UNIVERSIDADE FEDERAL DE OURO PRETO

Departamento de Direito

Walerson Duarte da Silva

RESPONSABILIDADE CIVIL E PRESTAÇÃO DE CONTAS NAS PRÁTICAS DE PUBLICIDADE DO GOOGLE ADS SOB A PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Ouro Preto

2025

WALERSON DUARTE DA SILVA

RESPONSABILIDADE CIVIL E PRESTAÇÃO DE CONTAS NAS PRÁTICAS DE PUBLICIDADE DO GOOGLE ADS SOB A PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Monografia apresentada ao Curso de graduação em Direito da Universidade Federal de Ouro Preto como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Roberto Henrique Pôrto Nogueira.

Ouro Preto

2025

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO

FOLHA DE APROVAÇÃO

Walerson Duarte da Silva

Responsabilidade civil e prestação de contas nas práticas de publicidade do Google Ads sob a perspectiva da Lei Geral de Proteção de Dados (LGPD)

Monografia apresentada ao Curso de Direito da Universidade Federal
de Ouro Preto como requisito parcial para obtenção do título de Bacharel em Direito

Aprovada em 03 de setembro de 2025.

Membros da banca:

Dr. Roberto Henrique Pôrto Nogueira – Orientador e Avaliador (Universidade Federal de Ouro Preto)
Dra. Juliana Evangelista de Almeida – Avaliadora (Universidade Federal de Ouro Preto)
Mestranda Maria Paula Correia Ramos – Avaliadora (Programa de Pós-Graduação em Direito - Mestrado Acadêmico – UFOP)

Dr. Roberto Henrique Pôrto Nogueira, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 04/09/2025.

Documento assinado eletronicamente por **Roberto Henrique Porto Nogueira**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 04/09/2025, às 20:21, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0973602** e o código CRC **7EDA0FE5**.

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35402-163
Telefone: (31)3559-1545 - www.ufop.br

RESUMO

A presente monografia investiga a intersecção entre as práticas de publicidade digital, especificamente através da plataforma Google Ads, e as exigências impostas pela Lei Geral de Proteção de Dados Pessoais (LGPD), com foco na responsabilidade civil e na prestação de contas por anunciantes. O problema central da pesquisa reside em identificar as boas práticas de conformidade com a LGPD identificáveis na política de tratamento de dados do Google Ads, tendo em vista a segmentação de anúncios personalizados e os direitos de titulares de dados pessoais. A metodologia empregada combina uma abordagem teórico-dogmática, com análise da legislação, com aplicação a estudo de caso, qual seja, o da plataforma Google Ads, examinado suas políticas e funcionalidades. O objetivo geral, portanto, é investigar a eventual adoção coerente de práticas de segmentação de anúncios do Google Ads para o propósito de atendimento às exigências da LGPD. Os objetivos específicos incluem: analisar as diretrizes da LGPD sobre responsabilidade e prestação de contas na publicidade digital; avaliar as práticas atuais no uso do Google Ads e sua conformidade com a LGPD; identificar os desafios na implementação de práticas que respeitem a LGPD em campanhas de anúncios personalizados; e propor recomendações práticas para aprimorar a conformidade. A justificativa para este estudo ancora-se na crescente relevância da publicidade digital para a economia, na preocupação jurídico-social com a proteção de dados pessoais, na necessidade de supervisão e regulação efetivas e no fomento ao debate acadêmico sobre tecnologia, privacidade e responsabilidade civil. Espera-se, como resultado, consolidar um conjunto de boas práticas que viabilizem a conformidade do tratamento de dados pessoais no contexto do Google Ads, equilibrando os interesses publicitários com a proteção dos diretos dos titulares de dados pessoais, no sentido de práticas mais éticas e responsáveis.

Palavras-chave: Google Ads; Lei Geral de Proteção de Dados; Prestação de contas; Publicidade; Responsabilidade Civil.

ABSTRACT

This monograph investigates the intersection between digital advertising practices, specifically through the Google Ads platform, and the requirements imposed by the General Law for the Protection of Personal Data (LGPD), with a focus on civil liability and accountability for advertisers. The central research problem lies in identifying the best practices for LGPD compliance that are identifiable in Google Ads' data processing policy, considering the segmentation of personalized ads and the rights of data subjects. The methodology employed combines a theoretical-dogmatic approach, with an analysis of the legislation, applied to a case study of the Google Ads platform, examining its policies and functionalities. The general objective, therefore, is to investigate the coherent adoption of ad segmentation practices by Google Ads for the purpose of meeting LGPD requirements. The specific objectives include: analyzing the LGPD guidelines on accountability and liability in digital advertising; evaluating current practices in the use of Google Ads and their compliance with the LGPD; identifying the challenges in implementing practices that respect the LGPD in personalized ad campaigns; and proposing practical recommendations to improve compliance. The justification for this study is anchored in the growing relevance of digital advertising to the economy, the legal and social concern with the protection of personal data, the need for effective supervision and regulation, and the promotion of academic debate on technology, privacy, and civil liability. As a result, it is expected to consolidate a set of best practices that enable compliance in the processing of personal data within the context of Google Ads, balancing advertising interests with the protection of the rights of data subjects, towards more ethical and responsible practices.

Keywords: Google Ads; General Data Protection Law; Accountability; Advertising; Civil Liability.

SUMÁRIO

1. INTRODUÇÃO

A transformação digital reconfigura as estratégias publicitárias, conferindo aos entes privados exploradores de atividade econômica a aptidão de atingir seus públicos-alvo com uma precisão sem precedentes. Neste contexto, os dados pessoais tornam-se ativos elementares, sendo pilares de um mercado condicionado à sua análise e gerência (Bioni, 2021, p.12).

Todavia, essa evolução suscita questões jurídicas, notadamente que tange à privacidade e à proteção de dados pessoais, demandando dos atores envolvidos no ecossistema digital a adoção de medidas coordenadas e robustas para assegurar a transparência, a segurança e a legalidade no tratamento dessas informações. Nesse cenário, a publicidade direcionada, impulsionada por algoritmos e pela coleta massiva de dados comportamentais, emerge com uma ferramenta poderosa, mas que, simultaneamente, acende alertas quanto aos seus potenciais impactos sobre os direitos fundamentais dos indivíduos.

No contexto jurídico brasileiro, a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 14 de agosto de 2018, representa um divisor de águas, estabelecendo um marco abrangente e detalhado para o tratamento de dados pessoais por pessoas naturais e jurídicas, de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde os dados sejam tratados, desde que a operação de tratamento seja realizada no território nacional, a atividade de tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional, ou dos dados pessoais objeto do tratamento tenham sido coletados no território nacional.

A LGPD impõe princípios, direitos dos titulares e deveres aos agentes de tratamento (controlador e operador) que reverberam diretamente nas práticas publicitárias, exigindo-se um novo paradigma de responsabilidade tanto por parte dos anunciantes quanto das plataformas que veiculam os anúncios. Entre estas, o Google Ads, uma das mais proeminentes e utilizadas ferramentas de publicidade digital em escala global, assume um papel central, uma vez que sua operacionalidade intrinsecamente se baseia na segmentação precisa de usuários, frequentemente fundamentada em dados do comportamento, preferências e outras características do perfil (Aliceda, 2021, p. 123).

Diante dessa conjuntura, a presente pesquisa se propõe investigar a eventual adoção coerente de práticas de segmentação de anúncios do Google Ads para o propósito de atendimento às exigências da LGPD. O problema fundamental que norteia este estudo pode ser sintetizado na seguinte questão: quais são as boas práticas de conformidade com a LGPD

identificáveis na política de tratamento de dados do Google Ads, tendo em vista a segmentação de anúncios personalizados e os direitos de titulares de dados pessoais?

