demonstrada por meio de teste de balanceamento, ponderando a legitimidade do interesse, a necessidade do tratamento, os impactos sobre os direitos dos titulares e suas legítimas expectativas. Essa avaliação deve ser ainda mais rigorosa quando envolver crianças e adolescentes, observando-se o princípio do melhor interesse e as restrições específicas aplicáveis a esse público, inclusive aquelas previstas no ECA Digital, conforme tratado no item 8 deste Guia.

Neste sentido o ICO aponta que, quando não proibida pela regulamentação específica (que, novamente, inexiste no Brasil), a atividade de *marketing* direcionado é considerada um "interesse legítimo", desde que satisfaça os testes de necessidade e proporcionalidade[9].

4.2 Consentimento e legítimo interesse: quando usar cada um

A aplicação dessa base legal requer que os interesses legítimos do Controlador sejam proporcionais aos impactos aos direitos e liberdades do titular.

O **Teste de Balanceamento documentado** é a forma mais adequada de verificar e demonstrar a proporcionalidade do legítimo interesse e se constitui das seguintes etapas

- **Teste de Finalidade:** para identificar se compatível com o ordenamento jurídico, fundado em situação concreta e vinculado a finalidade legítima, específica e explicitamente definida
- **Teste de Necessidade:** para verificar se o tratamento de dados pessoais é um meio razoável e proporcional de se atender a finalidade almejada, tratando o menor volume de dados possível
- **Teste de Proporcionalidade:** para avaliar os riscos e impactos do tratamento sobre os direitos e liberdades dos titulares e sua proporcionalidade em relação aos interesses perseguidos

Como o contexto e o próprio processo sofrem mudanças, é recomendável que o teste seja revisto periodicamente.

Observação: ANPD dispõe de modelo de teste de balanceamento em seu guia sobre o legítimo interesse[10].

🔔 **IMPORTANTE!** Além disso, quando a atividade de tratamento se operar em larga escala ou puder afetar significativamente direitos ou interesses relevantes do titular, é recomendável, além do teste de balanceamento, elaborar o relatório de impacto.

9 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/when-can-we-rely-on-legitimate-interests/#marketing_activities.
10 https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf

APLICAÇÃO PRÁTICA NO MARKETING: quando é mais adequado usar o legítimo interesse?

Embora não seja possível delimitar, em abstrato, as hipóteses em que o legítimo interesse se mostra juridicamente adequado, há elementos que auxiliam no enquadramento do tratamento nessa base legal:

Não tratamento de dados pessoais sensíveis

O legítimo interesse apenas é aplicável para o tratamento de dados pessoais comuns

Soft opt-in

Em regra, a existência de relação prévia entre o controlador e a titular impacta positivamente a expectativa legítima de tratamento de seus dados pessoais para fins publicitários[11]. É importante destacar que o *soft opt-in* não substitui a necessidade de fundamentação da atividade de tratamento em uma base legal ou garantir a transparência para com o titular

***Opt-out* de forma facilitada**

O direito de oposição deve ser assegurado de forma plena, possibilitando ao titular requerer, de maneira simples e facilitada, a sua interrupção[12]

Transparência

Quanto mais bem informado é o titular, de forma clara, direta e inequívoca, maior a probabilidade de fundamentação da atividade no legítimo interesse

Respeito à privacidade

Quanto menor o grau de intrusão em relação aos dados pessoais e de sua origem na esfera de intimidade do titular, maior tende a ser a aderência ao enquadramento da atividade de tratamento na base legal do legítimo interesse

ADEQUADO:	INADEQUADO:
Envio de e-mail marketing para base de clientes ou *leads* que forneceram os dados de contato Utilização, por e-commerce, de informações sobre histórico de ações e/ou compras do titular em sua própria plataforma para oferta de produtos de seu provável interesse Perfilamento de clientes para identificar potenciais casos de *churn* (perda de clientes e/ou receita) e atuação preventiva Segmentação demográfica da base de *leads* para direcionamento de ofertas	Construção de perfis baseados em dados pessoais sensíveis Rastreamento invasivo da atividade do titular através de múltiplos websites, sem transparência adequada, para a construção de perfis comportamentais Contatos direitos insistentes sem prévia relação com o titular

11 https://ferramentas.download.uol.com.br/uolhost/contratos/Codigo_de_Autorregulamentacao_para_pratica%20_de_email_Marketing.pdf
12 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/

Mas e o consentimento?

- Pode ser utilizado como alternativa ao legítimo interesse quando houver alta intrusão, ausência de relação prévia, expectativa reduzida do titular ou uso de dados sensíveis. Quando adequadamente empregado, tende a fortalecer a relação de confiança entre o Anunciante e o titular

- Contudo, sua adoção deve ser realizada de forma criteriosa (preferencialmente nas hipóteses em que o legítimo interesse não seja aplicável), visto que possui requisitos estritos de validade. Sua implementação inadequada pode comprometer a legalidade da atividade da atividade de tratamento[13,14]

☆ **LEMBRE-SE:** diferentemente do consentimento, que transfere ao titular a decisão inicial, o legítimo interesse exige maior responsabilidade interna, pois o controlador assume o ônus de demonstrar que o tratamento é proporcional e legítimo.

13 https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.
14 https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

USO DO CONSENTIMENTO COMO BASE LEGAL NO CONTEXTO DO MARKETING

Requisito: consentimento deve ser...	Aplicando na prática
Livre: titular precisa ter uma escolha real de não consentir (autorização apenas formal não basta). Sempre que possível, deve existir uma opção concreta de recusa, que não gere prejuízo ao titular	✓ O consentimento não deve ser requisito para obtenção de benefício ou serviço que não seja dependente da atividade de tratamento. ✓ Cada finalidade deve ser objeto de um consentimento apartado
Informado: titular deve receber informação suficiente sobre a atividade de tratamento para tomar uma decisão consciente sobre ela	✓ Elaborar um termo de consentimento (vide item 3 deste guia para requisitos) ✓ Apresentar a informação em camadas ✓ A primeira camada (*opt-in*) deve conter a síntese da atividade de tratamento a ser executada, com os elementos de dados pessoais mais impactantes ao titular, sendo acompanhada de *link* para o termo de consentimento
Inequívoco: titular deve fornecer o seu consentimento por meio de uma declaração afirmativa de vontade (não existe consentimento por omissão)	✓ Usar caixas de seleção (sempre desabilitadas) ou outros mecanismos ✓ Apenas iniciar a coleta de dados após o titular afirmar o seu consentimento
Finalidade específica: não pode ser fornecido de forma abstrata ou para finalidades genéricas	✓ Delimitar com cuidado a finalidade concreta da atividade ✓ Apresentar a finalidade de forma clara e objetiva ✓ Existindo múltiplas camadas de informação, a finalidade sempre deve se encontrar destacada na primeira camada
Destacado: deve ser destacado de outros termos (ex.: termo de uso, contratos...)	✓ Separar o termo de consentimento de outros documentos legais ✓ Na camada em que o consentimento é obtido, ele deve ser apartado de outros aceites

Fadiga do consentimento: o uso indiscriminado de consentimento pode gerar: saturação de solicitações; decisões automáticas e pouco refletidas pelo titular; redução da efetiva compreensão; perda de credibilidade da marca. Ou seja, consentimentos excessivos e mal estruturados não fortalecem a proteção de dados. Ao contrário, enfraquecem a experiência do usuário e podem comprometer a validade jurídica.

4.3 *Cookies* e *first-party*

Em guia orientativo, a ANPD presume que *cookies* utilizados para fins publicitários, em regra, não se enquadrariam na base legal do legítimo interesse[15].

15 https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf

Contudo, conforme já esclarecido, diferentemente da UE, no qual a coleta de consentimento para *cookies* publicitários decorre de imposição específica da Diretiva *ePrivacy*, não há obrigação equivalente na LGPD.

Tal presunção, portanto, não pode ser tratada como absoluta, sob pena de afronta ao princípio constitucional da legalidade, pois a LGPD não hierarquiza bases legais.

***FIRST-PARTY COOKIES*: há medidas capazes de favorecer o enquadramento da atividade de tratamento na base legal do legítimo interesse no direito brasileiro (vide quadro "atenção" e orientações sobre transparência, política e banner, abaixo),** dentre as quais se destaca a utilização de *first-party cookies*, isto é: *cookies* originados e utilizados exclusivamente pelo próprio website acessado pelo titular, vinculados ao seu domínio[16], os quais, diferentemente dos *cookies* de terceiros, não implicam, em regra, o compartilhamento automático de dados com fornecedores externos voltados à realização de perfilamento abrangente do titular e através de diferentes aplicações de internet por ele acessadas.

⚠ ATENÇÃO!

Embora os *first-party cookies* reduzam significativamente os riscos à privacidade quando comparados aos cookies de terceiros, é imprescindível que o enquadramento no legítimo interesse seja sempre objeto de avaliação concreta – sendo recomendável sua formalização por meio do teste de balanceamento.

Isso porque podem existir situações em que a coleta de informações de navegação na própria aplicação de internet da organização resulte na revelação de informações intrusivas à esfera privada do titular, inclusive dados pessoais sensíveis.

A título exemplificativo, o rastreamento da atividade de um titular em um website de relacionamentos pode revelar preferências sexuais, as quais constituem dado pessoal sensível, sendo o legítimo interesse, consequentemente, uma base legal inadequada.

***COOKIES* DE TERCEIROS:** como não há hierarquia entre as bases legais para o uso de *cookies*, as empresas podem adotar o Legítimo Interesse ou o Consentimento, dependendo da natureza da campanha e do nível de intrusividade. Embora o Guia Orientativo de *Cookies* da ANPD privilegie o consentimento, vale destacar que o legítimo interesse também pode ser aplicável, especialmente quando a personalização visa a eficiência do marketing e o benefício do consumidor (ofertas relevantes), desde que acompanhada de transparência absoluta, respeito à expectativa do usuário, baixa intrusividade das informações coletadas e tratadas, além da garantia de *opt-out* facilitado. A decisão deve ser fundamentada em uma Avaliação de Legítimo Interesse (LIA) documentada, que pondere os interesses do negócio e os direitos do consumidor, assegurando que o rastreamento não seja abusivo ou inesperado.

16 https://iabbrasil.com.br/wp-content/uploads/2021/08/IAB-BRASIL_PARECER-JURIDICO_LGPD-E-PUBLICIDADE-PERSONALIZADA_MARCEL-LEONARDI.pdf

TRANSPARÊNCIA: Independentemente da base legal adotada, é indispensável assegurar a transparência e, conforme o caso, a adequada oferta do consentimento e, sempre, a possibilidade clara e efetiva de gerenciamento das preferências de privacidade. No contexto do uso de *cookies*, tais requisitos são, em geral, atendidos por dois mecanismos principais: (a) a elaboração de uma Política de *Cookies*, seja como documento autônomo, seja integrada ao Aviso de Privacidade; e (b) a disponibilização de um cookie banner com opções funcionais e acessíveis de gerenciamento dos *cookies*.

POLÍTICA DE *COOKIES*: o documento segue os mesmos requisitos do Aviso de Privacidade vistos acima, com enfoque no tratamento executado por meio dos *Cookies*[17]. É uma prática habitual do mercado que se especifique quais *cookies* são utilizados, suas respectivas finalidades e seu prazo de validade.

BANNER DE *COOKIES*: trata-se de uma ferramenta que auxilia as organizações na conformidade com a LGPD, na medida em que oferece ao titular informações claras e automatizadas sobre o tratamento de seus dados pessoais e lhe permite o gerenciamento de suas preferências de privacidade. Tipicamente, essas ferramentas são estruturadas em duas camadas.

- Na primeira camada, o cookie banner deve fornecer ao titular uma síntese clara das finalidades para as quais seus dados podem ser tratados por meio de *cookies*, bem como uma opção de acesso à segunda camada de informações e de seleção ou gerenciamento dos *cookies*. Além disso, quando a base legal adotada for o consentimento, é indispensável a existência de opção clara e inequívoca de rejeição dos *cookies* tratados com base nessa hipótese, a qual deve ser apresentada com destaque equivalente à opção de aceitação, de modo a evitar a configuração de *dark patterns*

- Na segunda camada, acessível a partir da primeira, os *cookies* devem ser organizados em categorias, definidas e descritas de acordo com suas finalidades, permitindo ao titular habilitar ou desabilitar cada uma delas. Quando a base legal adotada for o consentimento, tais categorias devem permanecer desabilitadas por padrão

4.4 Dados sensíveis no marketing

Para que uma informação seja considerada um dado pessoal sensível, ela deve se enquadrar no rol taxativo[18] do art. 5°, II, da LGPD. Ou seja, ser relativo a: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

17 https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

18 https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788&registro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF

Para os negócios, isso traz maior previsibilidade: informações que não se enquadram estritamente nessas categorias são tratadas como dados comuns, o que pode permitir a avaliação do legítimo interesse para otimização de campanhas e personalização, desde que a base legal seja efetivamente aplicável ao caso concreto e acompanhada do respectivo teste de balanceamento.

A preocupação com dados sensíveis surge quando o cruzamento de dados comuns permite inferir uma característica sensível[19]. Contudo, para que essa inferência seja legalmente relevante, ela deve permitir a identificação ou individualização do titular sob aquela ótica de dado sensível.

"Quando o marketing sabe de sua saúde antes de sua família" – caso paradigmático de tratamento sensível de dados pessoais: a partir da análise de dados demográficos e do histórico de compras, uma grande rede varejista dos Estados Unidos, conseguiu inferir que uma adolescente estava grávida (dado ligado à sua saúde) antes mesmo de ela contar isso ao próprio pai, passando então a enviar cupons e ofertas direcionados a mulheres grávidas[20].

Como regra, o uso dessas informações no Marketing requer o consentimento específico e destacado do titular, de forma segregada dos demais consentimentos ou, minimamente, o uso de mecanismos para evidenciar o tratamento de dados pessoais sensíveis que serão objeto do tratamento (ex.: citando-os de forma específica e destacada na camada em que o titular efetivamente aceita o consentimento).

Por outro lado, o uso de dados agregados ou estatísticos para entender tendências de mercado (ex.: aumento de busca por produtos de maternidade em certa região) não constitui tratamento de dado sensível, pois não foca na individualização do titular (dados anonimizados).

4.5 *Consent or Pay*

O *Consent or Pay* é um modelo alternativo de negócio, que se propagou, sobretudo, em algumas redes sociais e outros serviços "gratuitos", decorrentes das limitações pelas autoridades supervisoras de proteção de dados europeias do uso de dados pessoais para a publicidade direcionada.

19 https://www.cjf.jus.br/cjf/corregedoria-da-justica-federal/centro-de-estudos-judiciarios-1/publicacoes-1/jornadas-cej/enunciados-aprovados-2022-vf.pdf
20 https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

No contexto publicitário, o *Consent or Pay* refere-se a modelos de negócio que, cumulativamente[21]:

Oferecem ao titular duas ou mais opções com a possibilidade de: • consentir com o tratamento de seus dados pessoais, sem a exigência de pagamento para acesso ao produto ou serviço • optar pelo pagamento para obtenção de acesso ao produto ou serviço, com consequente redução do tratamento de seus dados pessoais	Direciona o consentimento **de forma específica para fins publicitários, em especial para a publicidade comportamental** (aquela baseada na perfilização do titular a partir de seu comportamento ao longo do tempo, ainda que possa ser agregada a dados fornecidos proativamente pelo próprio usuário).

A ANPD ainda não se posicionou sobre esse modelo, mas o European Data Protection Board - EDPB o aborda em sua Opinião n° 08/2024[22], na qual apresenta cuidados relevantes para garantir que o consentimento atenda aos quesitos de validade listados acima:

Requisito 1: consentimento livre

Existência de alternativa viável ao consentimento:

- **Fornecimento de alternativa gratuita:** embora **inexista obrigatoriedade de oferta de serviços gratuitos,** a disponibilização de alternativa que envolva menor grau de tratamento de dados pessoais para fins publicitários, como a utilização exclusiva de dados fornecidos diretamente pelo próprio titular, tende a reforçar a validade do consentimento
- **O valor cobrado deve ser razoável:** a taxa deve (i) ser razoavelmente necessária; (ii) não inviabilizar, na prática, a recusa do consentimento; e (iii) ter seu valor definido de forma documentada, em observância ao princípio da prestação de contas

Inexistência de detrimentos significativos ao titular:

- **Custo acessível:** o valor cobrado não pode inibir, na prática, a liberdade de escolha
- **A ausência de acesso ao serviço não pode levar a impactos substanciais na vida do titular:** o consentimento tende a não ser considerado livre se o serviço (i) ser essencial ou insubstituível na vida do titular; (ii) for um condicionante prático a participação na vida social; (iii) impedir acesso a emprego ou redes profissionais; (iv) criar efeitos de rede que inviabilizem a recusa do consentimento; ou (v) gerar efeito de *lock-in*, em razão da presença digital previamente consolidada do usuário

Desequilíbrio de poderes:

- **Ausência de consequência negativa:** em cenários de desequilíbrio de poderes, o consentimento deve ser utilizado apenas na medida em que se garanta a ausência de consequência negativas. São exemplos de indicadores desses cenários: (i) posição dominante do agente no mercado; (ii) serviços que tenham formado grande base de usuários a partir de oferta originalmente gratuita; e (iii) tratamento direcionado a públicos vulneráveis

21 https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en
22 https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-082024-valid-consent-context-consent-or_en

Requisito 2: consentimento informado

Além das informações requeridas pela legislação nacional, o EDPB recomenda que sejam informados aos titulares:

- Quais dados são coletados independentemente da opção do titular quanto à publicidade comportamental
- O direito de revogação do consentimento e suas consequências
- A eventual combinação ou uso cruzado de dados, indicando se e em que medida os dados são compartilhados com outros serviços ou controladores

Requisito 3: consentimento inequívoco

Cuidado especial quanto à linguagem utilizada, de modo que:

- Seja evidente para qual finalidade o titular está consentindo
- O consentimento não seja apresentado meramente como alternativa à cobrança
- Sejam evitadas expressões que destaquem apenas a gratuidade do serviço, em detrimento da explicitação do tratamento de dados decorrente do consentimento

Requisito 4: consentimento específico

A finalidade do tratamento deve ser específica, explícita e legítima, formulada de modo a permitir que o titular compreenda claramente quais atividades de tratamento serão realizadas a partir do consentimento fornecido.

5. Publicidade direcionada e perfilamento

O perfilamento consiste na análise sistemática de dados pessoais para avaliar, inferir ou prever aspectos da personalidade, do comportamento, dos interesses e dos hábitos de um indivíduo. Tipicamente é uma forma de tratamento automatizado de dados pessoais que utiliza essas informações para analisar ou antecipar elementos como desempenho profissional, situação econômica, saúde, preferências, confiabilidade, comportamento, localização, preferências ou movimentos de uma pessoa física[23].

23 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/

No âmbito do *marketing* o perfilamento é habitualmente utilizado para:

- Identificar as preferências dos consumidores, direcionando publicidade de produtos que estejam mais alinhados ao seu desejo
- Prever o comportamento de clientes, ex.: identificando prováveis casos de *churn* para permitir a atuação preventiva
- Tomar decisões, ex.: elegendo a melhor estratégia publicitária para cada perfil

---

⚠ ATENÇÃO!

Segmentação publicitária, não necessariamente é perfilamento.

Em que pese a segmentação do público em campanhas publicitárias possa ocorrer com base em técnicas de perfilamento, tal prática não constitui requisito necessário para o direcionamento de anúncios. O simples direcionamento de publicidade com fundamento em informações demográficas básicas – como a segmentação de consumidores por faixa etária, sexo ou localização geográfica – não configura, por si só, perfilamento, na medida em que não envolve a análise de dados pessoais destinada a avaliar, inferir ou prever aspectos do comportamento, da personalidade ou das preferências individuais dos titulares.

Quando o perfilamento resultar em decisão tomada unicamente com base em tratamento automatizado de dados pessoais e produzir efeitos jurídicos ou impactos práticos relevantes ao titular, devem ser observados os **direitos previstos no art. 20 da LGPD**. O simples uso de perfilamento para fins de segmentação ou personalização publicitária, sem decisão automatizada relevante sobre o titular, não deve ser tratado, por si só, como hipótese automática de incidência do art. 20.

24 ICO. **Automated decision-making and profiling**. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/

Direitos do art. 20	
Explicação: possibilidade de solicitar informações claras e adequadas sobre os critérios e procedimentos utilizados na decisão automatizada, respeitados o segredo comercial e industrial. • Recomendação: informação deve incluir, ao menos, os dados pessoais utilizados na formação do perfil e suas respectivas fontes (Sumula n° 550 do STJ[25]) • Quando parte das informações não é inteligível para pessoa humana, podem ser substituídas por esclarecimentos: (a) em que constitui a informação; (b) por que ela não pode ser fornecida ; e (c) como ela é mantida[26]	**Revisão:** possibilidade de solicitar a revisão de decisões tomadas de forma automatizada, inclusive baseadas em perfilamento. • Atualmente, não há obrigação legal de que essa revisão seja realizada por uma pessoa humana[27], mas é indispensável que ocorra uma revisão efetiva e justa, capaz de alterar o resultado da decisão • Exemplo: permitir que o titular aponte informações incorretas ou desatualizadas, promovendo-se a sua correção e a reexecução do processo de perfilamento com base nos dados atualizados

Embora a LGPD não afirme expressamente, é uma interpretação razoável que os direitos acima descritos apenas são aplicáveis em situações nas quais a decisão automatizada gera efeitos jurídicos ou práticos relevantes ao titular, assim como no GDPR. São exemplos em que decisões no âmbito do marketing podem gerar efeitos relevantes ao titular:

- Definição automatizada de elegibilidade para ofertas ou benefícios
- Perfilamentos que definam de forma material ou relevante a experiência do titular, como prioridade de suporte, tipo de atendimento, acesso a ofertas substancialmente diferenciadas ou outras condições relevantes da relação com a marca
- Sistemas de precificação baseado em perfil (embora a licitude de tais sistemas seja questionável no direito do consumidor brasileiro)
- Aprovação da participação ou exclusão automática de programas de fidelidade ou recompensas

---

ATENÇÃO!

Decisões relevantes podem demandar a elaboração do Relatório de Impacto.

Quando o tratamento de dados pessoais para fins de decisões automatizadas gerar efeitos jurídicos ou impactos práticos relevantes ao titular, recomenda-se a elaboração de Relatório de Impacto à Proteção de Dados Pessoais. Isso porque, nessas hipóteses, é provável que se esteja diante de uma atividade de tratamento de alto risco, nos termos do art. 4º da Resolução CD/ANPD nº 2, cujo enquadramento decorre do fato de a atividade satisfazer um critério geral (potencial de afetar significativamente interesses e direitos fundamentais dos titulares) e um critério específico (decisões tomadas unicamente com base em tratamento automatizado de dados pessoais).

25 https://arquivocidadao.stj.jus.br/index.php/sumula-550-2;isad?sf_culture=en

26 https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/#access

27 https://www.congressonacional.leg.br/materias/vetos/-/veto/detalhe/12445

6. Publicidade programática e ecossistema de adtech

A publicidade programática revolucionou o setor ao permitir a compra automatizada de mídia em milissegundos, garantindo que a mensagem certa chegue ao consumidor certo no momento ideal. O modelo de *Real-Time Bidding* (RTB) é o pilar dessa eficiência, otimizando orçamentos e democratizando o acesso de pequenos anunciantes a grandes inventários.

Habitualmente, o fluxo de dados no ecossistema da Publicidade Programática funciona nos seguintes termos[28]:

- Usuário acessa o site de um Veículo
- O Veículo apresenta uma demanda ao SSP, compartilhando eventuais informações detidas sobre o usuário e conteúdo que ele está visualizando
- A SSP envia uma solicitação de anúncio para múltiplas DSPs que representam Anunciantes interessados em adquirir o inventário de anúncios (a requisição geralmente inclui dados do usuário tais como geolocalização, endereço de IP, detalhes do dispositivo, eventuais interesses inferidos (perfil), informações demográficas e aplicação de *internet* que o usuário está acessando)
- As DSPs analisam automaticamente os dados disponíveis sobre o usuário, como informações demográficas ou comportamento de navegação, com o objetivo de avaliar o valor daquela impressão publicitária. Além dos dados fornecidos pela SSP, essa avaliação pode basear-se em perfis de usuários que os Anunciantes tenham construído previamente
- Com base nessa análise, as DSPs realizam lances automáticos pelo inventário de anúncios disponível
- A SSP conduz um leilão em tempo real e seleciona o maior lance vencedor
- O anúncio do Anunciante vencedor é então exibido no site do Veículo

Todo esse processo ocorre em instantes – sendo conhecido como *Real-Time Bidding* (RTB)

28 https://www.waytogrow.com/blog/ssp-platforms/; https://www.eff.org/deeplinks/2026/01/google-settlement-may-bring-new-privacy-controls-real-time-bidding

DESAFIOS:

- No modelo de *Real-Time Bidding* (RTB), as informações necessárias para a segmentação circulam entre múltiplos agentes para que o leilão ocorra em milissegundos. O mercado deve atuar para que esse fluxo seja pautado pelo princípio da proporcionalidade, garantindo que apenas os dados estritamente necessários para a precificação da impressão sejam compartilhados
- O risco de agentes maliciosos buscarem acesso a dados sem a intenção real de compra de mídia deve ser combatido através de uma curadoria rigorosa de parceiros tecnológicos. Anunciantes e agências devem priorizar o uso de redes e plataformas (DSPs e SSPs) que adotem protocolos de segurança robustos
- Avaliar, quando pertinente, outras modalidades de publicidade direcionada, como a contextual (contextual advertising), na qual o direcionamento não se baseia no tratamento de dados do usuário, mas no contexto do ambiente em que ele se encontra, alocando a publicidade de forma coerente com o conteúdo acessado – ex.: a exibição de anúncios de tênis de corrida em uma página de um evento de corrida de rua[29]
- Utilização de Walled Gardens (ecossistemas fechados nos quais as operações e os dados são centralizados e controlados pelo operador da plataforma) nos quais o acesso dos anunciantes a dados dos usuários é limitado, o que contribui para a proteção da privacidade do titular em comparação ao modelo de RTB. Esse modelo, contudo, é alvo de críticas no contexto do marketing em razão da menor transparência quanto aos dados, métricas e processos envolvidos
- Lidar e regular a relação de controladores independentes que intervenham no processo, como agregadores e fornecedores de dados pessoais (data brokers), que coletam, enriquecem e comercializam bases de dados entre anunciantes e plataformas – garantindo o atendimento das obrigações correspondentes de transparência, base legal, segurança e resposta a direitos dos titulares

7. Transferência internacional de dados no marketing[30]

Nas operações de marketing digital, a maior das transferências internacionais de dados frequentemente ocorre de forma acessória. Isso se verifica, ex.: quando:

- A plataforma de disparo de e-mails está hospedada em servidor no exterior
- O CRM utiliza infraestrutura em nuvem localizada fora do Brasil
- Ferramentas de analytics ou mídia programática operam a partir de data centers estrangeiros

Nesses casos, a transferência não constitui a finalidade principal do tratamento, mas sim uma consequência técnica da arquitetura tecnológica adotada.

29 https://iabeurope.eu/wp-content/uploads/IAB-Europe-Guide-to-Contextual-Advertising-July-2021.pdf
30 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396

Para que a Transferência Internacional de Dados seja lícita é necessário o atendimento de dois requisitos:

- Se fundamentar em uma das bases legais dos arts. 7° e 11, da LGPD, conforme o caso
- Se fundamentar em um dos Mecanismos de Transferência Internacional de Dados, listados no art. 33°, da LGPD

Quando a transferência for meramente instrumental ou secundária, a base legal que fundamenta o tratamento principal (como legítimo interesse ou consentimento) pode, em regra, sustentar também a transferência, desde que sejam adotadas as salvaguardas exigidas pela regulamentação aplicável.

Ainda assim, permanece a obrigação de:

- Garantir mecanismo jurídico válido para a transferência
- Assegurar nível adequado de proteção de dados
- Informar o titular de forma clara sobre a ocorrência da transferência internacional

Situação distinta ocorre quando a própria transferência internacional constitui elemento central da operação. Isso pode acontecer, ex.: quando:

- Há compartilhamento estratégico de base de dados com matriz estrangeira para fins analíticos
- Dados são enviados para terceiros no exterior para enriquecimento, modelagem comportamental ou consolidação global de perfis
- A operação de marketing é estruturada a partir de processamento concentrado em outro país como parte essencial do modelo de negócio

Nesses casos, a transferência é parte estruturante da finalidade do tratamento, devendo-se avaliar com maior rigor a compatibilidade da base legal utilizada.

Superada a base legal, cabe avaliar a implementação dos mecanismos de transferência internacional de dados (ex.: as hipóteses previstas no art. 33° da LGPD), cujo objetivo é assegurar que os dados estarão com o mesmo nível de proteção legal, mesmo saindo do país.

O Controlador apenas implementa diretamente o mecanismo de transferência internacional de dados quando é o responsável por exportar os dados a agente de tratamento localizado em país terceiro.

Exemplos práticos	Controlador é o Exportador?
O Controlador contrata serviço que, por sua própria natureza, envolve fluxos de dados transfronteiriços (ex.: rede global de processamento e armazenamento de dados em nuvem)	✅ Sim
O Controlador contrata um fornecedor nacional e o fornecedor opta por contratar um suboperador localizado no exterior	❌ Não

Portanto, quando o Controlador figurar como exportador, é essencial que implemente diretamente o mecanismo de transferência internacional – o que, em regra, implicará exigir do importador a adesão às cláusulas-padrão contratuais[31].

Quando o Controlador não atuar como exportador, deverá demandar que seu fornecedor se comprometa contratualmente a implementar os mecanismos de transferência internacional aplicáveis e a fornecer evidências de sua efetiva implementação.

EXCEÇÃO: transferência para agentes de tratamento localizados na União Europeia, dada a existência de decisões de adequação mútuas, dispensam quaisquer outros mecanismos.

OBSERVAÇÃO

Quando o mecanismo de transferência internacional tiver natureza contratual, o Titular possui o direito de solicitar cópia do respectivo clausulado, resguardados eventuais elementos protegidos por segredo comercial nele constantes. Assim, é essencial que o Controlador mantenha cópia do clausulado aplicável. Ademais, cabe ao Controlador fornecer informações relativas à transferência internacional, conforme já tratado no tópico de transparência.

8. Crianças e adolescentes no marketing digital

A Lei nº 15.211/2025 (ECA Digital), interpretada em conjunto com a LGPD, reforça a proteção de crianças e adolescentes no ambiente digital e estabelece parâmetros mais rigorosos para o tratamento de seus dados pessoais no contexto publicitário.

A proteção integral desse público exige que estratégias de marketing digital sejam estruturadas com governança reforçada, critérios de necessidade e mecanismos preventivos de risco.

31 https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396

a) Base legal para tratamento de dados de menores de idade:

O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei, conforme enunciado CD/ANPD 1/2023.

Legítimo interesse: embora seu emprego seja juridicamente possível, ele deve sempre observar o princípio do melhor interesse da criança e do adolescente.

⚠ **ATENÇÃO!**

O consentimento para o tratamento de dados pessoais de crianças deve ser concedido pelos pais ou responsáveis legais, conforme previsto pela LGPD. Em relação aos relativamente incapazes, ou seja, adolescentes de 16 a 18 anos, é recomendável que se assegure, pelo menos, a assistência dos pais ou responsáveis legais.

---

b) Melhor Interesse de crianças e adolescentes:

O melhor interesse do menor é conceito que abrange três aspectos[32]:

- **Direito substantivo:** garantia de que o melhor interesse da criança será considerado de forma primária em qualquer decisão que a afete, individual ou coletivamente
- **Princípio:** determinação de que, diante de múltiplas interpretações possíveis de uma norma, deve prevalecer aquela que melhor atenda ao interesse da criança
- **Regra processual:** exigência de que decisões que impactem crianças incluam a avaliação de seus efeitos, com garantias procedimentais e justificativa explícita de como o melhor interesse foi considerado

O principal ponto é que a estratégia não instrumentalize a vulnerabilidade como vantagem competitiva.

- **Exemplo:** é adequado o tratamento de dados pessoais para o direcionamento de livros e outros conteúdos educativos compatíveis com a idade do menor. Por outro lado, qualquer tipo de publicidade direcionada mediante perfilamento é vedada pelo ECA Digital

Qualquer que seja o caso, é sempre importante documentar o processo de avaliação do melhor interesse do menor.

32 https://www.gov.br/anpd/pt-br/assuntos/noticias/nota-tecnica-50_pub_0153891.pdf

c) Gestão de riscos:

O ECA Digital estabelece que, sempre que fornecedores de produtos ou serviços de tecnologia da informação tratarem dados pessoais de menores de idade para finalidades distintas da mera operacionalização do produto ou serviço, deverão realizar atividades de gestão de riscos, que incluam, no mínimo: (a) o mapeamento e a mitigação dos riscos envolvidos; e (b) a elaboração de relatório de impacto à proteção de dados pessoais.

d) Perfilamento:

O Perfilamento é técnica que tem sido amplamente utilizada nos últimos anos como estratégia de marketing, pois permite uma compreensão mais profunda do cliente e otimiza campanhas de marketing ao viabilizar o direcionamento da mensagem correta (e personalizada) ao público desejado. Por meio da coleta e análise de dados pessoais, identifica características, comportamentos, interesses e necessidades que resultam na construção de perfis detalhados para cada indivíduo, possibilitando individualização e criação estratégias de marketing mais personalizadas e eficazes.

De acordo com o entendimento consolidado pelo ECA Digital, as técnicas de perfilamento, quando direcionadas a menores (mais suscetíveis à sugestão), tem maior potencial de explorar a vulnerabilidade psicológica desse público que, em linha com a Constituição Federal e o Estatuto da Criança e do Adolescente (ECA), são considerados pessoas em condição peculiar de desenvolvimento sem discernimento suficiente para compreender estratégias de marketing digital baseadas em dados. **Por essa razão, a Lei veda o perfilamento e a análise emocional de crianças e adolescentes com a finalidade de direcionamento de publicidade comercial para esse público.**

Assim, ao desenhar suas campanhas com estratégias de perfilamento para direcionamento publicitário, marcas e agências agora devem adotar diretrizes absolutas, não apenas evitando qualquer uso de dados pessoais que pressuponha identificação ou segmentação de menores, mas adotando medidas de segurança eficazes para excluir titulares menores de idade da sua realização.

🔔 IMPORTANTE!

A mera segmentação publicitária ou o perfilamento em si não implica em violação ao ECA Digital ou à LGPD. Permanecem juridicamente possíveis e muitas vezes necessárias: segmentações amplas por faixa etária; classificação de conteúdo adequada à idade; filtros de segurança; ferramentas de verificação etária; comunicação contextual não baseada em rastreamento individual. Inclusive, o uso de dados pessoais de forma responsável e ética é premissa inclusive para viabilizar à proteção integral da criança e do adolescente.

Para mitigar os riscos de realização de perfilamento publicitário em relação a menores de idade, é relevante a adoção de medidas específicas no desenvolvimento de campanhas com restrição etária, tais como[33]:

- Evitar a utilização de mídias com volume significativo de menores de idades (ex.: mais de 25% do público), incluindo a análise de dados demográficos de seguidores de influenciadores antes de parcerias

- Utilizar a tecnologia disponível para garantir que os ads são negativamente direcionados para esse público, de modo que menores de idade não recebam o conteúdo publicitário (ex.: *negative targeting, age-gating*)

- Evitar o uso de *lookalike audiences* / expansão automática de público quando houver risco de alcançar menores: essas técnicas consistem em ampliar automaticamente a segmentação para usuários "semelhantes" à audiência original (com base em padrões de comportamento, interesses ou perfis), o que pode incluir inadvertidamente menores — especialmente quando os dados de origem não são totalmente confiáveis ou quando há sobreposição de interesses entre adultos e jovens. Nesses casos, recomenda-se desativar esse tipo de otimização automática ou utilizá-la apenas com camadas adicionais de restrição (ex.: exclusões etárias robustas e filtros de interesse claramente adultos)

- Avaliar as políticas de restrição de idade para publicidade da plataforma que se deseja fazer uso

Além disso, quando da celebração de contratos com agências publicitárias e outras entidades que participem da cadeia de marketing, é importante estabelecer obrigações contratuais a respeito da adoção de medidas apropriadas para evitar o perfilamento publicitário de menores de idade.

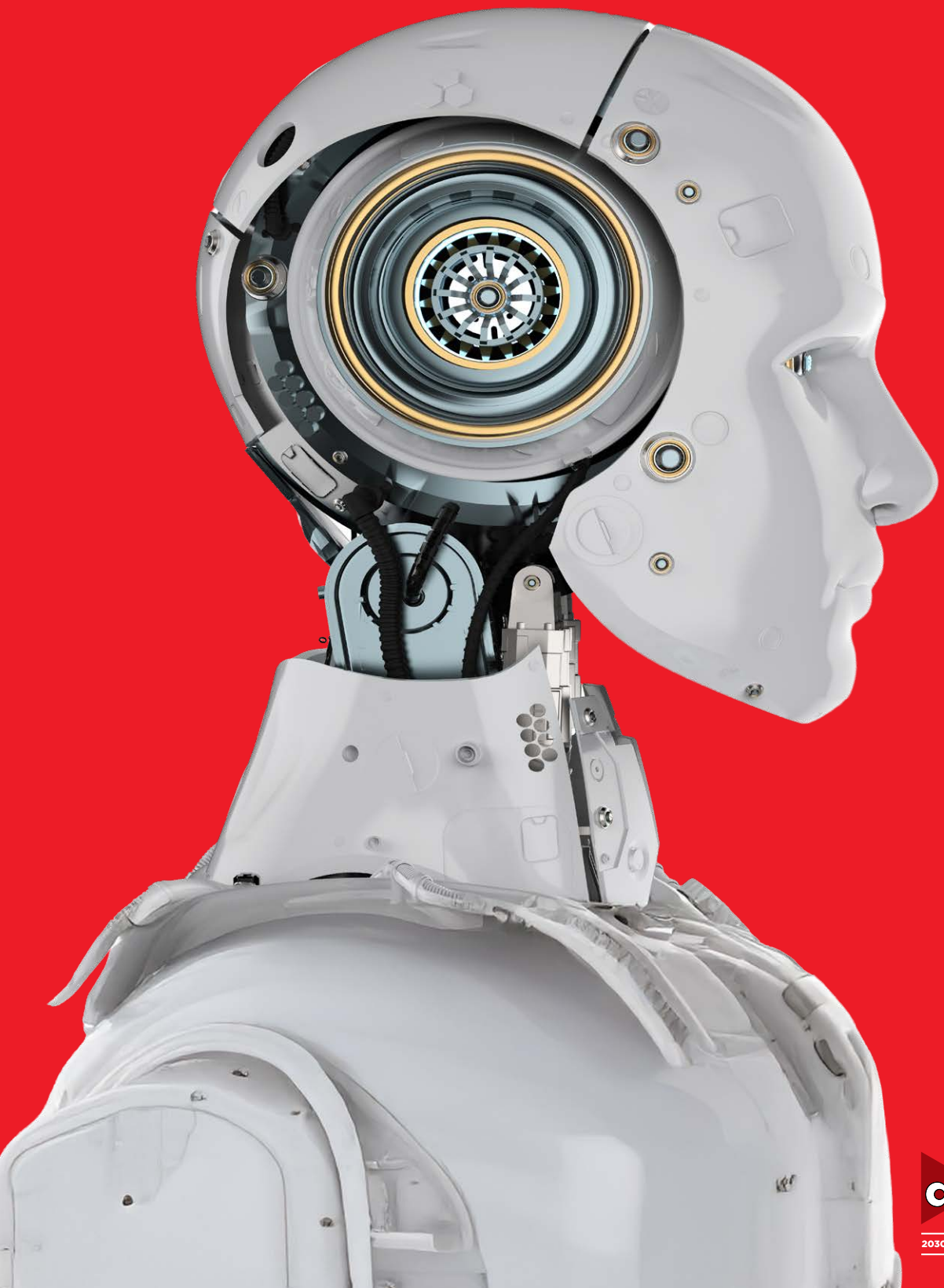
e) Verificação de idade:

Para atender a obrigações regulatórias, especialmente aquelas previstas no ECA Digital, será necessária a adoção de mecanismos de verificação de idade – por ex mecanismos que permitam confirmar a idade do titular e possibilitem a observância das regras aplicáveis ao tratamento de dados pessoais de crianças.