A hipótese subjacente é que, apesar dos desafios inerentes à implementação das diretrizes da LGPD no dinâmico ambiente da publicidade digital, especialmente no que concerne à transparência, à obtenção de consentimento válido e à minimização do tratamento de dados, é factível, por meio de uma pesquisa jurídico-exploratória, fundamentada na análise das políticas operacionais do Google Ads e nas normativas da LGPD, consolidar um conjunto de boas práticas que viabilizem a conformidade do tratamento de dados pessoais, de maneira a analisar as posturas documentalmente adotadas para a promoção de equilíbrio entre a eficiência publicitária e a proteção dos direitos dos titulares.

Através de uma abordagem teórico-dogmática, são examinadas as práticas de segmentação de anúncios no Google Ads, avaliando sua adequação às normas estabelecidas pela LGPD, com o propósito de levantar boas práticas empregadas ou empregáveis na articulação de dados pessoais. Inicialmente, são analisadas as determinações da LGPD concernentes à responsabilidade e à prestação de contas no âmbito da publicidade digital, com ênfase nos princípios que regem o uso de dados pessoais em anúncios segmentados. Ao final, são discutidas as práticas da plataforma e sua aptidão para aprimorar a conformidade transversalizada entre os atores do ecossistema de publicidade digital envolvidas no processo em apreço.

De forma progressiva, há uma condução do tema com início nos fundamentos conceituais, abordando-se surgimento da publicidade direcionada e a responsabilidade civil aplicável aos anunciantes. Em seguida, faz-se o exame da LGPD e seus reflexos na publicidade digital, descrevendo os direitos dos titulares de dados, os limites da segmentação e as exigências de governança.

O estudo dedica-se, ainda, a uma análise detalhada do Google Ads, para avaliar sua conformidade com a LGPD, suas políticas de segmentação e os riscos de responsabilização civil.

Por fim, discutem-se a prestação de contas e a governança nas campanhas publicitárias, para examinar e discutir o potencial de boas práticas para contratantes, com medidas técnicas, protocolos administrativos e transparência.

A relevância deste estudo, no âmbito econômico, é decorrente do fato de que a publicidade digital, especialmente em plataformas como o Google Ads, desempenha papel de relevo no atual mercado de anúncios, influenciando as decisões de consumo e impulsionando o crescimento empresarial. A conformidade com a LGPD, nesse contexto, não é apenas uma

exigência legal, mas também um fator para a construção de um ambiente comercial competitivo, mas juridicamente estruturado. No plano social, a proteção de dados pessoais é preocupação crescente, e a aplicação da LGPD às práticas publicitárias digitais pode adjuvar na privacidade de titulares na promoção da confiança e da transparência nas relações entre fornecedores e consumidores. Além disso, a LGPD representa marco na evolução das políticas de proteção de dados no Brasil, e a análise da interação entre as práticas de publicidade e essa legislação reforça a necessidade de um controle robusto sobre o uso de informações pessoais. Do ponto de vista acadêmico, a pesquisa oferece um escorço nas implicações legais da LGPD sobre as práticas publicitárias, com o objetivo de compreender e elucidar o arcabouço jurídico, ampliar a conscientização sobre a responsabilidade no tratamento de dados pessoais e contribuir para o desenvolvimento do direito digital no Brasil, fomentando o debate sobre tecnologia, privacidade e responsabilização civil.

2. PUBLICIDADE DIRECIONADA E SEGMENTADA

A virtualização da informação trouxe impactos nas demasiadas formas de relações, sobretudo as de consumo. Uma consequência lógica deste contexto é a transformação nas estratégias adotadas pelos fornecedores para identificar, alcançar e angariar consumidores, em um cenário de competitividade globalizado. Conforme explicita Pavanelli (2020, p.15), o contexto representa um limiar entre o desafio e oportunidade para as empresas na busca por destaque no mercado digital, mercado este que ultrapassa as características do meio físico, em virtude de suas constantes inovações e da complexidade atrelada ao modelo. A forma interconectada de oferecer mais produtos por interações cada vez mais simples possui um aparato denso e elaborado.

A nova forma de relações consumerista possui como característica intrínseca a aglutinação de todos os processos que envolvam prestação de serviços, compra e venda nos meios digitais. Os dispositivos, tais como smartphones computadores substituem os recursos físicos e humanos necessários para atração de conversão de clientes. Contudo, o sucesso de uma empresa nessa cadeia de consumo é interdependente das informações que possua sobre seu público e seus concorrentes. O fácil acesso ao público desassociado a fatores geográficos possibilita o alcance de consumidores mais distante, mas também permite que outras empresas o façam, amplificando ainda mais a competição do mercado. Para otimização deste processo, o ato de segmentar, isto é, dividir o mercado em grupos com características e interesses comuns, possibilita que o comprador e o vendedor firmem sua relação de maneira eficaz e com menores esforços publicitários.

No que concerne à publicidade, conforme Kotler[1] (2021, *apud* Pavanelli, 2022, p.17), é atividade qual busca a satisfação dos desejos e necessidades por meio da relação entre empresa e cliente. Em caráter contínuo, Sant'Anna, Rocha Junior e Garcia[2] (2016, p. 67, *apud* Trevisan *et al.*, 2020, p.77) trazem a qualificação da publicidade através da etimologia da palavra, designando a qualidade do que é público, isto é, tornar público um fato ou uma ideia. Ainda, Pavanelli (2022, p.17) destaca a evolução do conceito, ampliando cada vez o que venha a ser. A evolução tecnológica trouxe incursão na transformação, qual veio a ser mais acelerada e multifacetada. Transforma-se o perfil do consumidor e o mercado de consumo, quais objetivam a praticidade e facilidade em seu relacionamento. A publicidade digital é o fator essencial neste

[1] KOTLER, Philip. **Marketing Para o Século XXI**: Como criar, conquistar e dominar mercados. 1. ed. Rio de Janeiro: Alta Books, 2021.
[2] SANT'ANNA, A.; ROCHA JÚNIOR, I.; GARCIA, L. F. D. **Propaganda**: teoria, técnica e prática. 9. ed. São Paulo: Cengage Learning, 2015.

vínculo, com diferencial competitivo frente à capacidade de mensuração e sincronia que o ambiente on-line favorece.

Um dos grandes pilares para as estratégias de publicidade são as redes sociais, as quais são estruturas sociais formadas por indivíduos e organizações conectadas por múltiplos tipos de interdependências, como amizades, interesses comuns e relações profissionais, que se manifestam e se amplificam no ambiente online (Pavanelli, 2022, p.19). O comportamento humano e a forma com que as empresas se relacionam com o seu público associam-se através destas plataformas, que mais do que um ambiente de conexão, tornam-se instrumento do mercado publicitário. A forma com a qual as redes sociais aproximam titulares de dados e agentes de tratamento permite construir e engajar uma rede de seguidores e clientes, sendo as estratégias publicitarias determinadas não só pelo produto ofertado, mas pela forma de utilização do ambiente virtual pelo público-alvo, qual é destrinchado através de seu comportamento no ambiente digital.

Uma estratégia adotada para otimização das ações publicitárias é o tráfego pago. Esta estratégia auxilia na conexão entre os agentes de tratamento e o titular de dados, qual é estabelecida por meio de anúncios pagos em outras plataformas. Desta forma, um anunciante consegue atingir públicos diversos e segmentados com uma precisão inédita. Destaca-se que o sucesso da campanha publicitária está intimamente relacionado ao dispêndio que se impõe, de forma que quanto mais se investe nas plataformas anunciantes, maior o número de anúncios exibido e mais consumidores é atingido.

Ademais, uma inovação deste mercado digital é a publicidade direcionada. Através dela, os anúncios são exibidos a segmentos específicos de usuários a partir da coleta e análise de seus dados:

> Vale dizer que a publicidade se insere no movimento da chamada despersonalização das relações privadas. Trata-se de um método de abordagem que visa a alcançar uma gama de consumidores, difundindo informações de um objeto (produto) ou atividade (serviço) a um universo de pessoas (Bioni, 2021, p. 14).