Tais mecanismos devem ser implementados de forma proporcional ao risco, priorizando abordagens que minimizem a coleta adicional de dados pessoais. Além disso, é importante considerar que o ECA Digital proíbe a utilização de dados pessoais coletados para fins de verificação de idade para qualquer outra finalidade.

33 https://www.asa.org.uk/static/44dc1935-0766-4378-91171e6954ae560a/Age-restricted-ads-online-targeting-guidance.pdf

CAPÍTULO II
Inteligência Artificial no Marketing



1. IA “tradicional” x IA generativa no marketing

De forma ampla, inteligência artificial (IA) pode ser entendida como um conjunto de técnicas e modelos computacionais projetados para, a partir de dados e outros insumos, identificar padrões, estimar probabilidades, gerar recomendações, classificar informações ou apoiar decisões, de acordo com objetivos e parâmetros definidos.

No marketing e na publicidade, modelos de IA já são usados há anos, por exemplo, para segmentação de audiência, personalização de anúncios, previsão de comportamento do consumidor, recomendações, otimização de mídia e mensuração de performance. Muitas vezes, esses modelos estão integrados ou “embutidos” em plataformas e ferramentas e operam a partir da leitura de dados de uso, telemetria, sinais derivados e métricas de performance (como impressões, cliques, tempo de permanência, eventos de conversão, frequência, *viewability*, contexto do anúncio e resultados agregados) para ajustar continuamente decisões como entrega, lances e priorização de criativos.

A IA generativa, por sua vez, constitui uma subcategoria voltada à criação de conteúdo original a partir de padrões aprendidos em grandes volumes de dados. a IA generativa produz texto, imagens, vídeos, áudio ou código; pode operar em formato conversacional; ajusta suas respostas conforme contexto e instruções recebidas (*prompts*); e permite interação dinâmica com usuários.

2. Onde a IA entra na cadeia publicitária

A IA está profundamente integrada em todas as etapas da jornada de marketing, transformando a maneira como os anúncios são concebidos, criados, direcionados e entregues. Sua aplicação não se limita a uma única função, mas abrange todo o fluxo de trabalho, desde o planejamento estratégico até a mensuração de resultados. Ela pode estar visível (quando uma equipe usa uma ferramenta generativa para criar peças) ou invisível / “embutida” (quando plataformas aplicam modelos para ranquear conteúdos, otimizar lances, distribuir anúncios e medir resultados).

Isso cria oportunidade de ganho de produtividade e qualidade, mas também eleva risco jurídico, reputacional e operacional, sobretudo quando o uso ocorre em escala e com baixa rastreabilidade[34]. Por isso, o ponto de partida deste Guia de Boas Práticas é mapear onde a IA aparece, quem controla cada decisão e quais evidências precisam existir para sustentar conformidade e confiança.

Planejamento, Insights e Inovação

- **Análise Preditiva:** Utiliza algoritmos de machine learning para prever o comportamento do consumidor e o desempenho de campanhas antes mesmo do lançamento

34 https://info.aana.com.au/hubfs/WFA-AANA%20Primer_Opportunities%20%26%20challenges%20in%20generative%20AI.pdf; https://iabbrasil.com.br/wp-content/uploads/2024/11/IAB_Guia_de_Uso_da_Inteligencia_Artificial_na_Publicidade_Digital_nov24_AF.pdf

- **Geração de Insights:** Analisa volumes massivos de dados estruturados e não estruturados para identificar padrões, tendências e novas oportunidades de negócio
- **Inovação de Produto:** Emprega insights gerados por IA para otimizar o desenvolvimento de produtos e experiências baseadas nas necessidades reais dos usuários

Criação e Produção de Conteúdo

- **Geração Multimodal:** Criação de textos *(copy)*, imagens fotorealistas, vídeos sem câmeras, áudios e trilhas sonoras a partir de comandos *(prompts)*
- **Conteúdo Dinâmico:** Ferramentas de IA geram variações de anúncios em tempo real, adaptando mensagens e ofertas às preferências individuais de cada consumidor
- **Ideação Criativa:** Apoio no processo de brainstorming e concepção de campanhas, permitindo explorar horizontes inexplorados de criatividade

Mídia, Segmentação e Entrega

- **Publicidade Programática:** Algoritmos automatizam a compra e venda de inventário publicitário, otimizando lances e alocação de orçamento em milissegundos
- **Perfilamento e Microsegmentação:** Utiliza deep learning para construir perfis comportamentais complexos, permitindo um direcionamento hyper-específico baseado em hábitos e preferências
- **Otimização de Campanhas:** Emprega aprendizado por reforço para melhorar continuamente o desempenho dos anúncios, ajustando parâmetros de veiculação em tempo real

Ativação e Relacionamento com o Cliente

- ***Chatbots* e Assistentes Virtuais:** O uso de Processamento de Linguagem Natural (NLP) permite atendimentos imediatos, personalizados e capazes de emular empatia humana
- **Personalização da Experiência (CX):** Analisa dados de compras passadas e navegação para oferecer recomendações de produtos e serviços sob medida

Mensuração e Resultados

- **Atribuição e ROI:** Ajuda a identificar quais canais e mensagens oferecem o melhor retorno sobre o investimento, permitindo uma tomada de decisão baseada em dados reais
- **Monitoramento de Marca *(Brand Safety):*** Ferramentas de IA realizam auditorias em tempo real para garantir que os anúncios não sejam exibidos ao lado de conteúdos inadequados ou fraudulentos

2.1 Atores da cadeia: quem faz o que e onde a IA costuma entrar

Para facilitar o entendimento, é possível agregar a cadeia publicitária em quatro núcleos e, para fins de governança, importa entender onde há decisão automatizada, quem controla o processo e quem mantém evidências[35].

35 https://aba.com.br/wp-content/uploads/2025/10/ChecklistIADIGITAL.pdf; https://iabbrasil.com.br/wp-content/uploads/2024/11/IAB_Guia_de_Uso_da_Inteligencia_Artificial_na_Publicidade_Digital_nov24_AF.pdf; https://drive.google.com/file/d/1_F4eGbP_HixRSks2SXNZS_LUR0MrZ0Fb/view

CADEIA PUBLICITÁRIA COM IA: ONDE APARECE

Ator	Presença da IA	Decisões
Anunciante	Aprovação de criação gerada por IA; personalização; atendimento; mensuração	Define diretrizes, aprova peça e "vai ao ar"
Agência	Geração de peças, variações, storyboards; automações; uso de APIs/modelos	Seleciona ferramentas, opera *prompts*, compõe materiais
Plataformas/ Veículos	Recomendação/ ranking; segmentação; otimização de entrega	Define parâmetros do sistema; anunciante define objetivo e público
Fornecedores de IA	Ferramentas de geração e edição; modelos de propósito geral	Fornecedor: define arquitetura; cliente: uso e insumos
Fornecedores de produção	Bancos de imagem / voz; estúdios; freelancers	Podem inserir inputs de terceiros
Consumidor/ público	*Chatbots* e experiências *IA-driven;* conteúdo sintético	Podem interagir com a IA induzir erro/enganar

2.2. IA como ferramenta, parceiro criativo e risco jurídico

Uma forma prática de entender o impacto da IA na cadeia é distinguir três modos de uso:

(i) IA como ferramenta ("copiloto")

A IA atua como apoio operacional: acelera tarefas, sugere alternativas e automatiza etapas repetitivas. Humano tende a manter o controle direto do resultado, mas ainda assim é essencial garantir revisão e rastreabilidade, porque velocidade e escala amplificam erros e violações.

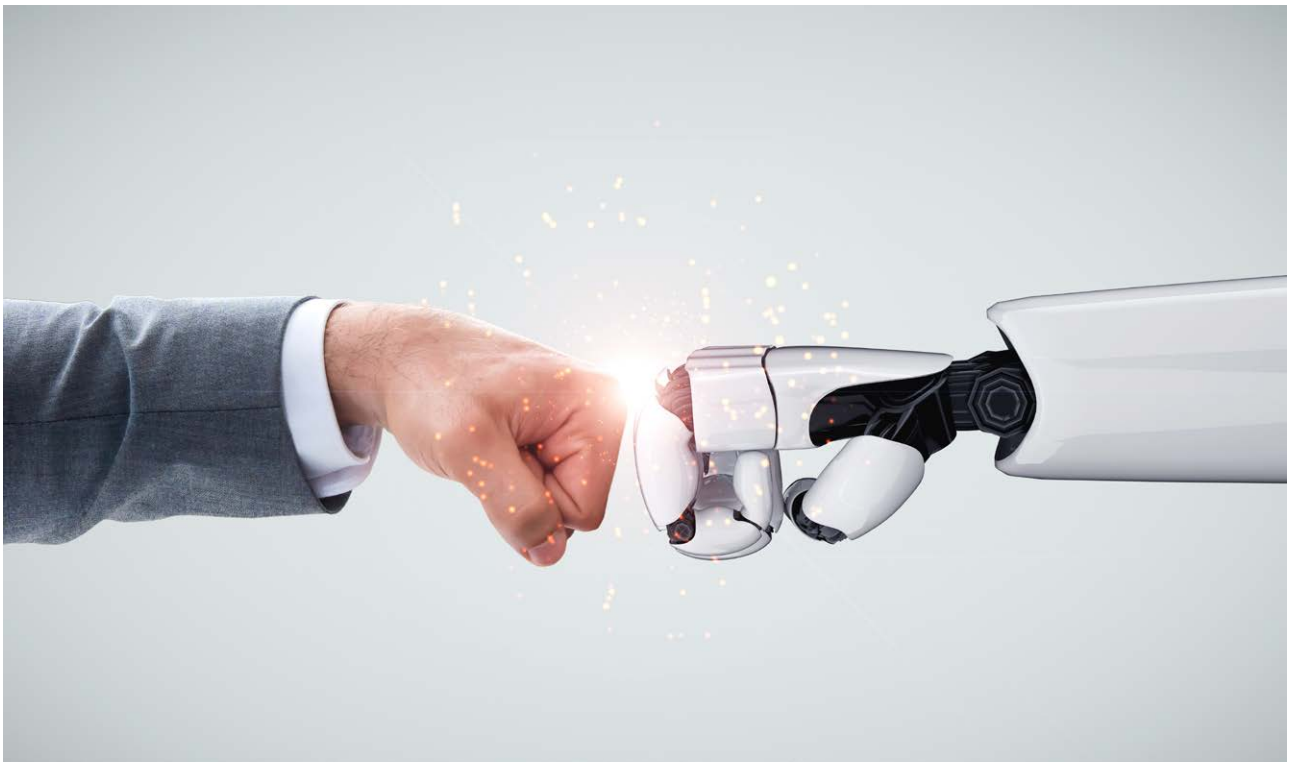
(ii) IA como parceiro criativo ("co-criação")

A IA passa a influenciar escolhas criativas, gerando imagens, roteiros, vozes, cenas e variações em escala. Esse modo traz ganhos de produtividade e novas possibilidades de expressão, mas aumenta riscos de conteúdo sintético enganoso, violação de direitos autorais, e uso não autorizado de imagem/voz. Por isso, a governança precisa tratar output como conteúdo publicitário sujeito a padrões de veracidade, responsabilidade e diligência.

(iii) IA como risco jurídico "embutido"

A IA opera "por trás", no "backstage", em plataformas e fornecedores, em ranking, recomendação, segmentação, *bidding*, atribuição e moderação. O risco aqui é duplo: opacidade (dificuldade de explicar por que uma decisão foi tomada) e impacto indireto ao consumidor (ex.: segmentação inadequada, discriminação, exposição a conteúdo manipulado, pressão persuasiva)[36].

36 https://drive.google.com/file/d/1_F4eGbP_HixRSks2SXNZS_LUR0MrZ0Fb/view; https://iabbrasil.com.br/wp-content/uploads/2024/11/IAB_Guia_de_Uso_da_Inteligencia_Artificial_na_Publicidade_Digital_nov24_AF.pdf



2.3 Responsabilidade na cadeia

Quando a inteligência artificial passa a integrar a cadeia criativa e operacional do marketing, ela impacta diretamente dimensões já reguladas e sensíveis da atividade publicitária, como veracidade das informações, vedação à publicidade enganosa ou abusiva, transparência, proteção do consumidor, direitos autorais e de personalidade, não discriminação e segurança da informação.

A utilização de IA não cria zona de exceção normativa. As obrigações legais e autorregulatórias permanecem integralmente aplicáveis, inclusive quando se trata de:

- Alegações comerciais relacionadas ao uso de IA (*claims* tecnológicos)
- Conteúdos sintéticos que possam gerar confusão sobre autenticidade, sob pena de caracterizar engano ou abuso indevido da confiança do consumidor[37]

Além disso, quanto mais a IA se torna conversacional (assistentes, *chatbots*, avatares) e quanto mais "personaliza" decisões (segmentação/otimização)maior tende a ser o risco de confusão material, indução indevida de confiança e impactos relevantes ao consumidor. Nesses casos, transparência, *disclosure* e definição clara de responsabilidades deixam de ser cuidados acessórios. Por isso, é importante é tratar transparência e *disclosure* como parte do desenho da campanha, sem incorrer em *label fatigue*[38].

37 Nesse sentido: https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; https://www.asa.org.uk/news/generative-ai-advertising-decoding-ai-regulation.html; https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes; https://wp.nyu.edu/compliance_enforcement/2024/04/17/the-luring-test-ai-and-the-engineering-of-consumer-rust/

38 https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/

LABEL FATIGUE e quando incluir *DISCLOSURE*

Para reduzir *label fatigue* sem perder confiança, a abordagem recomendada é baseada em materialidade. A realização de *disclosure* é:

- mais importante quando a IA pode alterar a percepção do consumidor sobre autenticidade, identidade ou representação (ex.: pessoa/voz/performer sintético, cena sintética realista, depoimentos/experiências simuladas), influenciando no entendimento do produto ou serviço ofertado e até mesmo impactando na decisão de compra e/ou escolha
- menos relevante quando a IA atua como ferramenta de bastidor sem risco material de engano

Diante da ausência de consenso regulatório e autorregulatório sobre uma regra geral de rotulagem de conteúdos gerados ou apoiados por IA, a decisão sobre *disclosure* deve permanecer vinculada à materialidade do risco de engano, confusão ou indução indevida do consumidor.

⚠ PONTO DE ATENÇÃO!

À medida que IA generativa e conteúdo sintético ganham escala, cresce a demanda por transparência consistente e critérios de divulgação (“quando” e “como” informar). Contudo, transparência e rotulagem podem fortalecer confiança, mas não substituem conformidade (nem “blindam” a campanha contra questionamentos de enganosidade, abuso ou práticas desleais)[39].

O QUE SE ESPERA DE CADA AGENTE DA CADEIA?

Agente	O que se espera	Onde termina a responsabilidade	Como endereçar “para dentro” (contrato/processo)
Anunciante (marca)	Definir limites e níveis de risco; aprovar uso de IA e ferramentas; exigir revisão humana antes do uso dos resultados gerados; definir quando haverá *disclosure*; ter plano de correção/remoção e resposta a incidentes, prever proibição de uso de informações do Anunciante para treinamento do sistema de IA, definir em contrato com a agência toda a regulação de Propriedade Intelectual dos entregáveis gerados por IA	Continua sendo o principal responsável perante o público por peça/claim/ *disclosure*	Políticas internas; estruturação de contratos robustos com as Agências; aprovação prévia de ferramentas; fluxo de revisão e aprovação; exigências de rastreabilidade e SLAs

39 https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/; https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes; https://www.asa.org.uk/news/generative-ai-advertising-decoding-ai-regulation.html

Agente	O que se espera	Onde termina a responsabilidade	Como endereçar "para dentro" (contrato/processo)
Agência	Informar e documentar uso de IA; usar apenas ferramentas aprovadas; manter rastreabilidade (data, *prompt*, *log*, versão do modelo); checar fatos e riscos legais; obter/confirmar direitos; notificar terceirização, caso seja contratualmente permitida	Pode compartilhar responsabilidade quando cria/controla conteúdo em nome do Anunciante, mas não substitui a responsabilidade final perante o público/consumidor	Obrigações de notificação prévia, documentação, revisão humana, rastreabilidade e aprovação prévia pelo anunciante antes da veiculação e cláusulas de responsabilidade por *inputs* e *outputs*, incluindo declarações e garantias sobre direitos de terceiros, obrigação de indenização e responsabilização por outputs incorretos, prejudiciais ou em desconformidade
Fornecedores	Transparência mínima de funcionamento e limitações; segurança e confidencialidade; opções claras sobre retenção/treinamento; suporte a *logs* e auditoria; notificação rápida de incidentes	Normalmente não tem relação com o consumidor, mas podem gerar dano operacional e jurídico; ainda assim, a publicidade segue imputável ao Anunciante/Agência	SLAs, obrigação de notificar incidentes, direito de auditar/ avaliar controles, subcontratados com mesmos padrões
Plataformas (Veículos)	Enforcement das políticas do ecossistema; mecanismos de rotulagem quando disponíveis; possibilidade de rejeição/*flag* de anúncios	Não assumem a *accountability* do Anunciante; labels aplicados pela plataforma podem complementar, não substituir	Preferir *disclosure* integrada na peça/material publicitário; ainda que o label seja da plataforma, Anunciante continua responsável por garantir adequação do *disclosure*

CONCLUSÃO

A responsabilidade principal por decidir se deve haver divulgação/rotulagem de uso de IA (e como essa informação será apresentada) costuma recair sobre o Anunciante (marca) ou sobre a Agência que cria e controla o conteúdo, atuando em nome do Anunciante. Já as plataformas aplicam suas próprias regras e mecanismos de moderação/rotulagem dentro do ambiente em que o anúncio circula, mas isso não transfere nem substitui a responsabilidade do anunciante pela conformidade e pela transparência da comunicação.

3. Casos de uso reais de IA no marketing

Na cadeia publicitária, a IA aparece tanto em tarefas "de bastidor" (análises, automações, otimização) quanto em entregas que impactam diretamente o público (peças, *claims*, atendimento).

A IA (especialmente a generativa) já é muito usada por profissionais para encurtar ciclos de produção, apoiar a criação e automatizar tarefas. Ela pode apoiar desde a geração de peças e variações até a criação de planos de mídia, extração de insights e respostas em atendimento. Ao mesmo tempo, a qualidade pode ser variável e a revisão humana é imprescindível para garantir adequação e evitar riscos.

Regra de bolso: tudo que for para o público (ou que influencie decisões de marketing relevantes) deve ter **revisão humana e rastreabilidade** (ex.: *prompt/log*/modelo/versão/quem aprovou).

VISÃO GERAL: ONDE A IA COSTUMA ENTRAR (DA CRIAÇÃO AO PÓS-CAMPANHA)

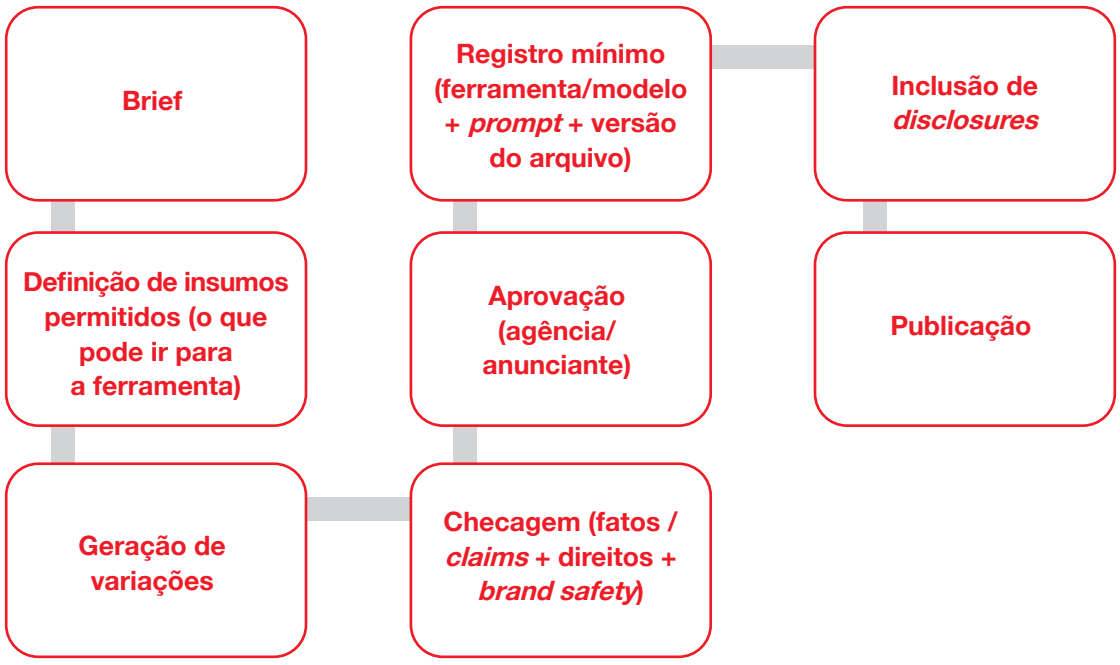
Etapa	O que a IA costuma fazer	Exemplos práticos	Riscos típicos	Salvaguardas rápidas
Estratégia e briefing	Organizar *inputs,* mapear público e hipóteses	Sumarizar insights; sugerir mensagens; priorizar testes	Vieses; "alucinações"; decisões sem base	Revisão humana e validação de fontes *(do's & don'ts)*
Produção de conteúdo	Acelerar criação e variações	Textos, imagens, roteiros, versões A/B	Propriedade Intelectual, direitos de personalidade; conteúdo enganoso	Revisão humana; checagens; rastreabilidade
Mídia e otimização	Apoiar segmentação/ compra e ajustes	Pacing; lances; alocação por performance	Discriminação; opacidade	Auditoria e transparência; documentação
Mensuração e atribuição	Modelar impacto e estimar contribuição	Modelos, leitura de sinais, dashboards	Confusão entre correlação e causalidade ("causa efeito") e *overclaim*	Testes, validação, governança e trilha de decisão
Atendimento e *research*	Automatizar interações e *insights*	*Chatbots*; resumo de *feedback;* pesquisa, personas sintéticas para *insights*	Respostas erradas; *prompt injection* (tentativa de manipulação do modelo)	Supervisão; testes; mecanismos de resiliência

3.1 Criação de conteúdo (texto, imagem, vídeo, áudio e variações)

IA generativa e ferramentas correlatas são usadas para ideação, produção e adaptação de peças com mais velocidade e escala (*headlines, slogans, posts*, descrições de produto, *voiceovers*, roteiros e variações criativas). No contexto de publicidade digital, o uso também se estende a imagens de referência (*moodboards*, *storyboards*), imagens para campanhas, ilustrações, fotorrealismo e edição/ajustes (remoção/adição de elementos, mudança de fundo, *generative fill).*

O QUE FAZER	O QUE NÃO FAZER
✓ Garanta revisão humana antes de publicar, incluindo aprovação prévia do anunciante para conteúdos destinados à veiculação, especialmente para fatos, comparações, promessas, temas sensíveis, saúde/finanças, direitos de PI e uso de imagem/voz ✓ Capacite a equipe e estabeleça diretrizes internas de uso seguro ✓ Exigir rastreabilidade (*prompt*/*log*/modelo/versão) e registro de aprovações ✓ Tenha um check de direitos (Direitos autorais, Propriedade Intelectual, uso de imagem e voz) e registre evidências de autorização quando aplicável	✗ Publicar ou reaproveitar output sem revisão humana ✗ Deixar de treinar quem usa IA no dia a dia ✗ Produzir conteúdo sem trilha mínima (sem *prompt*/*log*/versão) ✗ Não use IA para criar "provas" ou "depoimentos" simulados que possam induzir o público a erro sobre autenticidade (*deepfake*/encenação) sem salvaguardas e transparência quando material

MODELO DE FLUXO OPERACIONAL



Exemplo de *prompt* com "freios"

"Crie 10 variações de título e descrição para anúncio de [produto], mantendo: (i) tom [X], (ii) sem promessas absolutas ('garantido', '100%'), (iii) sem comparações com concorrentes, (iv) sem menções a atributos sensíveis, (v) com 2 opções mais conservadoras para compliance. Ao final, liste quais afirmações exigem checagem factual."

3.2. Mídia e otimização (compra, segmentação, *bidding* e decisão em tempo real)

Em mídia e otimização, a IA é usada para automatizar decisões que antes eram operacionais e manuais, como *bidding* (lances), seleção de inventário, segmentação, pacing de orçamento e otimização de criativos. Esses sistemas processam grandes volumes de sinais (contexto do usuário, comportamento agregado, performance histórica, ambiente do anúncio, tempo/dispositivo etc.) e fazem ajustes dinâmicos para atingir objetivos definidos (alcance, CPA - Custo por Aquisição, ROAS - Retorno sobre Gasto com Anúncios, *leads*, vendas).

Na prática, a IA funciona como um piloto automático que toma microdecisões a cada impressão: qual anúncio exibir, para quem, quando, em qual local e a que preço. Isso permite ganho de eficiência e escala, mas também cria um ponto de atenção na medida em que as decisões ficam menos intuitivas e mais difíceis de explicar, pois a otimização se dá por modelos que ajustam entrega continuamente.

Assim, o risco não está apenas na criação, mas também em como a campanha é distribuída e refinada, incluindo efeitos sobre exclusões, públicos vulneráveis, brand safety e eventuais vieses de segmentação.

O QUE FAZER	O QUE NÃO FAZER
✓ Defina *guardrails* antes de ligar a automação: objetivo de campanha, KPIs de qualidade (não só volume), orçamento, janela de otimização, limites de frequência, exclusões e critérios de brand safety	✗ Não trate a otimização automatizada como "piloto automático sem dono": automação sem supervisão e sem evidências aumenta risco de entrega inadequada, vieses e exposição reputacional
✓ Estabeleça limites claros para segmentação e exclusão (inclusive para evitar impacto em crianças e grupos vulneráveis, quando aplicável – por exemplo produtos eróticos em páginas de conteúdo infantil), e revise periodicamente se a entrega está respeitando as regras definidas	✗ Não otimize apenas por métricas "fáceis" (clique, *view*, *lead* bruto) sem indicadores de qualidade e validação; isso tende a induzir decisões que maximizam volume, mas degradam valor real e podem incentivar práticas questionáveis
✓ Garanta supervisão humana em rotina: crie uma cadência mínima de monitoramento (ex.: diário no início e após grandes ajustes; semanal em operação estabilizada) para checar anomalias, deriva de performance e eventuais efeitos indesejados da otimização	✗ Não permita mudanças contínuas sem registro ("ajustes invisíveis") — isso compromete explicabilidade, auditoria e capacidade de corrigir rota quando algo dá errado
✓ Registre as decisões e mudanças relevantes: alterações em objetivo, públicos, exclusões, criativos, lances, orçamento, janela de atribuição e configurações de automação. Isso é essencial para explicar resultados e sustentar diligência	✗ Não use segmentações/expansões automáticas sem limites quando houver risco de atingir públicos indevidos ou sensíveis; "ampliar audiência" sem *guardrails* aumenta risco de erro de contexto e exposição desnecessária
✓ Tenha trilha de responsabilidade: quem aprovou a estratégia de mídia, quem executou mudanças, quem revisou e qual foi o racional, especialmente quando agência opera a conta e ativa automações	✗ Não dependa exclusivamente de rótulos/ regras da plataforma como substituto de governança: as regras do ecossistema ajudam, mas não eliminam a responsabilidade do anunciante/agência sobre como a campanha é configurada e otimizada
✓ Inclua plano de contingência (fallback): se a automação começar a gerar resultados anômalos, defina gatilhos de pausa, reversão para configurações anteriores e escalonamento rápido	✗ Não ignore sinais de anomalia (picos súbitos, queda brusca de CPA com piora de qualidade, mudanças relevantes sem causa aparente, concentração em inventário suspeito). Em mídia automatizada, essas "anomalias" são precisamente o tipo de risco que exige pausa e revisão

3.3. Mensuração e atribuição

Mensuração e atribuição, no contexto de marketing, reúnem metodologias para quantificar impacto de iniciativas de marketing e atribuir parte do resultado (vendas, *leads*, tráfego qualificado) aos diferentes canais e ações. Com o avanço da IA, esse trabalho passou a combinar modelos tradicionais e técnicas de machine learning para integrar múltiplas fontes (mídia, CRM, site/app, varejo, contexto), reduzir ruído e produzir leituras mais acionáveis, como estimativas de contribuição por canal, previsões de performance e recomendações de realocação de orçamento.

A IA entra, em geral, para: (i) organizar grandes volumes de sinais, (ii) detectar padrões (ex.: sazonalidade, resposta a preço/promoção), (iii) prever desempenho e (iv) gerar insights acionáveis — desde que haja validação, governança e documentação adequadas. O ponto-chave é que atribuição não é "conta exata", mas uma inferência baseada em dados e hipóteses, por isso exige transparência de método, validação e documentação.

O QUE FAZER	O QUE NÃO FAZER
✓ Trate "insight de IA" como hipótese testável, validada com contexto e método, não como verdade automática ✓ Documente metodologia, limitações e mudanças (ex.: janela, variáveis, supostos) para permitir auditoria e comparação histórica	✗ Não confunda correlação (associações estatísticas encontradas nos dados – ex.: "Usuários expostos ao anúncio converteram mais") com causalidade, ao justificar decisões de orçamento, segmentação ou *claims* de performance, pois o aumento reportado pode ter vindo de outros fatores, que não aqueles correlacionados pela IA ✗ Não "otimize a mensuração" para parecer melhor: escolher métricas fáceis (ex.: clique) ou eventos frágeis para inflar performance tende a distorcer decisões e pode virar *claim* enganoso

3.4 Atendimento e pesquisa (*chatbots*, agentes e pesquisa de mercado)

A IA pode gerar respostas imediatas e personalizadas no atendimento, inclusive em múltiplos idiomas, e em alguns casos emula características humanas como empatia. Em paralelo, ganha espaço na pesquisa: síntese de informações, leitura de grandes volumes de dados e apoio a insights.

O QUE FAZER	O QUE NÃO FAZER
✓ Deixe claro o papel do assistente: comunique que se trata de uma solução automatizada quando isso for relevante para evitar confusão material, especialmente em atendimentos mais "humanizados" (chat/voz/avatar) e em interações prolongadas ✓ Defina uma "base de verdade" para respostas: limite o que o agente pode afirmar a partir de fontes oficiais (políticas de troca, condições, preços, prazos, termos), e atualize essas fontes com governança (owner + versão) para reduzir resposta desatualizada	✗ Não desenhe chatbot/assistente para **induzir confiança indevida** ("sou especialista", "garanto", "é 100% seguro") — risco de prática enganosa e de dano reputacional ✗ **Não deixe o assistente "inventar"** (alucinação) para responder rápido: respostas erradas em atendimento viram promessa indevida e dano reputacional ✗ **Não apresente chatbot/assistente como humano** ou como "autoridade" quando não é; isso aumenta risco de indução indevida de confiança e frustração do consumidor[40]

40 https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust?utm_source=govdelivery

O QUE FAZER	O QUE NÃO FAZER
✅ Implemente escalonamento para humano (*handoff*) com gatilhos objetivos: crie regras claras para encaminhar ao atendimento humano (ex.: reclamações graves, cancelamento, cobrança, disputa, fraude, dados pessoais sensíveis, crianças/vulneráveis, temas regulados) e registre o motivo do *handoff* ✅ Use *guardrails* de conteúdo e tom: configure limites para evitar promessas, garantias indevidas, linguagem agressiva ou persuasão excessiva — e para impedir recomendações incompatíveis com política comercial ou com deveres de transparência	❌ **Não permita que o bot faça afirmações factuais sensíveis sem base definida** (preço, prazo, cobertura, condições contratuais, políticas), sobretudo quando a resposta pode ser interpretada como compromisso da empresa ❌ **Não use o atendimento automatizado para empurrar decisões do consumidor de forma manipulativa** (pressão, urgência artificial, exploração de vulnerabilidades) ou para *nudge* oculto

4. Princípios que devem regrar a IA Responsável e Ética no Marketing

Os princípios abaixo funcionam como critérios para decidir quando usar IA, como desenhar campanhas e quais controles exigir ao longo da cadeia (Anunciante, Agência, Plataformas e Fornecedores). Eles refletem convergências entre materiais setoriais brasileiros e internacionais, com ênfase em proteção do consumidor, integridade da comunicação comercial, mitigação de riscos e governança.

4.1. Finalidade legítima e alinhamento com o negócio

O uso de IA deve estar conectado a um objetivo claro do negócio, com escopo e limites definidos (o que será automatizado, o que exige criação humana e o que é proibido). A finalidade deve ser compatível com o contexto da campanha e com as expectativas do público.

O uso de IA deve começar pela pergunta **“para quê?”** buscando avaliar qual objetivo legítimo ela ajuda a alcançar (eficiência, escala, qualidade, personalização responsável, *insights),* e quais limites são necessários para evitar que a tecnologia crie risco desproporcional.

Materiais internacionais voltados a anunciantes reforçam a lógica de: definir previamente onde a IA pode ser aplicada, quais casos devem ser evitados e quais controles mínimos acompanham cada uso[41]. Finalidade legítima também significa evitar usos “decorativos” (ex.: *AI washing)* e concentrar esforços onde a IA melhora o processo sem comprometer veracidade, transparência e confiança[42].

41 https://info.aana.com.au/hubfs/WFA-AANA%20Primer_Opportunities%20&%20challenges%20in%20generative%20AI.pdf
42 https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

4.2. Transparência e explicabilidade proporcional ao risco

Transparência e explicabilidade sustentam a confiança no uso de IA no marketing, pois permitem que consumidores, clientes e parceiros entendam quando há automação relevante, façam escolhas informadas e, quando necessário, questionem ou contestem decisões e comunicações. Embora complementares, esses conceitos não se confundem: a transparência se relaciona ao dever de informar com clareza; a explicabilidade, à possibilidade de compreender e avaliar, em medida adequada, como a IA foi utilizada e quais fatores relevantes influenciaram o resultado.

No caso da **transparência**, é útil distinguir duas dimensões complementares:

(i) Transparência sobre tratamento e automação: é comunicar, de forma clara e compreensível, se, quando e em que medida a IA, a automação ou o tratamento de dados foram utilizados, sempre que essa informação for relevante para a compreensão do público, do cliente ou de parceiros na cadeia. Essa frente abrange, conforme o contexto, informações sobre tratamento de dados pessoais, existência de automação relevante, natureza da interação automatizada e demais elementos cuja omissão possa comprometer direitos do titular ou induzir o consumidor em erro. Nessa dimensão, ganham especial relevo as obrigações de transparência e informação previstas na LGPD, especialmente quando houver tratamento de dados pessoais, perfilamento ou decisões apoiadas em automação. Quando o uso de IA influenciar de modo material a formação, a personalização, a entrega ou a avaliação de conteúdos, ofertas ou interações, essa transparência deve ser acompanhada de explicabilidade proporcional ao risco e ao impacto do caso concreto

(ii) Transparência sobre a natureza da comunicação: refere-se à clareza, honestidade e inteligibilidade da mensagem na experiência concreta do público. Busca evitar confusão material ou indução do consumidor em erro quanto à autenticidade, autoria, identidade, endosso humano, caráter publicitário ou natureza sintética de conteúdos e interações. Essa dimensão se torna particularmente sensível quando o uso de IA puder alterar de forma relevante a percepção do público sobre a origem, a mediação tecnológica ou a apresentação da comunicação. Nesse contexto, destacam-se os deveres de clareza, não enganosidade e não indução do consumidor em erro, nos termos do CDC, sem prejuízo da incidência de outros parâmetros legais e autorregulamentação aplicáveis, tal como o CBAP

Nessa primeira dimensão, a **explicabilidade** não significa “abrir o código” ou revelar segredos de modelo. Significa assegurar, quando necessário, uma explicação suficiente e proporcional ao risco sobre aspectos relevantes do uso da IA, como: que tipo de automação ocorreu, para qual finalidade; quais dados/insumos foram usados em nível adequado, quais limitações são conhecidas (ex.: possibilidade de erro/alucinação, vieses, dependência de contexto), e quais controles foram aplicados (ex.: revisão humana, checagem de fatos, filtros, auditorias).

No campo publicitário, esses princípios são especialmente importantes porque a IA pode simular autoria humana, gerar conteúdo sintético realista e personalizar interações em escala, o que aumenta o risco de confusão material e de indução a erro se não houver clareza suficiente sobre o uso da tecnologia[43].

A base é a mesma da autorregulamentação publicitária constante no Código do CONAR: comunicações devem ser honestas, verificáveis e não enganosas. Nesse contexto, transparência e explicabilidade funcionam como instrumentos para preservar confiança e *accountability*, sem substituir os demais deveres de conformidade (ex.: veracidade de *claims*, proteção do consumidor e não discriminação).