Observa-se o distanciamento da publicidade de massa comum aos meios de comunicação televisivos por exemplo, os quais se direciona a publicidade a um número indiscriminado de pessoas. O ponto chave dessa modalidade publicitária é a precisão entre o anúncio e o indivíduo que recebe. Parte-se da análise tanto da característica quanto do comportamento do usuário, com fito em segmentar o público e direcionar o produto ao seu consumidor final. Enquanto a forma tradicional de anúncio demanda estratégias que equacione

consumidores em meio à multidão, a publicidade direcionada tem acurácia e otimiza os custos para conversão de clientes.

Neste contexto, a capacidade de segmentação detalhada confere à publicidade digital maior eficácia. A plataforma Google Ads, por exemplo, processa os emoticons utilizados pelo usuário e mídias digitais consumidas de forma a discernir as suas emoções para conversão de anúncios (Aliceda, 2021, p. 145). Para além do comportamento de usuário, fatores como idade, sexo, sexualidade, posição política, são capazes de proporcionar que seu algoritmo decida em tempo real qual campanha publicitária será exibida. Essa prática, embora apresentada como uma forma de "aprimorar a experiência do usuário" (Caribé, 2019, p.13) ao oferecer-lhe conteúdo e ofertas mais pertinentes, representa uma nova fronteira comercial composta de conhecimento sobre o comportamento em tempo real, que cria oportunidades sem precedentes para intervir e modificar o comportamento humano visando o lucro. A publicidade direcionada, portanto, mais que uma ferramenta eficiente, é a manifestação visível de uma nova lógica econômica baseada na extração e comercialização de dados pessoais.

A engrenagem que move a publicidade direcionada é a extração massiva e contínua de dados dos usuários, um processo multifacetado que ocorre, em grande parte, de forma invisível e sem pleno consentimento informado dos indivíduos. Essa coleta se dá por meio de diversas fontes e tecnologias. Em primeiro lugar, há as informações que os usuários fornecessem voluntariamente, como dados cadastrais, informações de perfil e conteúdo gerado ativamente. Contudo, a porção mais significativa dos dados é coletada de forma passiva, através do monitoramento das interações dos usuários com a plataforma e com a web em geral. Sobre estes dados, Zuboff (2015, p. 85) explicita serem "dados residuais", rastros comportamentais deixados pelos usuários a cada clique, curtida, compartilhamento, tempo de visualização de um vídeo ou rolagem de tela. Embora pareçam intangíveis e irrelevantes isoladamente, esses dados residuais, quando agregados e analisados em grande escala, permitem que as plataformas conheçam o usuário de forma profunda e íntima:

> O Google, Amazon e Facebook utilizam complexos algoritmos para intermediar as relações entre usuários e conteúdos. As transações mediadas por computador permitiram observar comportamentos que antes não eram observáveis, isto passa a permitir transações que não eram viáveis anteriormente, estabelecendo novos modelos de negócio. (Caribé, 2019, p.9)

Para além das interações dentro de seus próprios domínios, as plataformas utilizam tecnologias para monitorar a navegação dos usuários em outros sites. Quando um site ou blog utilizar o serviço do Google Ads, ele insere um código em sua página permitindo-lhes coletar informações sobre o conteúdo da página visitada, o tempo de permanência, os links clicados e

os produtos consultados (Caribé, 2019, p.7). O usuário, quando navega por várias páginas que utiliza este serviço, permite de maneira involuntária, que seja traçado um perfil detalhado de seus interesses e hábitos. Há vigilância do comportamento humano, de forma a transformar a conduta dos usuários em ativos financeiros. Conforme Zuboff (2015), as pessoas são reduzidas a uma mera “biomassa humana”, inclinadas a servir às novas regras do capital, impostas através de uma implacável relação algorítmica. A publicidade digital, nesse contexto, deixa de ser apenas uma forma de comunicação persuasiva para se tornar o principal vetor de um sistema que não apenas vende produtos, mas também vende os dados de seus usuários.

3. A LGPD E SEUS IMPACTOS NA PUBLICIDADE

3.1. Prerrogativas do titular de dados e limites para publicidade dirigida

A promulgação da LGPD institui uma reconfiguração do panorama jurídico brasileiro no que concerne ao tratamento de dados pessoais, transpondo um modelo até então fragmentado e setorial para um sistema normativo unificado e abrangente. O regramento tem cerne na proteção dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento humano. Tal premissa desloca o eixo do poder, conferindo ao indivíduo, agora denominado titular de dados, protagonismo e um conjunto robusto de prerrogativas para exercer controle efetivo sobre o fluxo de suas próprias informações. No contexto da publicidade digital, essa mudança de paradigma impõe limites claros e inafastáveis às práticas de mercado, notadamente à publicidade dirigida, que se fundamenta na coleta e análise massiva de dados para a segmentação e personalização de anúncios. As estratégias de publicidade, que por décadas operaram sob uma lógica de extração irrestrita de dados, agora se deparam com a necessidade imperativa de se adequar a um arcabouço legal que privilegia a autodeterminação informativa.

Para a devida compreensão da extensão e da profundidade do regime imposto pela LGPD, é imprescindível delimitar o objeto central de sua tutela: o dado pessoal. A legislação estabelece, em seu artigo 5º, inciso I, uma definição ampla e tecnologicamente neutra, segundo a qual dado pessoal consiste em toda "informação relacionada a pessoa natural identificada ou identificável". Esta conceituação abrange, de um lado, as informações que permitem a identificação direta de um indivíduo. Por outro lado, e de forma ainda mais relevante para o ecossistema digital, a definição alcança as informações que tornam uma pessoa natural "identificável". Neste campo, inserem-se os dados que, isoladamente ou em conjunto com outras informações, são capazes de singularizar um indivíduo em meio a uma coletividade. Tais elementos, quando agregados e analisados por algoritmos, no contexto da publicidade digital, permitem a construção de perfis comportamentais detalhados, tornando possível não apenas identificar um usuário específico, mas também inferir seus hábitos, interesses e vulnerabilidades, o que os qualifica inequivocamente como dados pessoais e os submete integralmente ao rigor normativo da LGPD.

A autodeterminação informativa está contida na LGPD como um dos fundamentos que disciplina a proteção de dados no Brasil. Compreende-se por ela, o arbítrio do titular de dados em decidir sobre o uso, coleta e armazenamento destes ativos, como expressão do desenvolvimento de sua personalidade (Bioni, 2021, p. 98). O art. 2º da LGPD em que este fundamento está disposto ainda elenca um conjunto de pilares que devem ser observado no contexto da publicidade digital. A análise desses fundamentos revela que a lei não busca a

supressão de atividades econômicas, mas sim sua harmonização com os direitos do titular de dados (Almeida; Soares, 2022, p. 30-31). Entre eles, o respeito à privacidade (inciso I), à inviolabilidade da intimidade, da honra e da imagem (inciso IV) formam o núcleo de proteção do indivíduo.

A privacidade, no contexto da LGPD, se relaciona ao direito do indivíduo de proteger os seus próprios dados. A esfera proteção dos ativos dos titulares tem interferência direta da publicidade comportamental, ao criar perfis detalhados e inferir preferências e vulnerabilidades. Quando essa segmentação se baseia em inferências sobre condições de saúde, situação financeira, orientação sexual ou opiniões políticas, mesmo que a partir de dados não sensíveis, ela pode levar à estigmatização ou à exploração de vulnerabilidades, tangenciando a violação da honra e da imagem do indivíduo.