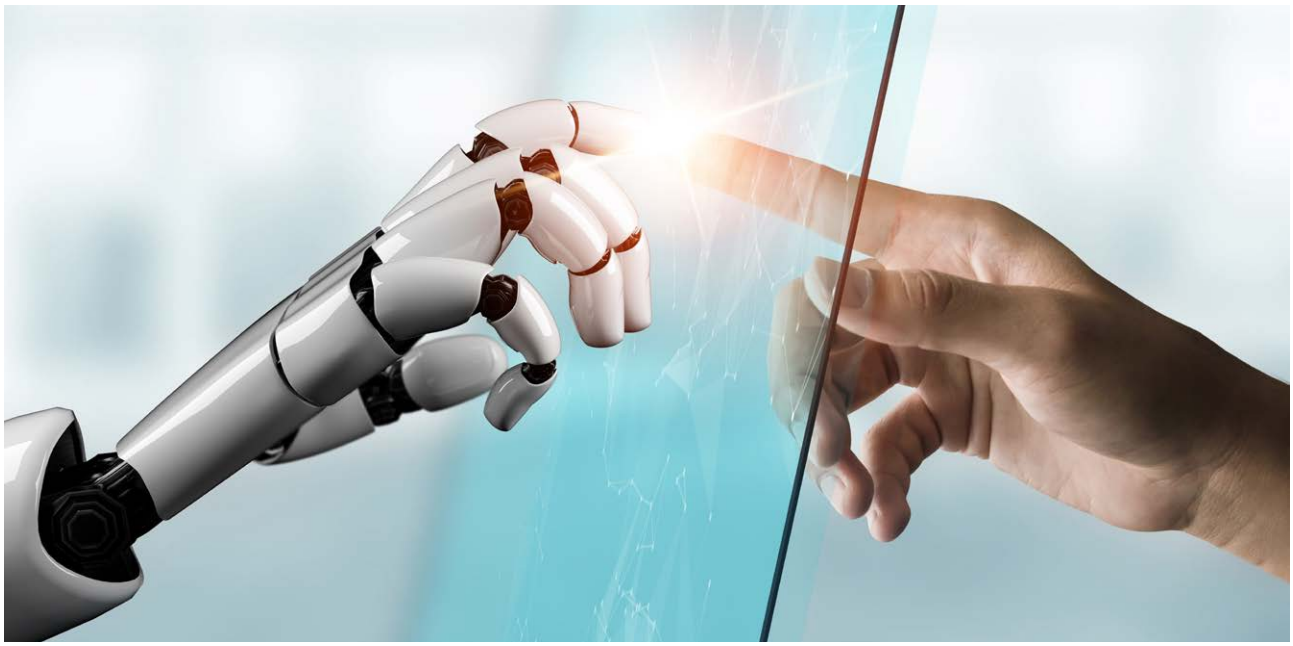
4.3. Centralidade e supervisão humana

A IA acelera fluxos, mas não substitui a responsabilidade humana, sobretudo quando o output pode impactar o consumidor (ex.: *claims*, recomendações, atendimento) ou quando a automação influencia ou toma decisões relevantes (segmentação, otimização, atribuição).

Princípios setoriais para IA generativa na publicidade enfatizam que deve haver dono humano, pontos de aprovação e mecanismos que possibilitem a correção antes e depois da publicação.

A supervisão humana é o que transforma IA de ferramenta "eficiente" em ferramenta "confiável", incluindo conforme o caso: checagem de fatos/*claims*, revisão de linguagem, adequação a públicos sensíveis, validação de direitos autorais e de imagem e revisão de decisões automatizadas de maior impacto.

A centralidade humana, porém, não exige a mesma intensidade de intervenção em todos os usos, devendo ser calibrada de forma proporcional ao risco, ao impacto potencial e ao grau de autonomia do sistema.



43 https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/

É importante distinguir, nesse contexto, dois cenários:

(i) IA como ferramenta de apoio: quando a IA é utilizada para brainstorming, organização de insumos, geração de rascunhos, variações criativas, sumarização, apoio analítico ou recomendação de caminhos, sem produzir por si só decisão final com efeito relevante para o titular ou consumidor. Nesses casos, a supervisão humana deve existir, mas pode ser organizada por meio de revisão por amostragem, aprovação por etapa, *guardrails*, checklists e monitoramento periódico, sem exigir revisão humana contínua ou individualizada de cada interação ou output de baixo risco

(i) IA em decisões automatizadas com efeitos relevantes: quando a automação influencia ou determina, de forma material, a elegibilidade para ofertas ou benefícios, a experiência do titular, a precificação, a priorização de atendimento, ou outras decisões capazes de produzir efeitos jurídicos ou impactos práticos relevantes sobre o titular ou consumidor. Nesses casos, são necessários controles reforçados, maior rastreabilidade, critérios claros de escalonamento, transparência adequada e mecanismos efetivos de contestação e revisão. Adicionalmente, em usos de IA de alto risco, recomenda-se avaliar a elaboração de AIA – Avaliação de Impacto Algorítmico como boa prática de governança, diligência e mitigação de riscos reputacionais e regulatórios, inspirada em referências internacionais e no debate regulatório brasileiro em evolução. Considerando o estado atual da legislação brasileira, a AIA não constitui obrigação legal expressa e geral para usos de IA no marketing, sem prejuízo de obrigações específicas que possam decorrer de regulação setorial, contrato, política de plataforma ou incidência territorial de normas estrangeiras[44]

Em síntese, usos de baixo risco podem ser governados por controles prévios, regras de uso, supervisão periódica e trilha de aprovação; usos de maior risco ou impacto exigem intervenção humana reforçada, com possibilidade real de revisão e correção do resultado e, quando caracterizados como alto risco, podem justificar a avaliação de elaboração de AIA como boa prática de governança e documentação de riscos.

4.4. Não discriminação, equidade e mitigação de vieses

A IA pode reproduzir e amplificar vieses presentes em dados, em padrões de consumo e na própria forma como o modelo "aprendeu" o mundo. No marketing, isso aparece de duas formas:

- no **conteúdo** (representações estereotipadas, linguagem discriminatória)
- na **distribuição do conteúdo** (segmentações e otimizações que excluem indevidamente ou reforçam disparidades)

Nesse contexto, a não discriminação, equidade e mitigação de vieses são um princípio essencial de confiança e responsabilidade. Materiais setoriais e internacionais sobre IA em publicidade tratam diversidade e *fairness* como pilares, com ênfase em revisão humana, testes e *guardrails* antes da veiculação[45].

44 https://vlklaw.com.br/wp-content/uploads/2025/12/VLK_O-Papel-do-DPO_2025.pdf

45 https://icas.global/wp-content/uploads/AI-In-Advertising.pdf; https://www.isba.org.uk/system/files/media/documents/2023-10/AI%20Principles%20-%20Oct%202023.pdf

Um ponto prático importante é que o risco não depende apenas do "modelo" de IA, ele também pode surgir do *brief/prompt,* da seleção de referências criativas, do histórico de performance que alimenta a otimização e das restrições impostas pela própria campanha (ex.: metas de conversão que induzem o sistema a concentrar entrega em perfis mais "baratos" ou "com maior probabilidade de conversão").

Além disso, o uso de IA pode criar "ilusão de neutralidade". *Outputs* convincentes podem parecer objetivos e "baseados em dados", quando na verdade refletem padrões históricos e suposições embutidas.

Para evitar esse efeito, recomenda-se adotar um padrão mínimo de diligência: checklist de estereótipos e linguagem sensível, revisão humana (com diversidade de olhares quando possível), testes controlados e documentação das decisões de mitigação (ex.: ajustes de *prompt*, filtros e critérios de segmentação). Isso aumenta a qualidade dos conteúdos de marketing e reduz riscos regulatórios e reputacionais associados a práticas discriminatórias.

4.5 Segurança, integridade e confiabilidade

A segurança em IA aplicada ao marketing envolve proteger insumos (briefs, prompts, dados, imagens, peças e informações estratégicas), prevenir vazamentos e usos indevidos, reduzir riscos de manipulação (inclusive por terceiros) e garantir que a solução opere com confiabilidade no contexto em que é utilizada. Em marketing, uma falha técnica rapidamente vira falha de experiência do consumidor e risco reputacional; um output incorreto, uma resposta indevida de chatbot ou um conteúdo manipulado pode gerar reclamações, autuações, judicialização e perda de confiança.

Diretrizes setoriais de boas práticas destacam a necessidade de diligência na seleção e contratação de ferramentas, definição de controles de acesso, governança de *logs* (incluindo o que é armazenado e por quanto tempo) e protocolos claros para incidentes e resposta rápida nestes casos.

Além dos riscos clássicos de segurança, a IA traz riscos específicos de integridade informacional: *outputs* podem estar factualmente incorretos (inclusive por "alucinação"), podem misturar fontes e podem soar convincentes mesmo quando errados — o que exige verificação antes de publicar ou de responder diretamente ao consumidor[46].

> Na prática, "confiabilidade" deve ser tratada como um pacote de controles integrados: (i) uso de ferramentas homologadas e com termos adequados para uso comercial; (ii) segurança operacional (perfis de acesso, segregação de ambientes, proteção de dados e de ativos criativos); (iii) validação humana proporcional ao risco (especialmente para *claims*, dados, comparativos, recomendações e atendimento); e (iv) rastreabilidade mínima do que foi gerado e aprovado (ferramenta, versão, responsável e evidências de revisão), para permitir auditoria e correção rápida quando necessário.

46 https://icas.global/wp-content/uploads/AI-In-Advertising.pdf; https://info.aana.com.au/hubfs/WFA-AANA%20Primer_Opportunities%20&%20challenges%20in%20generative%20AI.pdf

4.6. Responsabilidade e prestação de contas *(accountability)*

Accountability na publicidade se traduz na definição de papéis claros entre Anunciante, Agência e Fornecedores para definição de quem responde pelo uso de IA e pela aprovação dos conteúdos, além da preservação de evidências (qual ferramenta/modelo foi usado, quem aprovou, qual versão foi publicada e quais controles foram aplicados).

O Interactive Advertising Bureau - IAB, ao tratar *disclosure* e transparência, reforça que decisões sobre rotulagem e comunicação não podem ser improvisadas, precisam de critério, consistência e registro[47]. Reguladores também têm sinalizado que alegações sobre IA e promessas ao consumidor exigem substanciação e não se beneficiam de "exceção tecnológica"[48].

4.7. Legalidade e conformidade regulatória

O uso de IA no marketing não ocorre em ambiente normativo vazio. O arcabouço jurídico brasileiro já contempla, de forma transversal, os principais riscos associados à automação, personalização, geração de conteúdo e uso intensivo de dados. Na prática, isso significa que a utilização de IA deve observar, de forma cumulativa e integrada: Código de Defesa do Consumidor (CDC); LGPD; Código Brasileiro de Autorregulamentação Publicitária (CONAR); regras de propriedade intelectual, incluindo direitos autorais sobre conteúdos utilizados como insumo ou gerados por IA; direitos da personalidade, incluindo imagem e voz; além dos termos de uso e políticas de plataformas e ferramentas tecnológicas.

Direito do consumidor e regras contra publicidade enganosa/ abusiva	A comunicação comercial continua sujeita a padrões de não enganosidade, clareza de informação, não abusividade e não indução a erro, inclusive quando o conteúdo é gerado ou otimizado por IA. Isso abrange (a) *claims* de produto/serviço, (b) comparativos, (c) promessas de performance, e (d) mensagens que possam explorar vulnerabilidades (especialmente em temas sensíveis). Autoridades têm sinalizado, inclusive, fiscalização e repressão a alegações enganosas envolvendo IA (*AI washing*) e a práticas que induzam confiança indevida do consumidor por meio de interfaces conversacionais[49].
Proteção de dados pessoais (LGPD) no uso de IA	Quando a IA envolve dados pessoais (segmentação, personalização, profiling, mensuração, pesquisa com base em interações ou uso de bases proprietárias) aplicam-se plenamente os princípios e obrigações da LGPD (finalidade, adequação, necessidade/minimização, transparência, segurança, prevenção e responsabilização). Na prática, os pontos críticos costumam estar em: (a) definição de bases legais e finalidades, (b) minimização e governança de bases, (c) gestão de operadores e suboperadores (ferramentas e fornecedores), (d) retenção e uso de *logs*, e (e) medidas de segurança e resposta a incidentes. **Implicação operacional:** sempre que houver dado pessoal no fluxo, é recomendável exigir do fornecedor clareza sobre retenção, uso para treinamento, local de processamento e controles de segurança, além de registrar decisões e medidas adotadas.

47 https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/

48 https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

49 https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes; https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale

Propriedade intelectual (direitos autorais, marcas, licenças e segredos comerciais)	Em contextos de IA generativa, riscos de PI aparecem em duas frentes: **(1) *inputs*** — materiais de terceiros incluídos no *prompt* (textos, imagens, vídeos, layouts, obras, bases, slogans) **(2) *outputs*** — peças geradas que podem reproduzir elementos protegidos, criar similaridade relevante com obras existentes ou incorporar marcas/elementos de terceiros sem autorização. Também é necessário considerar limites contratuais/licenças de ferramentas (o que é permitido gerar e como pode ser usado comercialmente)[50] **Implicação operacional:** para reduzir exposição, convém estabelecer "regras de *clearance"* (checagem) para criativos gerados com IA e manter trilhas mínimas (ferramenta/versão/arquivo) para demonstrar diligência.
Direitos da personalidade (imagem, voz, nome e identidade)	O uso de IA pode intensificar riscos ligados a imagem, voz e identidade, especialmente com avatares, *voice cloning*, manipulação realista e *deepfakes*. Mesmo em campanhas com fins lícitos, o uso de semelhança identificável (ou elementos que sugiram endosso) exige cuidado reforçado com autorização, finalidade, limites de uso, e prevenção de confusão do público quanto à autenticidade. Esse tema é particularmente sensível em influenciadores, celebridades e "personas" que imitam pessoas reais. **Implicação operacional:** quando houver risco de confusão material, a conformidade envolve não só autorização/*clearance*, mas também decisões adequadas de transparência e rotulagem na peça criativa ou na experiência.
Regras publicitárias e autorregu-lamentação	Além do CDC, a conformidade publicitária passa por autorregulamentação, com destaque para o **CONAR** no Brasil, internacionalmente, o **ICC Code**, ambos ancorados em critérios como veracidade, identificabilidade, responsabilidade social e lealdade na comunicação[51]. A presença de IA no processo deve ser tratada como parte do "como" a publicidade é produzida — sem mudar o "o quê" é exigido em termos de honestidade e não enganosidade.
Termos de uso e políticas de plataformas e ferramentas	Em campanhas com IA, conformidade inclui observar (e documentar) o que as plataformas e ferramentas permitem quanto a: categorias proibidas, uso de dados, conteúdo sintético, rotulagem, publicidade política, restrições de segmentação, e regras de integridade (ex.: *deepfakes* e desinformação). Mesmo quando não há ilegalidade, violação de política de plataforma pode gerar remoção de anúncio, bloqueio de conta, perda de alcance ou impacto reputacional. **Implicação operacional:** processos internos e contratos com agência/fornecedores devem prever a obrigação de cumprir políticas de plataforma, manter evidências e acionar rapidamente correções quando houver *flag* ou remoção.
Regulações emergentes e operações internacionais	Para grupos com atuação internacional (ou que contratam fornecedores globais), é relevante considerar regulações estrangeiras com efeitos práticos sobre fornecedores e fluxos — como o **AI Act** da União Europeia[52]. E outros regimes que vêm tratando de transparência, conteúdo sintético, *deepfakes* e rotulagem, a exemplo de China e Califórnia. Essas referências devem ser avaliadas conforme a incidência concreta de cada norma e podem servir como indicativos de tendência regulatória, sem transposição automática para operações não sujeitas a tais regimes. Portanto, não devem ser lidas, por si só, como obrigação equivalente no Brasil.

50 https://www.isba.org.uk/system/files/media/documents/2023-10/AI%20Principles%20-%20Oct%202023.pdf

51 https://www.conar.org.br/pdf/Codigo-CONAR-2024.pdf; https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf

52 https://eur-lex.europa.eu/eli/reg/2024/1689/oj

4.8. Proporcionalidade entre risco, controle e impacto

O princípio da proporcionalidade orienta que as obrigações de governança e responsabilidade no uso de IA em marketing devem ser aplicadas na medida do risco e do impacto, levando em conta (i) o grau de controle do anunciante/agência sobre a tecnologia e o resultado, (ii) a previsibilidade do sistema (o quanto o comportamento e os *outputs* são estáveis e explicáveis), e (iii) o potencial de impacto sobre pessoas e consumidores.

Nível de risco / impacto	
Baixo	Uso interno para brainstorming, sumarização e apoio a rascunhos (sem publicação direta). **Controles típicos:** ferramenta homologada, orientação de uso, revisão humana antes de qualquer publicação.
Médio	Geração de variações de conteúdos criativos que serão revisadas e aprovadas; otimização de mídia com *guardrails*. **Controles típicos:** checklist de *claims*/PI, revisão humana, documentação mínima (ferramenta/versão), monitoramento de desempenho e *brand safety.*
Alto	*Deepfakes*/voz/imagem realista, avatares e chatbots voltados ao público, personalização intensa, campanhas para crianças/vulneráveis, decisões automatizadas com risco de discriminação. **Controles típicos:** aprovação reforçada (multiárea), critérios de *disclosure*, testes controlados, rastreabilidade ampliada, plano de incidentes e resposta rápida.

A proporcionalidade, assim, permite alinhar inovação e diligência: quanto maior o risco e o impacto, maiores devem ser as camadas de revisão, documentação e salvaguardas.

CHECKLIST RÁPIDO POR PRINCÍPIO: PERGUNTAS E EVIDÊNCIAS

Princípio	Pergunta de decisão (na prática)	Evidências mínimas (para comprovar)
Finalidade legítima e alinhamento com o negócio	Para que estamos usando IA aqui e qual resultado esperamos?	Objetivo documentado; escopo de uso + limitações e aprovações
Transparência e explicabilidade adequada ao contexto	O público pode ser induzido a erro se não souber que há IA ou automação?	Critério de *disclosure*; rótulo/aviso/FAQ registro da decisão
Centralidade humana, supervisão e revisão	O que exige revisão humana antes de ir ao ar (e em quais casos escalonar)?	Fluxo de revisão/aprovação; amostragem/monitoramento; registro de revisões
Não discriminação, equidade e mitigação de vieses	Há risco de estereótipos, exclusões injustas ou segmentação discriminatória?	Testes/checagens de viés + checklist de sensibilidade; revisão com time diverso
Segurança, integridade e confiabilidade	Estamos protegendo insumos e *outputs* e prevenindo uso indevido?	Controle de acesso; *logs*; regras para dados/*prompts* plano de incidentes
Responsabilidade e prestação de contas (*accountability*)	Quem responde por *outputs*, correções e incidentes?	Matriz RACI (papéis); cláusulas e SLA; canal de resposta rápida
Legalidade e conformidade regulatória	Cumpre LGPD, CDC/CONAR e direitos de PI/personalidade aplicáveis?	Validação jurídica quando necessário; checagem de *claims*; observância de termos de uso
Princípio da proporcionalidade entre risco, controle e impacto	O nível de controle/validação e supervisão humana é proporcional ao risco e ao impacto potencial do uso de IA?	Matriz de classificação de risco/criticidade do caso de uso; registro dos controles adotados compatíveis com o nível de risco

5. Riscos-chave e salvaguardas práticas

A IA permite escala, automação e criatividade, mas também aumenta a chance de erro e de dano, especialmente quando o output vai ao público, quando há personalização/segmentação, quando se simulam pessoas reais (imagem/voz) ou quando a campanha envolve temas sensíveis (saúde, finanças, crianças). Por isso, este Guia de Boas Práticas estabelece salvaguardas proporcionais ao risco, combinando revisão humana, rastreabilidade, transparência, governança de dados, controles contratuais e resposta rápida a incidentes[53].

53 https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf

Nível	Quando tende a ocorrer	Exemplos	Salvaguardas mínimas
Baixo	IA como apoio interno, sem personalização e sem alegações sensíveis	Brainstorm de headlines; resumo de insights	Revisão humana; checagem factual; registro básico (*prompt*/versão/aprovação)
Médio	IA gera conteúdo que vai ao público ou ajusta criativos/mídia	Variações de imagem/*copy*; otimização criativa	Revisão humana reforçada; checklist de compliance; checagem de direitos
Alto	Pode confundir/enganar, tocar vulneráveis, usar dados/biometria, ou simular pessoas	*Deepfake*/voz sintética; avatar "humano"; *chatbot* com oferta; segmentação sensível	Aprovação jurídica/ compliance; transparência ao público; testes/validação; rastreabilidade completa; plano de incidentes

5.1. Publicidade enganosa/abusiva, *AI washing* e *claims* sobre IA

AI washing é a prática exagerar, distorcer ou apresentar de forma vaga capacidades de IA para tornar um produto/serviço "mais atraente", ou para atribuir ao uso de IA uma autoridade indevida visando elevar credibilidade ou justificar preço/performance, sem lastro real[54].

Em geral, aparece em três formas:

1. IA como rótulo genérico (mencionar IA sem explicar minimamente o que ela faz)

2. *claims* absolutos ("100%", "sem erros", "infalível", "garantido")

3. atribuição indevida de confiança (usar IA para simular neutralidade, auditoria, certificação ou expertise)

Esse tipo de prática é alvo de atenção de autoridades, inclusive com iniciativas de repressão a *claims* enganosos e esquemas associados à IA[55]. Na prática, é importante ter em mente que dizer "usamos IA" ou "IA fez" não reduz responsabilidade e não substitui evidência. Ao contrário: pode elevar o padrão de diligência esperado, porque cria percepção de superioridade tecnológica[56].

Salvaguardas práticas

1. **Regra de comprovação ("substanciação") para *claims*:** todo claim sobre IA (precisão, eficiência, segurança, performance) deve ter evidências verificáveis e guardadas para auditoria
2. **Governança de *claims* de IA:** *claims* de IA devem passar por validação conjunta (Marketing + Produto/TI + Jurídico/Compliance)
3. **Comunicação com limites e linguagem precisa:** preferir descrições concretas ("usa IA para sugerir…" / "auxilia…") e evitar superlativos absolutos ("infalível", "garantido")[1]
4. **Arquivo de evidências e rastreabilidade:** guardar versão final, justificativas, estudos/ testes e aprovações

54 https://www.asa.org.uk/news/generative-ai-advertising-decoding-ai-regulation.html; https://www.ftc.gov/business-guidance/blog/2023/05/luring-test-ai-engineering-consumer-trust; https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

55 https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes; https://www.ftc.gov/business-guidance/blog/2023/03/chatbots-deepfakes-voice-clones-ai-deception-sale

56 https://wp.nyu.edu/compliance_enforcement/2024/04/17/the-luring-test-ai-and-the-engineering-of-consumer-rust/

O QUE FAZER	O QUE NÃO FAZER
✓ Descreva a IA de forma concreta e verificável (o que faz, para que serve e limites)	✗ Não atribua “autoridade automática” à IA
✓ Valide *claims* “sensíveis” (precisão, segurança, impactos) antes de ir ao ar	✗ Não prometa precisão/resultado garantido sem evidências robustas
✓ Substitua “IA” genérico por descrição funcional (“automatiza triagem”, “gera variações”, “otimiza lances”) e use linguagem proporcional ao que é demonstrável	✗ Não use IA como “selo” de superioridade sem evidência robusta e contexto adequado
✓ Mantenha substanciação e evidências para *claims* relevantes (testes, métricas, limites e condições)	✗ Não faça *claims* absolutos (“100%”, “infalível”, “sem erro”) nem apresente resultados como garantidos por IA
✓ Revise com rigor peças e scripts gerados por IA, principalmente para fatos, números, comparações e promessas	✗ Não utilize depoimentos, reviews, “provas sociais” ou demonstrações sintéticas de modo que o consumidor possa interpretar como reais quando não são
✓ Em experiências conversacionais, desenhe o fluxo para reduzir “excesso de confiança”: respostas seguras, limites, escalonamento para humano e transparência proporcional	✗ Não presuma que *disclosure* elimina risco: transparência não substitui conformidade com CDC/ autorregulamentação, nem “blinda” contra alegação de enganosidade/abusividade

5.2. Conteúdo sintético e integridade

Conteúdo sintético é qualquer material (texto, imagem, áudio, vídeo) gerado ou alterado por IA. O ponto central não é a sua natureza sintética, mas o impacto que pode gerar na integridade da comunicação.

Exemplos: simulação de pessoas reais (*deepfakes*), criação de depoimentos que parecem autênticos, alteração de evidências visuais (“antes e depois”), ou manipulação do contexto de forma que o consumidor acredite em algo que não aconteceu.

Em marketing, isso é especialmente crítico porque confiança é um ativo e porque conteúdos hiper-realistas podem reduzir a capacidade do público de distinguir ficção de realidade[57].

57 https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf

Salvaguardas práticas

1. **Decisão de transparência proporcional ao risco:** se a ausência de informação puder induzir erro, recomendar *disclosure* (“imagem gerada por IA”, “voz sintetizada”, etc.)
2. **Autorizações e controles para imagem/voz:** uso de imagem/voz/avatares requer autorização formal e definição de escopo
3. **Controles de origem e trilha de criação:** manter *logs*, versões, e registros do processo de geração
4. **Resposta rápida:** procedimento de retirada/retificação quando houver confusão pública ou erro material

O QUE FAZER	O QUE NÃO FAZER
✓ Trate “conteúdo sintético” como item obrigatório do checklist pré-publicação (“pode confundir?” → “precisa *disclosure*?”)	✗ Não crie depoimentos falsos, avaliações sintéticas ou prova social artificial
✓ Reforce revisão humana quando houver simulação de pessoas, “prova social” ou testemunhais	✗ Não simule pessoa real sem autorização (imagem/voz/ trejeitos reconhecíveis)

Portanto...

A sinalização de que o conteúdo foi gerado por IA (ex.: marcas d’água ou avisos como “imagem gerada por IA”) deve ser avaliada caso a caso e tende a ser recomendável quando a ausência dessa informação puder gerar risco concreto de engano material ao consumidor sobre a natureza, autenticidade, origem, endosso ou características do produto ou serviço oferecido. Quando o uso da IA for meramente instrumental (ex.: apoio criativo interno), não alterar fatos, não simular pessoa real, não reforçar artificialmente credibilidade ou não influenciar o peso do claim publicitário, o *disclosure* pode não ser necessário ou pode ser realizado de forma simplificada e contextual, preservando a fluidez da comunicação.

Em síntese, a rotulagem deve ser proporcional: suficiente para evitar engano material, sem transformar o uso legítimo de IA em ruído desnecessário na experiência do consumidor.

5.3 Personas sintéticas e dados sintéticos

Personas sintéticas são personagens/avatares (incluindo influenciadores virtuais e assistentes) criados com IA para comunicar, atender, “conversar” e gerar conteúdo. Essas personas podem apresentar alto grau de realismo e, justamente por isso, possuem elevado potencial de engajamento e persuasão.

O risco surge quando houver:

- Confusão relevante quanto à natureza não humana da interação
- Simulação de experiência ou autoridade inexistente
- Exploração indevida de confiança ou vulnerabilidade

O critério regulatório central não é a existência da persona virtual, mas a possibilidade de indução a erro material.

Personas sintéticas são juridicamente viáveis e estrategicamente valiosas, desde que a interação preserve clareza suficiente sobre sua natureza quando isso for relevante para a compreensão do público.

Salvaguardas práticas

1. **Transparência na interação:** deixar claro quando o público interage com persona/assistente virtual, mas apenas quando houver risco de confusão
2. **Limites de persuasão:** proibir scripts e estratégias que explorem vulnerabilidades emocionais, especialmente com crianças
3. **Governança de dados sintéticos:** documentar finalidade, método, testes de risco (reidentificação/inferências) e vieses. Se a geração de dados sintéticos usar dados pessoais como insumo, a atividade continua sujeita à LGPD (finalidade, adequação, necessidade, segurança, prevenção e responsabilização). “Virar sintético” não elimina a necessidade de governança do dado de origem, nem autoriza reuso ilimitado
4. **Contratos e direitos:** definir titularidade/licenças sobre o avatar/persona, escopo de uso, encerramento e remoção

O QUE FAZER	O QUE NÃO FAZER
✓ Use persona sintética como personagem identificado e com "roteiro de limites" (o que pode e não pode dizer) ✓ Documente o uso de dados sintéticos (origem, método, finalidade e testes): quais dados foram usados, para que foi gerado, e onde o sintético pode (ou não) ser aplicado ✓ Aplique controles de privacidade e segurança na geração: minimização, anonimização quando aplicável, regras de retenção e acesso, e avaliação de risco de reidentificação ✓ Faça checagem de viés/estereótipos nas personas e nos *outputs*, com revisão humana e diversidade de avaliadores ✓ Se houver uso externo (relatório, divulgação, conteúdo), descreva com clareza metodologia e limitações, evitando confundir simulação com pesquisa real	✗ Não apresente personas sintéticas como "consumidores reais" nem como "pesquisa de mercado" concluída; isso pode induzir a erro e elevar risco reputacional e regulatório ✗ Não deixe a persona "improvisar" ofertas sensíveis sem supervisão humana (especialmente em *chatbots*) ✗ Não use dados sintéticos gerados a partir de dados pessoais sem governança clara (finalidade, retenção, segurança, fornecedores) ✗ Não use personas sintéticas para justificar segmentações sensíveis, exclusões ou decisões com impacto relevante sem validação adicional e sem controles de não discriminação ✗ Não tome *outputs* "convincentes" como "verdadeiros": simulações podem refletir viés do modelo e do *prompt*

5.4 Viés, discriminação e estereótipos

Viés em IA acontece quando modelos reproduzem padrões distorcidos do treinamento ou do contexto de uso e isso pode gerar discriminação (tratamento injusto) ou estereótipos (representações reducionistas de grupos).

Em marketing, o risco aparece tanto no conteúdo (imagens/textos que reforçam preconceitos) quanto na operação (segmentação e otimização que excluem públicos ou exploram vulnerabilidades). Como plataformas e ferramentas "aprendem" com dados históricos, é comum que elas reproduzam desigualdades e preferências problemáticas presentes na sociedade sem que isso fique visível na peça final.

Salvaguardas práticas

1. **Supervisão humana** com foco em governança dos dados, diversidade, equidade e inclusão
2. **Testes e amostragem** de *inputs* e *outputs* e segmentações para detectar discriminação
3. **Diretrizes claras de linguagem e casting** (linhas vermelhas contra estereótipos e atributos sensíveis)
4. **Monitoramento contínuo** (viés não é "evento único": pode surgir por mudança de dados, tendências e contexto)
5. **Quando a geração, seleção ou controle operacional de conteúdos, publicações ou segmentações com IA** estiver a cargo de agência ou fornecedor, prever obrigação contratual de revisão independente e proporcional ao risco para mitigação de vieses, com registro das checagens realizadas e escalonamento ao anunciante quando houver risco relevante

O QUE FAZER	O QUE NÃO FAZER
✓ Incorpore **equidade e inclusão** como requisito de qualidade: trate viés como risco de marca e de conformidade, não como "tema secundário" ✓ Revise *inputs* e *outputs* de IA com checklist de estereótipos/representação e, quando relevante, com avaliadores diversos ✓ Quando a geração ou seleção do conteúdo estiver a cargo de agência/fornecedor, atribua contratualmente a eles a obrigação de realizar ou viabilizar essa revisão, mantendo evidências para validação do anunciante ✓ Monitore segmentação/entrega para identificar exclusões não intencionais e corrija parâmetros e criativos ✓ Documente decisões de mitigação e correção (*prompt*, filtros, bibliotecas, ajustes)	✗ Não presuma neutralidade automática *outputs* convincentes podem carregar vieses do modelo e do contexto ✗ Não automatize segmentação/otimização sem *guardrails* e sem revisão quando houver impacto potencialmente desigual ✗ Não publique conteúdos que reforcem estereótipos (gênero, raça, idade, deficiência, classe, território), mesmo "sem intenção": o critério é o efeito e a leitura provável pelo público

5.5 Propriedade intelectual e direitos de personalidade

IA generativa ampliou a capacidade de criar textos, imagens, vídeos, trilhas, locuções e avatares em escala, mas isso não elimina obrigações legais sobre propriedade intelectual (PI) e direitos de personalidade. Ao contrário: como a produção se torna mais rápida e distribuída, aumenta o risco de que conteúdos protegidos sejam utilizados sem licença, de que "semelhanças" com obras e pessoas reais passem despercebidas e de que se descumpram regras contratuais (termos de plataformas, bancos de imagem/voz, contratos com agências e talentos).

Em campanhas, os problemas mais recorrentes surgem em três pontos: (i) *inputs* (o que entra na ferramenta — *brief*, *prompts*, imagens, referências, *assets* e dados), (ii) *outputs* (o que a ferramenta gera — e se há risco de reprodução relevante, similaridade, marca/obra/personagem, ou "voz/imagem" reconhecível) e (iii) uso e licenciamento (como o resultado será explorado — comercialmente, em quais mídias/territórios — e sob quais termos, inclusive quanto a retenção, reutilização e eventual treinamento do fornecedor).

Salvaguardas práticas

1. **Checklist de direitos antes de publicar:** verificar licenças, releases, autorizações, termos de bancos de mídia e compatibilidade com o uso pretendido (mídia/território/prazo), além de checagem de similaridade/risco de confundibilidade
2. **Contratos com agência/fornecedor:** prever regras sobre *inputs* de terceiros; obrigação de *disclosure* interno do uso de IA; declarações e garantias de que a agência/fornecedor possui as autorizações necessárias para os materiais utilizados e de que os *inputs* e *outputs* não violam direitos de terceiros; obrigação de indenização em caso de reivindicações; limites de reuso/exclusividade; e obrigação de manter evidências de clearance e documentação de origem/licenças quando aplicável e proporcional ao risco
3. **Treinamento e reutilização de materiais do anunciante:** proibir o treinamento, *fine-tuning* ou reutilização de materiais do anunciante para melhorar modelos do fornecedor sem autorização expressa, com escopo, finalidade, retenção, segurança e possibilidade de auditoria definidos
4. **Política interna de confidencialidade e "inputs permitidos":** definir o que pode/não pode ser inserido em ferramentas (incluindo *assets* não lançados, estratégia, segredos comerciais, dados pessoais e materiais licenciados com restrições), e treinar times e parceiros

O QUE FAZER	O QUE NÃO FAZER
✓ Trate qualquer ferramenta de IA como fornecedor: valide termos, uso comercial, retenção e reuso antes de adotar	✗ Não presuma que "*output* é automaticamente original" ou que "se a IA gerou, está liberado"
✓ Exija do fornecedor documentação de origem/licenças quando aplicável e proporcional ao risco, defina a titularidade do entregável final e inclua declarações, garantias e indenização contratual por violações de Propriedade Intelectual, direitos de personalidade e quaisquer outros direitos de terceiros	✗ Não peça para a IA "imitar" obra/artista/marca de modo que gere derivação indevida
✓ Ajuste contratos para impedir "treinamento por padrão" com materiais do anunciante	✗ Não use voz/imagem de pessoa real (ou altamente similar) sem autorização
✓ Inclua cláusulas contratuais específicas: *disclosure* de IA, origem de insumos, direitos sobre *outputs*, reuso, indenização, auditoria e subfornecedores	✗ Não use voz/imagem "muito parecida" com celebridades, influenciadores ou pessoas reais sem autorização (mesmo que "não seja idêntica")
✓ Defina e aplique regra de ***inputs* permitidos** (o que pode entrar no *prompt*) + treinamento do time e da agência	✗ Não use ferramentas "gratuitas" ou não homologadas para projetos sensíveis, inserindo assets, brief confidencial ou dados do negócio
✓ Faça *clearance* prévio: checagem de PI e personalidade, com foco em **similaridade/confundibilidade** e presença de marcas/obras/personas reconhecíveis	✗ Não alimente IA com materiais de terceiros (imagens, músicas, roteiros, slogans, personagens) sem licença ou fora do escopo da licença

O QUE FAZER	O QUE NÃO FAZER
✅ Garanta **autorizações expressas** para uso de imagem/voz/nome/semelhança quando houver pessoa real ou risco de reconhecimento ✅ Para avatares e personagens, avalie risco de **confusão material** e adote *disclosure* proporcional quando necessário ✅ Tenha processo de resposta rápida: se houver contestação de PI/personalidade, pausar peça e revisar ativos e aprovações	❌ Não aceite contratos "genéricos" que não definam responsabilidade por *inputs/outputs* e por violações de PI/personalidade ❌ Não ignore sinais de risco (reclamação de semelhança, *takedown,* denúncia); a demora em adotar medidas de resposta amplia dano e exposição

5.6. Dados pessoais no treinamento

Quando se trata do treinamento de modelos de IA, é necessário especial cuidado para assegurar a conformidade com a legislação de Privacidade e Proteção de Dados. Dentre os múltiplos elementos abordados na seção de proteção de dados deste guia, dois merecem consideração especial no contexto do treinamento de IA – a transparência e a base legal para o tratamento de dados pessoais no contexto do treinamento de modelos de IA.

Transparência: é necessário que exista comunicação efetiva com os titulares de dados, de forma com que estes possam efetivamente compreender como os seus dados são utilizados no treinamento de modelos de IA e para qual finalidade.

Salvaguardas práticas

Como garantir adequada transparência?

Além dos quesitos apresentados acima (conforme item 3 deste guia), recomendam-se os seguintes cuidados adicionais no contexto do treinamento de IA[58]

- ✅ Informar ativamente os titulares de dados, sempre que possível, acerca do uso de seus dados para essa finalidade
- ✅ Fornecer ao titular informações como as categorias de dados utilizadas, sua origem e as formas de exercício de seus direitos, em especial o direito de oposição
- ✅ Disponibilizar tais informações no momento do início da coleta dos dados ou, quando isso não for possível, no primeiro contato subsequente com o titular

BASE LEGAL

Como regra, desde que não haja o tratamento de dados pessoais sensíveis, tal tratamento pode fundamentar-se no legítimo interesse, desde que atendidos os requisitos do teste de balanceamento (conforme item 4.2 deste guia). Existem recomendações adicionais àquelas já apresentadas ao longo desse guia que podem auxiliar no enquadramento com a base legal:

58 https://www.cnil.fr/fr/node/165891

Situação	Recomendações
Coleta de dados pessoais[59]	✅ Definir antecipadamente quais dados pessoais você precisa tratar e por qual motivo ✅ Realizar a filtragem de dados previamente à coleta, com a definição de critérios precisos que mitiguem a probabilidade de coleta acidental de dados pessoais sensíveis, dados de crianças e adolescentes ou dados irrelevantes ✅ Realizar a filtragem de dados após a coleta, mas de forma prévia ao treinamento do modelo de IA ✅ Documentar os processos de filtragem de dados ✅ Ao coletar dados de fontes públicas, respeite websites que claramente se opõem a scraping, ex.: por meio do uso de robot.txt. Além disso, elimine dados excessivos[60]
Exercício de Direitos pelo titular	✅ Garantir a possibilidade de o titular opor-se ao uso de seus dados para o treinamento de modelos de IA ✅ Assegurar que o direito de oposição seja disponibilizado de maneira simples e intuitiva, idealmente em posição de destaque nas configurações do portal de privacidade ou em outra solução adotada pela organização para a recepção e o tratamento das solicitações dos titulares[61]
Transparência	✅ Caso os titulares não possuam uma relação prévia com a organização (não tenham tido oportunidade de acessar seu Aviso de Privacidade), notificá-los proativamente, na medida do possível ✅ Atender as recomendações de transparência no quadro acima
Minimização de dados[62]	✅ Anonimize os dados logo após a sua coleta ✅ Avalie a viabilidade de uso de dados sintéticos (ex.: dados criados artificialmente para imitar dados estatisticamente reais, sem se referirem a pessoas ou fatos reais)

OBSERVAÇÕES:

- O atendimento destas recomendações não necessariamente implica na adequação do enquadramento do tratamento. O caso concreto sempre deverá ser considerado
- O enquadramento do treinamento do modelo sob o legítimo interesse não implica, necessariamente, que o uso do modelo se fundamente na mesma base legal, sendo possível que o treinamento se apoie no legítimo interesse enquanto o uso exija, ex.: o consentimento do titular[63]

59 https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf

60 https://www.cnil.fr/en/legal-basis-legitimate-interest-focus-sheet-measures-implement-case-data-collection-web-scraping

61 ANPD. Voto n° 11/2024/DIR-MW/CD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf

62 https://www.cnil.fr/en/relying-legal-basis-legitimate-interests-develop-ai-system

63 https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-46-2024.pdf

O QUE FAZER	O QUE NÃO FAZER
✓ Definir finalidade e escopo do treinamento (objetivo, categorias de dados, fontes, prazo, destinatários e ambiente de processamento) ✓ Utilizar apenas dados estritamente necessários; preferir dados agregados, pseudonimizados/ anonimizados quando viável ✓ Realizar triagem/filtragem prévia do dataset (remoção de dados sensíveis, dados de crianças/ adolescentes e dados irrelevantes ao objetivo) ✓ Documentar base legal e justificativa do uso de dados no treinamento, incluindo avaliação de proporcionalidade e riscos ✓ Garantir transparência proporcional sobre uso de dados em treinamento quando aplicável e disponibilizar canais para exercício de direitos ✓ Implementar e operacionalizar o direito de oposição quando aplicável, com fluxo interno e responsáveis definidos ✓ Estabelecer regras contratuais com agência/ fornecedores: vedação de reutilização/treinamento com dados do anunciante sem autorização expressa; retenção, descarte e auditoria ✓ Avaliar alternativas de menor risco (ex.: dados sintéticos, amostras reduzidas, técnicas de anonimização) quando atingirem o objetivo. ✓ Definir processo de aprovação interna para projetos que envolvam treinamento com dados pessoais (*gate* de privacidade/jurídico/ segurança, conforme risco)	✗ Não treinar IA com bases amplas e não delimitadas (“aproveitar tudo o que existe”), sem finalidade específica e documentada ✗ Não misturar dados sensíveis ou de menores no treinamento sem justificativa, controles reforçados e autorização aplicável ✗ Não usar textos genéricos que não expliquem finalidade e implicações relevantes ✗ Não dificultar ou inviabilizar oposição/ exclusão, criando fricção ou ausência de canal efetivo ✗ Não permitir “treinamento por padrão” pelo fornecedor com dados do anunciante, por cláusulas vagas ou ausência de cláusulas ✗ Não compartilhar dataset livremente com múltiplas áreas/terceiros sem controle de acesso e sem rastreabilidade ✗ Não usar dados pessoais reais por conveniência quando alternativas menos intrusivas atenderiam ao caso ✗ Não rodar “pilotos” com dados pessoais sem validação e sem controles mínimos de governança e segurança

5.7. Segurança da Informação na IA

Ao abordar a segurança da informação no contexto da IA, é necessário considerar três riscos recorrentes: (a) ataques cibernéticos tradicionais, que poderiam afetar qualquer sistema de IA; (b) ataques específicos direcionados a sistemas de IA, conhecidos como ataques adversariais; e (c) falhas humanas no uso da IA, capazes de expor dados pessoais e informações confidenciais da organização.