Por outro lado, a lei também protege a livre iniciativa, a livre concorrência e a defesa do consumidor (Art. 2º, V). A publicidade é uma expressão da livre iniciativa e um pilar da concorrência, permitindo que empresas alcancem seus clientes e disputem o mercado. Contudo, a LGPD condiciona esse direito à defesa do consumidor, o que significa que a livre iniciativa não é absoluta e não pode sobrepor-se à proteção contra práticas abusivas ou à falta de informação clara. A controvérsia jurídica sobre o uso de marcas de concorrentes como palavras-chave no Google Ads, muitas vezes vista como concorrência desleal, exemplifica como a livre iniciativa encontra barreiras na proteção de outros direitos.

A LGPD não hierarquiza esses fundamentos, exigindo uma ponderação em cada caso concreto. A compatibilização entre livre iniciativa e privacidade não se dá com a proibição da publicidade segmentada, mas com sua adequação às regras da lei. Uma campanha que preza pela transparência, baseada em consentimento livre e informado ou em legítimo interesse ponderado, e que evita discriminação, harmoniza o exercício da livre iniciativa com a proteção da dignidade humana.

Essa harmonização redefine o sucesso de uma campanha publicitária. O êxito não deve ser medido apenas por métricas de conversão e retorno sobre o investimento, mas precisa incorporar a conformidade ética e legal como um indicador-chave de desempenho. A longo prazo, marcas que constroem relações de confiança, tratando os dados dos consumidores com respeito, tendem a conquistar uma vantagem competitiva sustentável.

Quanto às prerrogativas dos titulares de dados, o legislador, no artigo 18 da lei 13.709 de 2018 (LGPD), constituiu um núcleo central da proteção conferida, representando as ferramentas jurídicas pelas quais o indivíduo pode exercer sua soberania informacional:

> **Art. 18.** O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> **I -** confirmação da existência de tratamento;
> **II -** acesso aos dados;
> **III -** correção de dados incompletos, inexatos ou desatualizados;
> **IV -** anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> **V -** portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> **VI -** eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> **VII -** informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> **VIII -** informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> **IX -** revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

O direito à confirmação da existência do tratamento e o direito de acesso aos dados, dispostos nos incisos I e II respectivamente, são basilares na medida que garantem a transparência necessária para que o titular possa compreender quais informações as empresas, incluindo anunciantes e plataformas, detêm a seu respeito, como foram obtidas e para quais finalidades são utilizadas, incluindo a criação de perfis para o direcionamento de publicidade. Igualmente fundamental, é o direito à correção de dados incompletos, inexatos ou desatualizados, conforme inciso III, que permite ao indivíduo zelar pela qualidade e veracidade do perfil comportamental que lhe é atribuído. Contudo, é no direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei (inciso IV) que reside um dos mais potentes limites à publicidade dirigida. Por meio dessa prerrogativa, o titular pode requerer ativamente a exclusão de seu histórico de navegação, de seus interesses inferidos e de outros dados que alimentam os algoritmos de segmentação, desfazendo, na prática, o perfil publicitário construído para si. O inciso VI traz direito com o mesmo potencial, ao passo que a eliminação dos dados pessoais tratados com o consentimento do titular, associada com a revogação do consentimento do inciso IX, permite que o usuário desfaça autorização previamente concedida para recebimento de comunicação publicitária. Em caráter contínuo, o inciso VII lança luz sobre a complexa cadeia de atores, coibindo práticas de comercialização indiscriminada de informações.

A eficácia dessas prerrogativas se materializa nos limites que a LGPD impõe diretamente às operações de tratamento de dados para fins publicitários, que agora devem, obrigatoriamente, se amparar em uma das bases legais previstas em seu artigo 7º:

> **Art. 7º** O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> **I -** mediante o fornecimento de consentimento pelo titular;
> **II -** para o cumprimento de obrigação legal ou regulatória pelo controlador;

> **III -** pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> **IV -** para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> **V -** quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> **VI -** para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> **VII -** para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> **VIII -** para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> **IX -** quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> **X -** para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A base legal do consentimento foi redefinida, exigindo uma manifestação livre, informada e inequívoca por parte do titular. Oliveira (2021, p. 21) destaca que o preceito elimina a prática do "soft opt-in", onde a pessoa era informada das comunicações que receberia, com o campo de autorização já preenchido, como uma forma de consentimento genérico e embutido em longos termos de serviço. A legislação agora demanda um consentimento granular e específico para a finalidade publicitária, o que autora conceitua como "hard opt-in", havendo o titular de confirmar expressamente a autorização. Essa exigência eleva o padrão para a construção de bases publicitárias, tornando-as potencialmente menores, porém mais qualificadas, uma vez que será composta por indivíduos genuinamente interessados na comunicação da marca. Alternativamente, a base legal do legítimo interesse, descrita no inciso IX, surge como uma opção mais flexível, mas demanda do controlador uma análise de ponderação criteriosa. Há para isso, o "Teste de Legítimo Interesse" (ou LIA – Legitimate Interest Assessment), ferramenta utilizada para avaliar se o tratamento de dados pessoais com base no legítimo interesse é válido e justificado sob a LGPD. Este teste, conforme detalhado por Bioni, Kitayama e Rielli (2021), desdobra-se em quatro fases essenciais: a verificação da legitimidade da finalidade; a análise da necessidade do tratamento, aplicando o princípio da minimização para utilizar apenas os dados estritamente necessários; o balanceamento entre os interesses da empresa e os direitos e liberdades fundamentais do titular, avaliando-se as suas legítimas expectativas; e, por fim, a implementação de salvaguardas, notadamente a transparência e a garantia de um mecanismos de oposição fácil e acessível para o titular, para caso deseje, não receba mais publicidade do anunciante.

Ademais, a LGPD estabelece um conjunto de princípios que devem nortear toda e qualquer atividade de tratamento, e que funcionam como barreiras adicionais à publicidade.

Ressalta-se o princípio da finalidade disposto no artigo 6º, inciso I, qual veda o chamado desvio de finalidade, impedindo que dados coletados para um propósito específico, como a execução de um contrato, sejam posteriormente utilizados para marketing sem uma nova base legal e a devida informação ao titular. Frente a este princípio, a prática de grandes empresas de tecnologia de combinar bases de dados de diferentes serviços para criar um perfil publicitário torna-se questionável, dada a dificuldade em justificar a necessidade de tal combinação e a ausência de mecanismos de oposição (Bioni; Kitayama; Rielli, 2021, p. 59). Ainda, o princípio da não discriminação, contido no inciso IX do artigo 6º, proíbe que o tratamento de dados seja realizado para fins discriminatórios, ilícitos ou abusivos, o que impõe um limite ético à segmentação que possa resultar na exclusão de determinados grupos do acesso a ofertas, créditos ou oportunidades. Ademais, o tratamento de dados pessoais sensíveis, como origem racial, convicções políticas e religiosas ou dados de saúde, recebe, conforme o artigo 11, proteção ainda mais rigorosa, de forma que se exige o consentimento específico e destacado do titular, o que praticamente inviabiliza seu uso para publicidade geral, restringindo severamente o escopo da segmentação baseada em características íntimas do indivíduo. A soma dessas prerrogativas e limites transforma a publicidade digital, demandando dos anunciantes responsabilidade, transparência e respeito pela autonomia do titular dos dados. A conformidade com a LGPD deixa de ser mera obrigação legal para se tornar um diferencial competitivo, capaz de construir confiança e fortalecer o relacionamento entre marcas e consumidores em uma sociedade da informação cada vez mais consciente de seus direitos.

A legislação, ciente do potencial discriminatório e dos riscos elevados associados a certas categorias de informações, estabeleceu um regime jurídico especial e mais rigoroso para os denominados dados pessoais sensíveis. O legislador os definiu de forma taxativa no artigo 5º, inciso II, da LGPD, como sendo o "dado pessoal sobre 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". A simples posse ou inferência de um dado sensível por um agente de tratamento já acarreta um risco intrinsecamente maior, justificando a imposição de salvaguardas e requisitos legais mais estritos para qualquer operação que os envolva, desde a coleta até a eliminação.