Para ataques cibernéticos tradicionais e ataques específicos direcionados a sistemas de IA, os cuidados recaem, em regra, sobre os responsáveis pelo desenvolvimento e pela implementação das soluções de IA. Assim, a depender do papel desempenhado pela organização, essas orientações podem servir tanto

como parâmetro para o cumprimento de suas próprias responsabilidades quanto como referência para a formulação de exigências contratuais a seus fornecedores. Já em relação a falhas humanas no uso da IA, as orientações destinam-se especificamente aos utilizadores das soluções de IA.

a) Ataques cibernético tradicionais

Sistemas de IA, como qualquer outro, dependem de ativos informacionais e computacionais para funcionar – bases de dados, infraestrutura de processamento, aplicações, APIs, dentre outros. Esses ativos encontram-se sujeitos aos riscos ordinários de segurança da informação[64], e devem ser integrados à gestão de segurança da informação existente na organização e protegidos com medidas técnicas apropriadas, tais como controles de acesso, criptografia, gestão de vulnerabilidades, cópias de segurança encriptadas, *logs*, práticas de prevenção ao vazamento de dados, dentre outras.

Vale mencionar que se no contexto do ataque houver o envolvimento de dados pessoais e risco ou dano relevante aos titulares, recomenda-se avaliar a aplicação da Resolução CD/ANPD nº 15 – Regulamento de Comunicação de Incidentes de Segurança, incluindo eventual necessidade de comunicação à ANPD e aos titulares, a adoção de medidas técnicas, administrativas e de governança adequadas, bem como a documentação e análise estruturada do incidente.

b) Ataques voltados especificamente para a IA

Modalidade	Descrição[64,65]
Abuso	Ataques na fase de coleta de dados, introduzindo informações inadequadas em fontes legítimas, inserindo informações incorretas que o sistema absorve, com o objetivo de desviar ou deturpar o uso pretendido do modelo, sem alterar diretamente o processo formal de treinamento.
Envenenamento	Ataques na fase de treinamento que introduzem dados corrompidos ou enviesados na base de dados de treinamento, levando o modelo a aprender padrões inadequados.
Evasão	Ataques na fase de teste ou uso operacional do sistema de IA, na qual o atacante manipula minimamente as entradas fornecidas ao modelo, sem alterar seu treinamento ou parâmetros internos, com o objetivo de induzir classificações ou decisões incorretas durante a inferência (ex.: fornecer a um sistema de um veículo autônomo placas de "pare" com pequenas alterações, para que ele passe a classificar as placas de pare como placas de limite de velocidade).
Privacidade	Ataques durante a fase de uso operacional em que buscam inferir informações sensíveis sobre o modelo ou seus dados de treinamento, por meio de interações legítimas usadas para engenharia reversa, exploração de fontes ou identificação de fragilidades.

64 https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
65 https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
66 https://csrc.nist.gov/pubs/ai/100/2/e2025/final

Salvaguardas práticas[67]

1. **Treinamento adversarial:** técnicas de mitigação que treinam o modelo com exemplos intencionalmente perturbados, visando aumentar sua resistência a ataques durante a inferência
2. ***Randomized smoothing:*** técnicas que adicionam ruído controlado às entradas para tornar as previsões do modelo mais estáveis frente a pequenas perturbações adversariais
3. **Higienização de dados:** técnicas projetadas para limpar o conjunto de treinamento e remover amostras envenenadas antes da realização do treinamento do modelo de aprendizado de máquina
4. **Inspeção e higienização do modelo:** técnicas de avaliação do modelo antes de sua implementação para detectar e corrigir indícios de envenenamento ou abuso

OBSERVAÇÃO

Os controles a serem implementados sempre vão depender do caso concreto, no entanto os ataques descritos acima e as medidas exemplificativas podem ser adotadas como parâmetro ao se avaliar os riscos envolvendo o desenvolvimento ou implementação de um modelo de IA, sobretudo se disponíveis ao público geral (ex.: *chatbots*).

c) Falhas humanas no uso da IA

Quando colaboradores utilizam soluções de IA no dia a dia (especialmente ferramentas generativas e assistentes conversacionais), a segurança da informação passa a depender menos apenas da robustez técnica do fornecedor e mais do comportamento operacional de quem usa a ferramenta. *Prompts*, anexos e interações podem, inadvertidamente, expor dados pessoais, informações confidenciais e ativos criativos; além disso, certas configurações podem ampliar o risco de reuso indevido do conteúdo inserido.

Por isso, mesmo ferramentas "confiáveis" podem se tornar vetor de incidente se forem usadas sem regras claras de acesso, de configuração e de conteúdo permitido, tornando indispensáveis políticas internas, treinamento e salvaguardas específicas para uso por colaboradores.

67 https://csrc.nist.gov/pubs/ai/100/2/e2025/final

Salvaguardas práticas

1. **Garantias contratuais e política de retenção:** obtenha garantias do fornecedor sobre retenção, reuso e treinamento com dados da companhia (*opt-out* por padrão quando possível) e sobre subcontratados e transferências
2. **Regra de ouro de *inputs*:** proibir a inserção de informações confidenciais (estratégia, contratos, preços, planos de mídia, negociações, listas de clientes) e dados pessoais, salvo em ferramentas homologadas e para casos de uso autorizados
3. **Classificação do que pode entrar:** crie uma matriz simples de classificação ("pode", "pode com cuidado", "não pode") para *prompts* e anexos, incluindo materiais sob NDA, ativos criativos não lançados e documentos internos
4. **Ferramentas homologadas e bloqueio de *shadow AI:*** permitir apenas ferramentas aprovadas para uso corporativo e desencorajar o uso de contas pessoais/plug-ins não autorizados para trabalho
5. **Acesso por perfil e segregação de permissões:** aplique mínimo privilégio (quem pode usar quais ferramentas e com que recursos), com SSO (*Single Sign-On*)/MFA (Autenticação Multi fator) e revogação rápida de acessos em desligamentos
6. ***Logs*, monitoramento e auditoria mínima:** manter registro de acesso/uso (quando possível e proporcional), para investigação de incidentes e melhoria de políticas, com retenção e acesso controlados
7. **Treinamento e comunicação contínua:** treinamento curto e recorrente com exemplos reais do dia a dia (o que é dado sensível, o que não pode ir no *prompt*, como configurar privacidade, como reportar incidente)
8. ***Playbook* de incidentes:** criar procedimento simples para "usei IA e acho que expus algo" - quem avisar, como registrar, como conter (revogar links, pausar integrações, notificar TI/Jurídico/Privacidade)

O QUE FAZER	O QUE NÃO FAZER
Homologar ferramentas com critérios mínimos de segurança, termos de uso, retenção, treinamento com dados, suporte a *logs* e incidentes	**Não tratar segurança como assunto exclusivo de TI**, sem regras operacionais para o time de marketing e parceiros
Definir política de *"inputs* permitidos": o que pode e o que é proibido inserir (dados pessoais, segredos comerciais, estratégias, contratos, ativos inéditos, materiais de terceiros)	Não permitir o uso de ferramentas não aprovadas, contas pessoais, extensões/plug-ins não validados
Desabilitar uso de *prompts*/arquivos para treinamento sempre que possível; restringir histórico e compartilhamento	**Não compartilhar credenciais e acessos** ou manter permissões amplas para "facilitar a operação"

O QUE FAZER	O QUE NÃO FAZER
✅ **Manter *logs* e rastreabilidade proporcional ao risco** (acessos, uso, versões, integrações, alterações relevantes), com retenção e controle de acesso ✅ **Estabelecer *playbook* de incidentes:** como conter (pausar bot/campanha), preservar evidências, acionar responsáveis e comunicar internamente ✅ **Treinar colaboradores periodicamente** com exemplos práticos (o que não pode entrar, como configurar, como reportar incidente)	❌ **Não conectar IA a sistemas internos (CRM, bases, *drive)*** sem conter *prompt injection* e sem delimitar escopo de acesso ❌ **Não contratar/usar fornecedor sem compromissos mínimos**, deixando obrigações de segurança indefinidas

5.8. Crianças e grupos vulneráveis: cuidados reforçados (conteúdo, segmentação, persuasão)

O uso de IA no marketing pode aumentar a capacidade de personalizar mensagens, ajustar materiais publicitários em tempo real e conduzir interações conversacionais com alto poder de persuasão. Quando o público inclui crianças/adolescentes ou grupos vulneráveis (por condição socioeconômica, idade, saúde, endividamento, fragilidade emocional, baixa literacia digital etc.), esses mecanismos elevam o risco de manipulação indevida e violação de padrões de publicidade responsável. Por isso, recomenda-se adotar um nível reforçado de diligência. Não basta "cumprir a regra geral", é necessário desenhar campanhas com *guardrails* específicos para proteção, transparência e adequação[68].

Onde a IA aumenta o risco (e por quê):

- **Persuasão "otimizada" e testes contínuos:** sistemas de otimização aprendem rapidamente quais mensagens geram mais clique, retenção e conversão. Em públicos vulneráveis, isso pode canalizar conteúdos com abordagem de venda/oferta mais agressiva (ex.: urgência artificial, culpa, medo, insistência), com impacto maior do que em adultos plenamente informados
- **Interações conversacionais (*chatbots*, avatares, "amigos virtuais"):** interfaces humanizadas podem gerar confiança desproporcional, em especial em crianças, que tendem a interpretar esse tipo de interação como relações sociais verdadeiras. A linha entre informação, entretenimento e persuasão pode ficar menos clara
- **Segmentação e inferências sensíveis:** a IA pode inferir preferências, estados emocionais e "propensão" a determinados comportamentos. Em grupos vulneráveis, isso pode aproximar-se de persuasão indevida — principalmente se combinado com *timing* e personalização em microcontextos

68 https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; https://www.conar.org.br/pdf/Codigo-CONAR-2024.pdf; https://icas.global/wp-content/uploads/AI-In-Advertising.pdf

Salvaguardas práticas

1. **Política de "tolerância menor" para risco:** campanhas com crianças/vulneráveis devem ter critérios mais restritivos para personalização, formatos conversacionais e otimização automatizada
2. ***Guardrails* de conteúdo:** proibir linguagem de pressão (ex.: "se você não comprar…", "última chance"), gatilhos emocionais indevidos e mensagens que explorem medo/culpa, especialmente em temas sensíveis
3. **Controles de segmentação:** revisar critérios, evitar inferências sensíveis e restringir lookalikes/expansões quando o público incluir menores ou grupos vulneráveis
4. **Design de atendimento**: em *chatbots*/agentes, adotar linguagem adequada, não simular relação afetiva, limitar recomendações, e escalar para humano quando houver sinais de vulnerabilidade
5. **Revisão humana reforçada:** dupla revisão (criativo + compliance) para campanhas e jornadas com risco aumentado

O QUE FAZER	O QUE NÃO FAZER
✓ Trate crianças/vulneráveis como categoria de risco alto para IA (personalização, *chatbots*, otimização)	✗ Não use IA para explorar impulsividade, medo, culpa ou urgência artificial, especialmente com menores
✓ Restrinja automação e exija revisão humana reforçada para mensagens e jornadas sensíveis	✗ Não usar *chatbots*/avatares para simular aconselhamento ou relação emocional, nem para pressionar decisões
✓ Garanta transparência adequada quando houver interação conversacional e evite criar "confusão social" (parecer amigo/terapeuta)	✗ Não aplicar *lookalikes*/expansões sem guardrails quando houver risco de atingir menores ou vulneráveis indevidamente
✓ Documente decisões: por que a segmentação foi escolhida, quais limites e controles foram aplicados	

5.9. Sustentabilidade e impactos sociais (energia, cadeia de fornecedores, reputação)

O uso de IA no marketing também traz impactos que extrapolam a campanha: consumo de energia, dependência de infraestrutura de terceiros, escolhas de fornecedores e efeitos sociais associados ao uso de automação em larga escala.

Ainda que muitas organizações tratem sustentabilidade como tema "corporativo", a IA torna esse tópico operacional: decisões sobre ferramentas, volume de geração, automações e governança de fornecedores podem afetar pegada ambiental, riscos reputacionais e expectativas de stakeholders.

a) Energia e eficiência (o que muda com IA)

Modelos generativos podem demandar recursos computacionais relevantes, especialmente em aplicações intensivas (vídeo, imagem de alta resolução, geração em massa, treinamento e *fine-tuning*). É importante avaliar: proporcionalidade de uso, reutilização de ativos e estratégias de redução de desperdício (ex.: evitar gerar centenas de variações sem necessidade)

b) Cadeia de fornecedores (riscos e diligência)

IA no marketing frequentemente envolve múltiplos fornecedores: modelos, plataformas, plugins, bancos de imagem/voz e serviços de anotação. Isso amplia riscos de:

- **opacidade** sobre onde e como o processamento ocorre
- **dependência** de um fornecedor e indisponibilidade/alterações de política
- **conformidade** contratual e de segurança
- **expectativas ESG** sobre a cadeia

c) Impactos sociais e reputação

A IA pode gerar repercussão negativa quando:

- substitui indevidamente trabalho criativo sem transparência interna ou com conflitos de Propriedade Intelectual
- produz conteúdos estereotipados ou desinformação
- é percebida como "automatização desleal" (ex.: personas sintéticas "fingindo" consumidores reais)

Além disso, *claims* ambientais *(green claims)* ou de responsabilidade associados a IA devem seguir o mesmo rigor de substanciação: prometer "IA sustentável" sem base pode aumentar risco reputacional e de questionamento.

O QUE FAZER	O QUE NÃO FAZER
✓ Inclua sustentabilidade como critério na **seleção e homologação** de ferramentas (eficiência, governança, transparência do fornecedor)	✗ Não incentive geração em massa sem objetivo ("gerar por gerar"), especialmente em formatos pesados (imagem/vídeo)
✓ Reduza "desperdício de geração": defina limites de volume, reutilize ativos e padronize *prompts*/briefs para evitar retrabalho	✗ Não use sustentabilidade como discurso ("IA verde", "baixo impacto") sem evidência e critérios claros
✓ Avalie riscos reputacionais: transparência adequada, integridade e respeito aos direitos de Propriedade Intelectual/personalidade	✗ Não terceirize sem governança: opacidade de fornecedores e mudanças de política podem virar risco operacional e reputacional
✓ Exija de fornecedores informações mínimas de governança (segurança, retenção, subcontratados), alinhando com diligência de cadeia	✗ Não autorize uso de IA sem capacitação mínima obrigatória, sobretudo para funções que publicam conteúdo ou atendem consumidores

6. Governança de IA aplicada à publicidade (como implementar)

Este item reúne práticas de governança para tornar o uso de IA em marketing executável no dia a dia, com critérios claros de aprovação, rastreabilidade e responsabilização ao longo da cadeia, sempre seguindo lógica prática e proporcional ao risco (ver princípios dos itens 4 e 5 deste guia). O objetivo é reduzir risco jurídico e reputacional sem travar a criatividade trazendo rotinas, papéis e evidências mínimas.

6.1 Transparência com o público: quando e como divulgar uso de IA

A transparência não implica, como regra geral, a obrigatoriedade de labelling ou identificação do uso de IA. Eventuais divulgações sobre o uso de IA devem ser avaliadas de forma excepcional, contextual e orientada por risco, considerando o potencial de confusão ao consumidor e o estado atual do debate regulatório no Brasil.

É importante observar que o tema ainda está em evolução e, portanto, não há consenso, inclusive no âmbito da autorregulamentação publicitária brasileira e das discussões internacionais, sobre um dever de rotulagem de conteúdos gerados ou apoiados por IA. As orientações abaixo, portanto, devem ser lidas como parâmetros de boa prática para avaliação casuística de risco, e não como obrigação setorial ou presunção de irregularidade pela ausência de aviso.

CRITÉRIO PRÁTICO

Observada a contextualidade da campanha publicitária, a divulgação pode ser recomendável, a depender do caso concreto quando o uso de IA pode influenciar a decisão ou a compreensão do consumidor e (i) envolve alto realismo (voz/imagem/avatares, deepfakes, conteúdo sintético que pareça factual); (ii) cria interação conversacional que pareça humana; (iii) automatiza decisões de segmentação/otimização com impacto relevante; ou (iv) afeta públicos sensíveis (crianças, vulneráveis, temas de saúde/finanças).