Dada a sua natureza delicada, o tratamento de dados pessoais sensíveis é regido por um rol de hipóteses legais mais restritivo, previsto no artigo 11 da LGPD, que se sobrepõe e limita as bases legais mais amplas do artigo 7º. A regra geral, estabelecida no inciso I do artigo 11, é que o tratamento somente pode ocorrer "quando o titular ou seu responsável legal consentir, de

forma específica e destacada, para finalidades específicas". Esta exigência qualificada de consentimento representa uma barreira significativa. A manifestação de vontade deve ser "específica", vinculada a um propósito claro e determinado, inviabilizando autorizações genéricas. Ademais, deve ser "destacada", o que impõe ao controlador o ônus de apresentar a cláusula de consentimento de maneira apartada das demais disposições contratuais ou termos de uso, garantindo que o titular tenha plena ciência e deliberação sobre a autorização que está concedendo para o uso de suas informações mais íntimas. Essa dupla qualificação do consentimento torna sua obtenção para fins publicitários uma tarefa complexa e de alto risco jurídico.

Para além do consentimento, o artigo 11, em seu inciso II, elenca as situações excepcionais em que o tratamento de dados sensíveis pode ocorrer sem a autorização do titular. Incluem-se nesse rol o cumprimento de obrigação legal ou regulatória pelo controlador (alínea “a”); o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (alínea “b”); a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis (alínea “c”); o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral (alínea “d”); a proteção da vida ou da incolumidade física do titular ou de terceiro (alínea “e”); a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária (alínea “f”); ou a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (alínea “g”). A análise dessas exceções demonstra seu caráter de necessidade e interesse público ou de proteção, distanciando-se por completo da lógica de mercado que orienta a publicidade.

3.2. Diretrizes de boas práticas e estruturas de governança previstas na LGPD

A instituição de um regime de governança em privacidade transcende a mera observância de um conjunto de regras prescritivas, representando, em sua essência, a internalização de uma cultura de proteção de dados que permeia toda a estrutura organizacional do agente de tratamento. Este paradigma, fundamentado na responsabilidade proativa e na prestação de contas, constitui um dos pilares mais inovadores e desafiadores da LGPD. Em um cenário digital caracterizado pela crescente complexidade das operações de tratamento e pela assimetria informacional entre os agentes e os titulares de dados, a governança emerge não apenas como um requisito de conformidade, mas como um diferencial estratégico para a

construção de confiança e a mitigação de riscos reputacionais e financeiros. A própria inserção de termos como governança, mitigação de riscos e accountability no vernáculo jurídico, impulsionada pela LGPD, sinaliza uma mudança de postura que vai além de um modismo passageiro, incentivando a implementação efetiva de novas técnicas de gestão e conformidade, uma vez que o tratamento ético de dados pessoais representa, na atualidade, um direito fundamental das pessoas (Ladeira Garbaccio; Lubieska, 2024, p. 157).

A noção de governança historicamente associada à gestão de Estado e corporações, adquire contornos específicos e multifacetados no contexto da Internet e do tratamento de dados. Kurbalija (2016, p.20) traz a sua definição a respeito do tema:

> Governança na Internet é o desenvolvimento e a aplicação pelos Governos, pelo setor privado e pela sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomadas de decisão e programas em comum que definem a evolução e o uso Internet.

A concepção do autor expande a compreensão para além da ação governamental, consonante com a LGPD quando convoca todos os agentes de tratamento a assumirem um papel ativo na criação de um ambiente seguro e transparente para os dados pessoais. A transição de um modelo de controle centralizado para um de governança distribuída e colaborativa reflete a própria na natureza do ambiente online (Kurbalija, 2016, p.35), e a LGPD importa essa lógica para o ambiente de cada organização que trata dados. Esta necessidade de governança é acentuada pela percepção contemporânea de que os dados se tornam um dos ativos mais valiosos, sendo frequentemente comparados ao petróleo ou mesmo ao urânio da era digital, dada a sua capacidade de, uma vez refinados, gerar valor imenso e, se mal gerenciados, representam um perigo significativo para o ecossistema de negócios e para indivíduos (Ladeira Garbaccio; Lubieska, 2024, p. 161). A seção II do Capítulo VII da lei, intitulada “Das Boas Práticas e da Governança”, materializa essa visão ao delinear os contornos do que se espera de um programa de governança em privacidade robusto e eficaz.

O artigo 50 da LGPD se apresenta como o núcleo desta nova abordagem, estabelecendo que os controladores e operadores “poderão formular regras de boas práticas e governança”. A utilização do verbo “poderão” indica a natureza, a princípio, voluntária da adoção de tais programas. Contudo, uma análise sistêmica da lei revela que esta facultatividade é matizada pela sua centralidade no sistema de responsabilidade e fiscalização. A existência de um programa de governança é um critério atenuante na aplicação de sanções administrativas, conforme disposto no artigo 52, §1º, inciso VIII. Mais do que isso, a implementação de tais regras é a manifestação concreta dos princípios da prevenção e da responsabilização e prestação

de contas, previsto no artigo 6º, incisos VII e X, respectivamente. Este último princípio, em particular, encapsula a essência do novo regime de "responsabilidade proativa", que exige do agente não apenas o cumprimento formal da lei, mas a "demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"(Bodin de Moraes, 2019, p. 5). Assim, o que se apresenta como uma faculdade converte-se, na prática, em um elemento indispensável para a demonstração de conformidade e boa-fé por parte do agente de tratamento. A própria lei, em seu §1º do artigo 50, orienta que o estabelecimento dessas regras deve levar em conta a natureza, o escopo, a finalidade do tratamento, bem como a probabilidade e a gravidade dos riscos e benefícios decorrentes para o titular, consolidando uma abordagem baseada em risco que é fundamental para a governança moderna. A convergência entre a proteção de dados e outras obrigações de transparência, é reforçada por essa estrutura, por uma governança de dados bem implementada "torna mais fácil o atendimento de pedidos à informação" e materializa "os princípios da eficiência e transparência na administração pública" (Bioni; Silva; Martins, 2022, p.12, 18).

O parágrafo 2º do artigo 50 detalha, em seu inciso I, os elementos mínimos que devem compor um programa de governança em privacidade, oferecendo um verdadeiro roteiro para os agentes de tratamento. A alínea "a" exige que o programa "demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais". Isso significa que a governança deve ser um compromisso institucional, endossado pela alta administração e não relegado a um mero exercício formal de um departamento isolado. A materialização desse programa ocorre por meio da produção de políticas, códigos, termos, treinamentos, registros de evidências e outros documentos, com sistemática adequada e proporcional ao porte da empresa ou ao órgão público (Ladeira Garbaccio; Lubieska, 2024, p. 158). A alínea "b", por sua vez, determina que o programa seja "aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta", exigindo uma visão completa do ciclo de vida dos dados na organização. Essa visão integral é complementada pela alínea "c", que demanda que o programa seja "adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados", afastando a ideia de soluções padronizadas e impondo uma análise customizada e proporcional à realidade de cada agente. Este conjunto de requisitos iniciais estabelece a base para uma governança que é, ao mesmo tempo, abrangente, comprometida e proporcional.

A dimensão proativa e preventiva da governança é aprofundada nas alíneas seguintes. A alínea d do mesmo dispositivo legal estabelece a necessidade de o programa possuir "políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade". A alínea “e” foca na relação com o titular, determinando que o programa "tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular". Este ponto conecta a governança interna à percepção externa de transparência e respeito, elementos fundamentais para a legitimação das atividades de tratamento e para a redução da assimetria informacional que historicamente marca a relação entre empresas e cidadãos (Bioni; Silva; Martins, 2022, p. 11). A integração do programa à "estrutura geral de governança" da organização, com o estabelecimento de "mecanismos de supervisão internos e externos", conforme a alínea “f”, reforça que a proteção de dados não é um silo, mas uma disciplina transversal que deve dialogar com outras áreas, como compliance, segurança da informação e gestão de riscos.

Finalmente, as alíneas “g” e “h” do inciso I do § 2º do artigo 50 fecham o ciclo da governança com a exigência de "planos de resposta a incidentes e remediação" e a obrigação de que o programa seja "atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas”. Isso consolida a governança não como um projeto com início, meio e fim, mas como um processo contínuo de avaliação, aprendizado e aprimoramento, em linha com os ciclos de melhoria contínua. A capacidade de responder a incidentes de forma rápida e eficaz, e de adaptar o programa às novas ameaças e mudanças no ambiente regulatório ou de negócios, é a prova final da maturidade de uma estrutura de governança. Kurbalija (2016, p. 40) destaca a importância de uma abordagem holística para a governança da Internet, que deve ser flexível e capaz de se adaptar a um cenário em constante mudança, princípio este que a LGPD aplica diretamente à governança de dados. A própria lei, no § 3º do artigo 50, prevê que essas regras de boas práticas poderão ser reconhecidas e divulgadas pela autoridade nacional, criando um sistema de incentivo e validação que pode culminar em selos e certificações, servindo como um atestado público de conformidade e responsabilidade. Este novo sistema de responsabilização dito “proativo” representa uma mudança paradigmática, pois não basta mais que as empresas simplesmente forneçam um conjunto de documentos formais. Elas devem ser capazes de provar que avaliaram e redesenharam seus processos, que as medidas de segurança são eficazes e que existe uma política de privacidade interna com responsabilidades claras e devidamente atribuídas (Bodin de Moraes, 2019, p. 5).

Complementando o artigo 50, o artigo 51 da LGPD atribui à Autoridade Nacional um papel de fomento, estipulando que "a autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares de seus dados pessoais". Este dispositivo, embora conciso, é de grande importância, pois sinaliza o compromisso do legislador com a promoção de tecnologias que empoderam o titular de dados. A atuação da autoridade na definição desses padrões e na promoção de sua adoção é fundamental para que a governança não se restrinja a documentos e políticas internas, mas se traduza em ferramentas e interfaces que permitam ao titular exercer, de fato, sua autodeterminação informativa. Em suma, a Seção II do Capítulo VII da LGPD não apenas descreve o que é uma boa governança, mas estabelece um ecossistema de responsabilidade compartilhada, onde agentes de tratamento são incentivados a se autorregular, com ação da autoridade como validadora e fomentadora, e o titular é colocado no centro do processo, com mecanismos para participar e controlar o uso de seus dados. A implementação efetiva dessas diretrizes é, portanto, o caminho para que a proteção de dados pessoais deixe de ser um mero discurso e se torne uma prática viva e pulsante no tecido social e econômico do país.

4. GOOGLE ADS: PUBLICIDADE DIRIGIDA E DESAFIOS JURÍDICOS

4.1. Políticas de uso e estrutura de segmentação de anúncios

O exame da plataforma Google Ads em seu aspecto fundamental exige a dissecação de suas políticas de uso e de sua estrutura de segmentação de anúncios que a sustenta, elementos determinantes da avaliação de sua conformidade (coerência) com a LGPD e a maneira com a qual absorve e registra compromissos pertinentes à responsabilização civil. A ferramenta se estabelece como um dos proeminentes serviços de links patrocinados, de forma a estabelecer publicidade direcionada concebida para que haja o encontro e o reconhecimento entre as marcas, produtos e serviços dos fornecedores com seus respectivos clientes e internautas. A sua capacidade de "agenciar confiança ao e-commerce e fomentar negociação online" (Aliceda, 2021, p. 6) reside na convergência entre a pesquisa realizada pelo usuário na web e a apresentação de anúncios diretamente vinculados à expressão digitada. Esta ferramenta, em sua essência, materializa a publicidade direcionada ao permitir que anunciantes paguem para seus links de vendas, sítios eletrônicos ou páginas pessoais sejam exibidos em posição de destaque nos terminais dos internautas que realizam pesquisas por palavras, frases ou termos específicos. O objeto declarado da plataforma, conforme seus Termos de Uso, é inserir materiais publicitários e tecnologia em qualquer conteúdo de propriedade do Google ou de seus parceiros, utilizando ferramentas automatizadas para formatar os anúncios no que se configura como uma vasta plataforma de publicidade (Google, *s.d.*). Sua dominância no mercado global é inquestionável, com estimativas que apontam sua participação em cerca de 94% das buscas no Brasil, o que a torna um parâmetro incontornável para o estudo da publicidade digital e suas implicações jurídicas (Aliceda, 2021, p. 135).

Para regular este complexo ecossistema, o Google Estabelece um conjunto de diretrizes e políticas com o objetivo de manter uma plataforma de publicidade "saudável, transparente e confiável para usuários, anunciantes e publishers" (Google, *s.d.*). Essas políticas são estruturadas em quatro áreas abrangentes, que governam o conteúdo e as práticas permitidas na rede. A primeira área, denominada "Conteúdo Proibido", veta de forma explícita a promoção de produtos falsificados, que imitam marcas registradas; produtos ou serviços perigosos, como drogas recreativas, armas e materiais explosivos; produtos ou serviços que viabilizam comportamento desonesto, como softwares de invasão ou serviços de fraude acadêmica; e conteúdo considerado inadequado, que promova ódio, intolerância, discriminação, violência ou que apresente conteúdo chocante.

A segunda área, referente a "Práticas Proibidas", coíbe na rede de publicidade, como a promoção de conteúdo com malware e o uso de técnicas para ocultar o destino real dos usuários;

a deturpação, que inclui a omissão de informações relevantes sobre faturamento ou a apresentação de ofertas que não estão efetivamente disponíveis; e, de maneira crucial para a presente análise, a coleta e uso irresponsável de dados. Neste ponto, a política determina que seus parceiros não devem usar informações pessoais de modo inadequado nem realizar a coleta para fins "pouco claros ou sem medidas apropriadas de segurança ou divulgação" (Google, *s.d.*), citando como exemplos a coleta de informações de cartão de crédito em servidor não seguro e promoções que afirmem conhecer a orientação sexual ou a situação financeira de um usuário.

A terceira área de regulação abrange os "Conteúdos e Recursos Restritos", que, embora permitidos, são submetidos a limitações rigorosas devido à sua natureza jurídica ou culturalmente sensível. Anúncios de conteúdo sexual, por exemplo, são exibidos de forma, limitada com base na idade do usuário e na legislação local, sendo vedado o seu direcionamento a menores de idade. De maneira similar, a promoção de bebidas alcoólicas e de jogos de azar é permitida apenas em países específicos e para públicos que não incluam menores, exigindo que os anunciantes obtenham certificação adequada. Conteúdos relacionados à saúde e medicamentos, bem como conteúdo político, também são submetidos a restrições e requisitos específicos de cada localidade.

A quarta e última área diz respeito aos "Requisitos Editoriais e Técnicos", que estabelecem padrões de qualidade para os anúncios e páginas de destino. Exige-se que os anúncios sejam claros, com aparência profissional e que direcionem os usuários para conteúdos relevantes e de fácil navegação, proibindo, por exemplo, a utilização de URLs de visualização que não correspondam à página de destino ou sites que desativem funcionalidades básicas do navegador, como o botão "Voltar". Este arcabouço normativo é fiscalizado por uma combinação de inteligência artificial e avaliação humana, com aplicação de medidas que vão desde a reprovação de anúncios até a suspensão de contas em casos de violações graves ou repetidas (Google, *s.d.*).