Gatilho de *disclosure*	Perguntas de decisão	Exemplo típico	Como divulgar
Interação que pareça humana	O consumidor pode presumir que fala com uma pessoa? Há risco de promessa indevida?	Atendimento via chat com respostas geradas por IA	Especialmente para público vulnerável, sinalização no início e durante a conversa: “Atendimento automatizado por IA”
Conteúdo sintético altamente verossímil	O público pode confundir como gravação/foto real? Pode haver “surpresa razoável”?	Imagem de modelo com cabelos tratados	Rótulo visível na peça/descrição e, quando aplicável, indicação no áudio/legenda

69 https://www.iab.com/guidelines/ai-transparency-and-disclosure-framework/

Gatilho de *disclosure*	Perguntas de decisão	Exemplo típico	Como divulgar
Imagem, voz, nome, semelhança de pessoa real	Pode gerar percepção de endosso/ autorização? Há direitos de personalidade envolvidos?	Locução "clonada" semelhante a celebridade	Avaliar contextualmente. A divulgação pode ser necessária caso gere percepção de endosso ou que possa afetar diretamente a decisão de compra ou compreensão da mensagem
Alegações sobre o uso de IA como diferencial do produto	O claim é verificável e não induz confiança indevida?	"100% criado por IA", "IA garante resultado"	Explicar limites e base do claim (lettering e/ou qualificador); evidências e documentação interna; evitar exageros
Conteúdo sobre temas sensíveis ou grupos vulneráveis	Há risco de manipulação, estigmatização ou engano ampliado?	Campanha de produtos de beleza com avatares gerados por IA, voltada a adolescentes	Divulgação e controles reforçados; revisão humana e adequação do tom
Uso "interno" sem exposição direta ao consumidor	Há algum elemento material perceptível pelo público?	IA usada só para brainstorming e rascunhos	Em regra, não exige *disclosure* ao consumidor; manter registro interno

Como divulgar: a comunicação deve ser clara, em linguagem simples e próxima ao ponto de contato (na peça, no início da interação ou em local de fácil acesso), não substitui conformidade (ver itens 4.7 e 5) e deve estar alinhada à autorregulamentação publicitária de comunicação honesta e não enganosa[70].

PROCEDIMENTO RECOMENDADO

- Informe o uso de IA quando isso for relevante para a compreensão do anúncio, produto/serviço ou interação, ou quando puder afetar diretamente a decisão de compra/uso do consumidor
- Use linguagem simples e sinalização no ponto de contato (peça, interface, início de conversa)
- Se for o caso de *disclosure*, indique em que etapa a IA foi aplicada (ex.: "imagem gerada por IA", "voz sintetizada", "atendimento via IA com supervisão")
- Mantenha registros internos do racional de divulgação (por que, onde e em quais peças/canais)
- Avaliar a divulgação do uso de IA quando a omissão puder gerar risco concreto de confusão material quanto à autenticidade, origem, endosso ou características do que está sendo comunicado
- Não rotular tudo indiscriminadamente *(label/ fatigue)* ou ocultar *disclosure* em rodapés inefetivos

70 https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf; http://www.conar.org.br/pdf/Codigo-CONAR-2024.pdf

6.2 *Assessment* para contratação de agências

O *assessment* é uma diligência prática para reduzir risco (jurídico, reputacional, **ético**, dados e Propriedade Intelectual) antes de contratar ou renovar com agências que usarão IA. Deve combinar perguntas objetivas, evidências documentais e cláusulas contratuais que garantam revisão humana, rastreabilidade, transparência, segurança e responsabilização por *outputs*.

Também é recomendável que o *assessment* avalie, desde as fases iniciais da contratação, a extensão da responsabilidade assumida pela agência ou fornecedor por *inputs* e *outputs* gerados ou apoiados por IA, inclusive em caso de reivindicações de terceiros decorrentes de uso não autorizado de propriedade intelectual e direitos de personalidade. Essa análise deve considerar declarações e garantias, obrigação de indenização, eventuais limitações de responsabilidade, exclusões contratuais e procedimentos de resposta a claims, permitindo ao anunciante calibrar riscos jurídicos e expectativas comerciais antes do avanço das negociações.

PERGUNTAS E EVIDÊNCIAS MÍNIMAS

Tema	Perguntas práticas	Evidências mínimas
Governança e capacitação	Existe responsável/comitê de IA? Há treinamento contínuo?	Política interna; trilha de treinamento; responsável nomeado
Ferramentas e subcontratação	Quais ferramentas serão usadas e para qual finalidade? Houve aprovação expressa do Anunciante para essas ferramentas? Há terceiros/subcontratados?	Lista de ferramentas aprovadas com finalidade e versão; subcontratados; fluxos
Revisão humana e qualidade	Quais níveis de revisão humana antes de publicar? Há checagem de fatos?	Fluxo de revisão/aprovação; *checklists;* amostragem
Transparência	Como viabiliza avisos/rotulagem quando necessário?	Modelos de avisos; exemplos; registro de decisão
Dados e confidencialidade	Como evita inserir dados pessoais/ confidenciais em *prompts*?	Regras de dados permitidos; controles; cláusulas
PI e direitos de personalidade	Como documenta origem/licenças e autorizações quando aplicável, e qual responsabilidade assume por *inputs*, *outputs* e reivindicações de terceiros envolvendo PI e direitos de personalidade?	Inventário de assets/licenças/ autorizações quando aplicável; cláusulas de declarações e garantias; matriz de responsabilidade por *inputs* e *outputs*; obrigação de indenização; limites ou exclusões de responsabilidade; fluxo de *clearance* e resposta a *claims*
Resposta a incidentes	Há plano e canal emergencial? Prazo de notificação?	*Playbook*; SLA; contatos

PROCEDIMENTO RECOMENDADO

- Peça evidências (não só “declarações”) e exija registro das ferramentas/versões e finalidade
- Exija fluxo de revisão humana e critérios de aprovação por risco/campanha
- Inclua SLA para correção/remoção e canal emergencial
- Não contrate com base apenas em “portfólio criativo”, sem checar processo e evidências
- Não aceite “caixa-preta” (sem lista de ferramentas, sem revisão, sem rastreabilidade)
- Não trate incidentes como consequências improváveis e remotas
- Avalie previamente se a agência/fornecedor assume responsabilidade e obrigação de indenização compatíveis com o risco por *outputs* gerados ou apoiados por IA, especialmente em caso de reivindicações de terceiros envolvendo PI e direitos de personalidade

6.3 Políticas internas e capacitação

Políticas internas traduzem princípios em regras simples: o que pode/não pode, quem aprova, como registrar e como escalar dúvidas. A capacitação contínua reduz riscos operacionais (ex.: uso de informações confidenciais em *prompts*) e aumenta a capacidade de revisão crítica dos *outputs*, especialmente em temas sensíveis.

PROCEDIMENTO RECOMENDADO

- Defina por escrito quais informações/dados podem ser inseridos em sistemas de IA
- Exija evidências de treinamento contínuo e, quando aplicável, estrutura de governança (responsável/comitê)
- Use *checklists* e *gates* de aprovação para atividades com IA (criativo, mídia, atendimento, pesquisa)
- Não trate “bom senso” como política: sem diretrizes, as equipes variam e o risco aumenta
- Não permita escolha de ferramentas sem triagem mínima (segurança, privacidade, PI)
- Realize treinamentos periódicos e se atente à atualização de práticas e materiais
- Ao elaborar uma Política de IA no Marketing, abordar: escopo e objetivos; papéis e aprovações; regras de dados e informações permitidas; ferramentas homologadas e proibições; transparência ao público; requisitos de revisão humana e *checklists*; rastreabilidade e retenção de evidências; gestão de incidentes; treinamento e atualização periódica

6.4 Seleção e homologação de ferramentas

Homologar ferramenta é validar, antes do uso, se ela é adequada ao risco da campanha e aos requisitos do anunciante (segurança, privacidade, Propriedade Intelectual, transparência e rastreabilidade). Na prática, isso significa aprovar previamente quais sistemas podem ser usados, exigir avaliações compatíveis com a complexidade da campanha e garantir mecanismos de rastreabilidade (data, *prompt*, *logs*, versão do modelo) e revisão humana.

CHECKLIST MÍNIMO DE HOMOLOGAÇÃO (EXEMPLO)

Critério	O que checar/registrar
Finalidade	Para que a ferramenta será usada (criativo, mídia, atendimento etc.) e quais limites
Dados de entrada	Se haverá dados pessoais/confidenciais; regras de anonimização; proibições
Treinamento com *prompts*	Se há opção de desabilitar uso de *prompts*/*inputs* para treino; configuração padrão
Segurança	Controles (acesso, MFA, *logs*, criptografia), evidências (ISO/SOC2 quando disponível)
PI e licenças	Direitos sobre *outputs*; limites de uso de bases/treino; documentação de origem/licenças quando aplicável e proporcional ao risco; previsões contratuais com o fornecedor sobre declarações, garantias e indenização em caso de violação de direitos de terceiros
Transparência	Se a ferramenta permite rótulo/metadado/*watermark* quando necessário
Rastreabilidade	Data, *prompt*, *log* de geração, versão do modelo, responsável, aprovações
Disponibilidade	Garantias sobre a disponibilidade do sistema e existência de SLA

SUGESTÃO PRÁTICA

Manter um inventário interno de ferramentas (nome, fornecedor, finalidade aprovada, responsável, riscos mapeados e data da última revisão).

6.5. *Gate* de governança antes do *go-live*

Como desdobramento prático das diretrizes acima, recomenda-se que campanhas com uso de IA passem, antes do *go-live*, por um *gate* formal de governança, proporcional ao risco do caso de uso, com participação integrada das áreas de marketing, jurídico, privacidade e compliance, sem prejuízo do envolvimento de outras áreas quando necessário.

Esse *gate* deve funcionar como um ponto mínimo de validação antes da publicação, para confirmar se a campanha atende aos requisitos de conformidade, integridade, transparência, rastreabilidade e resposta a incidentes compatíveis com o seu nível de risco.

O *gate* não deve ser tratado como formalidade burocrática, mas como mecanismo de coordenação mínima entre áreas, apto a assegurar consistência decisória, *accountability* e pronta resposta em caso de correção, retirada de conteúdo ou incidente.

6.6 Fluxo operacional com IA (*end-to-end*)

Um fluxo *end-to-end* deve definir etapas, revisões obrigatórias, evidências a guardar e prazos para correção/remoção, além de prever níveis claros de revisão humana antes da publicação e registro das revisões/aprovações e SLA para correções, retificações e retirada de conteúdo quando houver risco.

O fluxo abaixo é um mínimo operacional. Ele permite que IA seja usada com eficiência sem perder rastreabilidade, revisão e prontidão para correção. Os *gates* devem ser ajustados conforme risco (ver item 4.8 – proporcionalidade deste guia).

Etapa	Controle mínimo	Responsável primário
1. *Briefing* e escopo	Definir finalidade, público, canais e limites de IA	Anunciante e Agência
2. Triagem de risco	Classificar uso (baixo/médio/alto) e requisitos de *disclosure*	Agência (com validação do anunciante)
3. Seleção de ferramenta	Usar ferramenta homologada e configuração adequada	Agência / Fornecedor e Anunciante (aprovação)
4. Preparação de inputs	Checar dados pessoais, segredos e PI; aplicar políticas	Agência
5. Geração/produção	Registrar *prompts*/versões e parâmetros relevantes	Agência e Fornecedor
6. Revisão humana	Revisão criativa e jurídica proporcional ao risco	Agência e Anunciante
7. ***Gate* de governança antes do *go-live*** (*Clearance* e aprovações)	Direitos (PI/persona), *claims* e *disclosure* definidos; consolidação final das validações internas; revisão e aprovação prévia pelo anunciante antes da publicação ou veiculação de entregáveis gerados ou substancialmente alterados por IA, proporcional ao risco do conteúdo	Anunciante (decisão final) com validação das áreas internas competentes
8. Veiculação	Configurar segmentação/otimização e registrar mudanças	Agência
9. Monitoramento	Acompanhar performance, vieses, reclamações e anomalias	Agência e Anunciante
10. Encerramento	Guardar evidências e lições aprendidas; atualizar controles	Anunciante e Agência

6.7 Rastreabilidade e documentação

Rastreabilidade é a capacidade de reconstruir o como e o porquê de um conteúdo ou decisão: quais *inputs* foram usados, qual ferramenta/modelo, quem revisou e aprovou e quais controles foram aplicados. Em marketing, isso é crucial para demonstrar diligência, responder a reclamações e corrigir rapidamente problemas.

REGISTRO MÍNIMO POR CAMPANHA	PARA QUE SERVE
Caso de uso; ferramenta/modelo (nome, versão) e data	Identificar o que foi usado e quando
Responsáveis e aprovações (agência/anunciante)	*Accountability* e trilha de decisão
Insumos relevantes (fontes, bases, ativos criativos) e restrições	Controle de PI, confidencialidade e LGPD
Prompts/parâmetros essenciais e versões de peças geradas	Reprodutibilidade e investigação de incidentes
Decisão de *disclosure* (se aplicável) e justificativa	Evitar omissão material e *label fatigue*
Testes e validações realizadas (vieses, *claims*, qualidade)	Evidência de mitigação de risco
Logs operacionais relevantes (quando disponíveis)	Detecção de anomalias e auditoria

SUGESTÃO PRÁTICA

Se houver terceiros (agência/subfornecedor), prever obrigação contratual de manter e disponibilizar documentação em caso de questionamento.

6.8 Gestão de incidentes e resposta rápida

Incidentes em IA podem envolver: publicação de conteúdo enganoso ou discriminatório; violação de direitos (PI, imagem/voz); vazamento/exfiltração de informações em *prompts*; ou falhas de segurança do fornecedor.

Incidentes envolvendo IA nem sempre são “incidentes clássicos de dados pessoais”. Além de vazamentos e acessos indevidos (ver item 5.7 deste guia), é comum haver incidentes algorítmicos, reputacionais e de conteúdo (como *outputs* ofensivos, vieses, alucinações, uso indevido de avatares/personas sintéticas ou violações de direitos de personalidade). Diretrizes setoriais recomendam protocolos claros de resposta e documentação para reduzir dano e demonstrar diligência.

Tipo de incidente	Exemplos	Ações imediatas (primeiras horas)	Encaminhamento
Dados pessoais (LGPD)	Exposição de base, *prompt* com dados pessoais, acesso indevido	Conter (revogar acessos), preservar evidências, acionar DPO/segurança	Avaliar necessidade de notificação e medidas corretivas
Conteúdo e reputação	Peça ofensiva, estereótipos, *deepfake* sem autorização, voz/ imagem indevida	Pausar veiculação, remover/retificar, registrar versões, acionar jurídico e PR	Revisar processos, emitir esclarecimentos e reparar danos quando cabível
Algorítmico (vieses e decisões)	Segmentação excludente, otimização que reforça disparidades	Suspender regra/ modelo, investigar parâmetros e dados, testar correções	Atualizar critérios, monitorar e documentar medidas
Integridade informacional	Alucinação em chatbot, resposta indevida, claim incorreto	Interromper fluxo, corrigir base/*guardrails*, orientar atendimento	Revisão de conteúdo e validações; comunicar quando houver impacto
Terceiros e fornecedores	Mudança de termos, falha de serviço, vazamento no fornecedor	Acionar SLA, exigir notificação e plano de contenção, avaliar substituição	Auditar, ajustar contrato e controles; reportar internamente

A resposta deve ser rápida, com canal emergencial, prazos de notificação e um plano de ação inicial, incluindo retirada/correção e preservação de evidências.

CONDUTA RECOMENDADA

- Definir canal e responsáveis (marketing, jurídico, TI, DPO, PR) e realizar simulações periódicas
- Pausar rapidamente a campanha quando houver risco material; preservar evidências (versões, *prompts*, *logs*)
- Tratar incidentes de IA também como incidentes reputacionais e de conteúdo, com comunicação alinhada a stakeholders
- Executar pós-incidente ("*post-mortem*") e ajustar políticas, ferramentas e treinamento
- Não minimizar o incidente por ser "erro da IA" ou deixar a decisão apenas para "bom senso" individual
- Não aguardar confirmação total para agir quando houver risco de dano imediato ao consumidor
- Não apagar registros sem preservar evidências (prejudica correção, auditoria e defesa)
- Não reincidir no mesmo tipo de falha sem revisar controles e responsabilidades

Conclusão

A combinação de dados pessoais e IA é um dos principais motores de inovação do marketing — e, por isso, deve ser acompanhada de responsabilidade, transparência e governança efetiva. Este Guia de Boas Práticas reúne conceitos, casos de uso, princípios, riscos e salvaguardas com foco em aplicação prática, para apoiar anunciantes, agências, plataformas e fornecedores na adoção de IA de forma útil para o mercado e consistente com a proteção de consumidores, titulares de dados e direitos de terceiros.

Mais do que um guia conceitual, este conteúdo foi concebido como instrumento de governança e diligência do anunciante. Ele pode ser utilizado para estruturar políticas internas, definir papéis e responsabilidades, orientar fluxos de aprovação, estabelecer critérios objetivos de transparência/*disclosure* e registrar evidências mínimas de conformidade. Também serve como referência em processos de contratação, homologação e avaliação de fornecedores, traduzindo expectativas de conduta em cláusulas, checklists e rotinas verificáveis.

A implementação real depende de compromissos mínimos: definir finalidades e limites, manter supervisão humana, garantir rastreabilidade, promover transparência quando relevante e operar com prontidão para corrigir falhas e incidentes. Ao adotar essas rotinas, a cadeia publicitária fortalece confiança, reduz risco regulatório e reputacional e cria condições para que inovação e conformidade avancem juntas.

Nesse sentido, o Guia de Boas Práticas também apoia o diálogo qualificado com autoridades e stakeholders, demonstrando boas práticas de autorregulamentação efetiva e disposição para aprimoramento contínuo.

Por fim, trata-se de um instrumento vivo: orienta o presente e deve ser atualizado à medida que práticas, tecnologias e referências regulatórias evoluírem.

Sobre a ABA

A ABA (Associação Brasileira de Anunciantes) é uma entidade sem fins lucrativos, fundada em 1959, que reúne e representa as maiores empresas anunciantes do Brasil, responsáveis por cerca de 70% dos investimentos em propaganda realizados no País. A entidade foi criada para representar, defender interesses comuns e contribuir para a contínua evolução e profissionalização das empresas anunciantes.

Sua atuação tem como missão central o advocacy, com foco na defesa da liberdade de comunicação social, na representação, defesa e orientação dos anunciantes brasileiros e no diálogo permanente com a sociedade e seus diversos atores. A Entidade também é fundadora e integrante do CONAR, reforçando a centralidade da autorregulamentação como instrumento de integridade e confiança na publicidade. No cenário internacional, a ABA integra o Conselho Executivo da WFA (World Federation of Advertisers), conectando a agenda brasileira às melhores práticas globais.

Por meio de fóruns técnicos e grupos de trabalho — como o GT de Inteligência Artificial e GT de Privacidade e Proteção de Dados — a ABA desenvolve princípios, guias e iniciativas para fortalecer a autorregulamentação setorial e apoiara inovação responsável no marketing e na publicidade.

Sobre o VLK

O VLK é uma boutique de Direito Digital, Proteção de Dados, Cibersegurança, Inteligência Artificial e Legal Marketing, movida por entregas que fazem a diferença.

No VLK, o Direito não é barreira. É impulso para inovar, para viabilizar negócios e para construir uma sociedade mais próspera e justa, conciliando: risco e oportunidade; complexidade e clareza; e proteção e progresso. Participamos ativamente da construção de marcos regulatórios e atuamos em inúmeros projetos inovadores e estratégicos, o que nos permite antecipar tendências e gerar segurança jurídica.

Entre os profissionais do escritório que contribuíram com este Guia, destacamos:

- Rony Vainzof – Sócio
- Gisele Karassawa – Sócia
- Mariana Carlucci – Advogada
- Jean Santana – Advogado

APOIO:

ALMAP BBDO

globo

Unilever

ASSOCIAÇÃO BRASILEIRA DE ANUNCIANTES

2030: O futuro passa por aqui.

Associação Brasileira de Anunciantes
aba.com.br
comunicacao@aba.com.br
+55 11 3283-4588

bit.ly/facebook-aba
instagram.com/abatransformar/
bit.ly/linkedin-aba

Filiada à WFA
World Federation of Advertisers

WFA World Federation of Advertisers

wfanet.org
info@wfanet.org
+32 2 502 57 40

youtube.com/wfamarketers
linkedin.com/company/wfa