A estrutura de funcionamento do Google Ads, por sua vez, é fundamentada em um sistema de leilão de palavras-chave, operando sob o modelo "Pay-Per-Click" (PPC), no qual o anunciante paga apenas quando um usuário efetivamente clica em seu anúncio (Aliceda, 2021, p.126). O processo se inicia com a criação de uma conta e a definição de uma campanha publicitária, na qual o anunciante estabelece suas metas, o público-alvo, a área geográfica de alcance e o orçamento. O elemento central da campanha é a seleção de palavras-chave, que podem ser termos simples ou frases complexas, escolhidas para se conectarem com as buscas dos potenciais clientes. É imprescindível ressaltar a autonomia concedida ao anunciante neste

processo: a plataforma oferece ferramentas como o “Keyword Planner” para sugerir termos relevantes, mas a decisão final sobre quais palavras utilizar, incluindo aquelas que podem remeter a marcas de concorrentes, pertence exclusivamente ao anunciante. O Google, em sua arquitetura padrão, não realiza um filtro prévio ou edita as palavras-chave escolhidas, mantendo uma posição de neutralidade quanto ao conteúdo do anúncio e à estratégia de segmentação adotada pelo usuário (Aliceda, 2021, p. 139). Essa liberdade operacional é um ponto nevrálgico na análise da responsabilidade civil, pois desloca o protagonismo da criação do conteúdo publicitário para o próprio anunciante.

Para além da segmentação baseada em palavras-chave, a eficácia do Google Ads é potencializada pela análise de comportamento do usuário. A plataforma emprega algoritmos para processar uma vasta gama de dados, como os “emoticons” utilizados em comunicações, as mídias consumidas e o histórico da navegação, com o fito de inferir as emoções e os interesses do indivíduo e, assim, decidir em tempo real qual campanha publicitária será mais eficaz (Aliceda, 2021, p. 145). Fatores demográficos como idade, gênero e localização, bem como informações sobre filiação política ou orientação sexual, podem ser utilizados para refinar ainda mais a segmentação, inserindo a plataforma na lógica da “economia afetiva”, que busca explorar fundamentos emocionais humanos para influenciar a decisão de consumo. Ciente das implicações dessas práticas, especialmente após a vigência da LGPD, o Google afirma em sua documentação pública que oferece termos contratuais de proteção de dados e controle de produtos que podem ser utilizados pelos anunciantes como parte de suas próprias estratégias de conformidade. A empresa informa ter consolidado as obrigações da LGPD em seus termos de proteção de dados, buscando alinhar seus compromissos com a legislação brasileira (Google, 2023). No entanto, a plataforma reitera que a responsabilidade pela adequação à lei, incluindo o uso correto das ferramentas de conformidade oferecidas, recai sobre o anunciante, que deve buscar orientações jurídica para tal finalidade. Essa dinâmica, que combina uma sofisticada estrutura de processamento de dados com uma política de transferência de responsabilidade pela conformidade, estabelece um cenário complexo e desafiador para a aplicação da LGPD, cujos contornos e riscos de responsabilização serão explorados na seção seguinte.

A materialização dessa análise comportamental se dá por meio de um robusto arsenal de ferramentas de monitoramento e direcionamento, cujos recursos técnicos são capazes de vigiar os passos dos usuários na internet, registrando não apenas a frequência e a quantidade de acessos, mas também os sites visitados, a fim de arquivar preferências e construir perfis detalhados. Dentre as tecnologias disseminadas, destacam-se os cookies, que, conforme a doutrina, consistem em arquivos de texto armazenados no computador do usuário a partir do

primeiro acesso a um sítio eletrônico, com a capacidade de reter dados como códigos de identificação, senhas e o histórico de atividades e consumo dentro daquele ambiente digital (Generoso; Silva; Nogueira, 2022, p. 395). Embora concebidos com a função primária de notificar o site sobre o retorno do usuário para personalizar a experiência, seu emprego massivo na publicidade digital transformou-os em instrumentos de vigilância, permitindo o mapeamento da personalidade do indivíduo. A partir da compilação e do cruzamento dessas minúcias, as plataformas publicitárias não apenas inferem interesses comerciais, mas também podem deduzir informações sensíveis, erigindo um panorama de conhecimento que restringe o campo de visão do usuário àquilo que lhe é estrategicamente apresentado, em um ciclo de retroalimentação informacional que serve aos interesses do anunciante.

A sofisticação dessas tecnologias de rastreamento vai além dos cookies convencionais, abrangendo um aspecto amplo e, por vezes, invasivo de mecanismos. Há diferentes tipos de cookies, como os de sessão, que são temporários, e os permanentes, que subsistem na máquina do usuário mesmo após o término da navegação. Imperioso discernir cookies de primeiros e terceiros no contexto da publicidade direcionada, onde estes últimos são originados por domínios distintos daquele que o usuário está visitando, geralmente inseridos por empresas de publicidade para rastrear a navegação do indivíduo através de múltiplos sites, consolidando um perfil de interesses abrangente (Generoso; Silva; Nogueira, 2022, p. 400). Adicionalmente, existem tecnologias ainda danosas, como os denominados flash cookies ou supercookies, que se destacam por sua capacidade de armazenar um volume significativamente maior de informações, operar em diferentes navegadores e resistir aos mecanismos de exclusão tradicionais, podendo inclusive restaurar cookies que o usuário havia deliberadamente apagado. A esse arsenal somam-se os identificadores de publicidade (advertising IDs), empregados em ambientes onde os cookies não são aplicáveis, como em dispositivos móveis, garantindo a continuidade do rastreamento e da perfilização do usuário independentemente da plataforma utilizada (Generoso; Silva; Nogueira, 2022, p. 401).

O ecossistema da publicidade digital é composto por uma tríade de atores principais, cujos papéis e responsabilidades são distintos, mas interdependentes, e uma falha de conformidade em um dos elos da cadeia pode comprometer a legalidade de toda a operação. O anunciante é a entidade que deseja promover seus produtos ou serviços, sendo o "comprador" de mídia com o objetivo de alcançar um público-alvo específico para gerar resultados de negócio (Adbutler, 2021). No contexto da LGPD, o anunciante é quem define a finalidade da campanha e o público a ser atingido, qualificando-se como o Controlador dos dados pessoais tratados para aquele fim. O publicador é o detentor do "inventário" publicitário, como um portal

de notícias, blog ou canal no YouTube, que busca monetizar seu conteúdo e audiência (Sani, 2025). Ele tem a responsabilidade de interagir com o usuário final para obter o consentimento para o uso de cookies e outras tecnologias de rastreamento. A plataforma, como o Google Ads, é o intermediário tecnológico que conecta anunciantes e publicadores, operando o sistema de leilão e processando os dados para segmentação. Seu papel sob a LGPD é complexo, podendo variar entre Operador e Co-controlador, dependendo da natureza do tratamento de dados. Essa estrutura tripartite cria uma cadeia de responsabilidades interligada, onde a legalidade da campanha de um anunciante pode depender do consentimento obtido por milhares de publicadores desconhecidos, gerando um risco sistêmico significativo.

A Plataforma fornece os "Termos de Tratamento de Dados de Publicidade do Google" formalizando contratualmente a relação de tratamento de dados, estabelecendo o objetivo de refletir o acordo entre as partes sobre como os "Dados Pessoais do Cliente" são gerenciados. Neste documento, os papéis são claramente definidos no contexto das legislações de proteção de dados: o Google atua como um "operador" dos dados pessoais, enquanto o cliente (anunciante) é designado como "controlador" ou, em alguns casos, como um operador que age em nome de outro controlador, conforme o tópico “5.1 Funções e Conformidade Regulatória; Autorização” (Google, 2024).

A política de uso de dados é estritamente delimitada pelas diretrizes do cliente. Os termos estipulam que o Google tratará os dados pessoais do cliente somente de acordo com as instruções documentadas. Tais instruções são fornecidas pelo cliente através do uso e da configuração dos próprios "Serviços de Operador", bem como por meio do contrato e outras comunicações escritas. O “Apêndice 1: Objeto e Detalhes do Tratamento de Dados” expõe que a natureza e a finalidade do tratamento se restringem à prestação dos serviços de publicidade e suporte técnico associado, envolvendo atividades como coleta, organização, combinação, armazenamento e exclusão de dados, conforme aplicável e instruído pelo anunciante. Essa estrutura contratual reforça que o Google age sob o comando do cliente, que detém a autoridade sobre o ciclo de vida dos dados na plataforma.

O Apêndice 1 ainda, se tratando da estrutura de segmentação, detalha que os dados pessoais processados pertencem a categorias específicas de titulares. Isso inclui indivíduos que foram ou serão alvo de publicidade online, pessoas que visitaram os sites ou aplicativos nos quais o cliente utiliza os serviços do Google, e clientes e usuários dos próprios produtos do anunciante. Essa definição contratual do escopo dos titulares de dados fornece a base para as operações de segmentação, confirmando que o perfil de público-alvo é construído a partir de

dados de indivíduos que interagem direta ou indiretamente com os ativos digitais do anunciante ou com a própria rede de publicidade do Google.

O Google também estabelece um conjunto de compromissos para garantir a segurança e a conformidade do tratamento de dados no tópico “7.1 Medidas e Assistência de Segurança do Google”. A empresa se compromete a implementar e manter medidas técnicas e organizacionais robustas, detalhadas no Apêndice 2 do termo, que incluem a criptografia de dados pessoais, a garantia de confidencialidade e resiliência dos sistemas, a capacidade de restaurar o acesso aos dados após um incidente e a realização de testes de eficiência regulares. Para demonstrar conformidade, o Google informa no tópico “7.4 Certificação de Segurança” que mantém a certificação ISO 27001. Além disso, em caso de violação de segurança que afete os dados do cliente (tópico"7.2 Incidente com Dados"), o Google se obriga a notificar o cliente sem atraso injustificado, fornecendo informações sobre a natureza do incidente e as medidas tomadas para mitigar os riscos.

4.2. Conformidade com a LGPD e riscos de responsabilização civil

A entrada em vigor da LGPD representou uma ruptura paradigmática com o modelo de responsabilidade civil anteriormente aplicado aos provedores de aplicação, notadamente aquele consolidado sob a égide do Marco Civil da Internet. Se antes a discussão se centrava na responsabilidade subjetiva do provedor condicionada ao descumprimento da ordem judicial de remoção de conteúdo (Aliceda; Texeira, 2021, p. 120), a LGPD institui um regime de responsabilidade solidária e, em grande medida, objetiva, que redefine drasticamente o mapa de riscos para anunciantes e para a própria plataforma Google Ads. Nesta seção, além de análise pormenorizada dos riscos de responsabilização civil, serão elucidados os mecanismos de imputação de responsabilidade e os parâmetros legais que regulam a reparação de danos aos titulares de dados afetados, considerando a intrincada teia de relações entre o anunciante (controlador), a plataforma (operadora ou, em certas hipóteses, controladora conjunta) e o titular dos dados.

A estrutura de responsabilidade civil inaugurada pela LGPD, detalhada em sua Seção III do Capítulo VI, afasta-se deliberadamente do modelo condicionado à culpa que caracterizava o regime anterior. O artigo 42 da Lei estabelece o alicerce deste novo sistema, ao prever que:

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

A amplitude do dispositivo é notável, abarcando não apenas os dados patrimoniais, mas também os de natureza extrapatrimonial, sejam eles individuais ou coletivos, o que denota a preocupação do legislador com as múltiplas dimensões em que o tratamento inadequado de dados pode afetar a pessoa humana. O parágrafo primeiro do mesmo artigo aprofunda o regime de responsabilidade ao definir as hipóteses de responsabilização solidária do operador, que responderá conjuntamente com o controlador quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador:

> **§ 1º** A fim de assegurar a efetiva indenização ao titular dos dados:
> **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, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> **II -** os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Essa disposição é de suma importância para a análise do ecossistema do Google Ads, pois significa que a plataforma, ao atuar como operadora, não está imune à responsabilização, devendo sua conduta estar em estrita conformidade tanto com a lei quanto as diretrizes do anunciante, sob pena de ser chamada a reparar os danos em conjunto com este. A responsabilidade do controlador, por sua vez, é inerentemente objetiva, pois decorre diretamente do exercício da atividade de tratamento que, por sua natureza, implica risco para os direitos dos titulares:

> O §1º do art. 42, ao destacar a efetiva indenização do dano, acha-se consentâneo com a clássica função reparatória da responsabilidade civil, que consagra a obrigação de indenizar qualquer dano injustamente causado com vistas à recomposição do equilíbrio desfeito ou alterado pelo dano. Atualmente, sustenta-se que a atenção da responsabilidade civil deve voltar-se à plena proteção da vítima e à total compensação do dano sofrido, atendendo a determinação constitucional de tutela prioritária à dignidade da pessoa humana. A partir da dicção dos incisos V e X do art. 5º da CF/88, busca-se preencher de significado o princípio da reparação integral em sede de direitos de danos, que deve ser conjugado a partir da perspectiva de múltiplas funções para a responsabilidade civil contemporânea, combinando dimensões repressivas (compensatórias e/ou punitiva) e proativas (preventiva) para o enfrentamento da crescente complexidade dos casos concretos, em especial daqueles que envolver o emprego de novas tecnologias (Martins; Longhi; Faleiros Júnior, 2024, p. 429).

Ciente das novas exigências legais, o Google tem empreendido esforços significativos para demonstrar sua conformidade e mitigar seus próprios riscos, posicionando-se como um parceiro tecnológico que oferece as ferramentas necessárias para que seus clientes (os anunciantes) possam, por sua vez, cumprir suas obrigações legais. Em sua documentação oficial, a empresa destaca o compromisso em obedecer às leis aplicáveis, incluindo a LGPD,

afirmando que atualizou seus termos de proteção de dados para consolidar as obrigações da legislação brasileira no corpo principal de seus acordos (Google, 2023). Essa padronização contratual visa criar um ambiente de segurança jurídica para suas operações globais. Ademais, o Google ostenta um robusto programa de segurança da informação, evidenciado por certificações internacionais como a ISO 27001 (Gestão de Segurança da Informação), ISO 27017 (Segurança na Nuvem) e ISO 27018 (Privacidade na Nuvem), que atestam a adoção de salvaguardas técnicas e organizacionais para proteger os dados processados em plataformas, incluindo o Google Ads (Google, 2023). A empresa também salienta a existência de um rigoroso programa de gerenciamento de incidentes, funcionando 24 horas, e o compromisso contratual de notificar seus clientes sem demora sobre incidentes que envolvam seus dados, em linha com as obrigações de comunicação previstas no artigo 48 da LGPD:

> **Art. 48.** O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Contudo, apesar de todo esse aparato de conformidade, a própria empresa deixa claro que a responsabilidade é compartilhada, aconselhando seus clientes a procurarem seus próprios advogados para determinar as medidas necessárias para a adequação à lei, o que evidencia que a plataforma se vê primordialmente como uma fornecedora de infraestrutura e ferramentas, recaindo sobre o anunciante a responsabilidade primária pelas decisões estratégicas de tratamento de dados (Google, 2023).

Neste contexto, os maiores riscos de responsabilização civil recaem, de fato, sobre os anunciantes, que na vasta maioria das operações realizadas via Google Ads, figuram como os controladores dos dados pessoais. É o anunciante quem define a finalidade do tratamento (por exemplo, aumentar as vendas de um produto específico), o público-alvo da campanha e a origem dos dados que serão utilizados para a segmentação. Quando uma empresa utiliza a funcionalidade de “Customer Match” (correspondência de clientes), fazendo o upload de uma lista de e-mails ou telefones de seus clientes para encontrá-los na rede do Google, ela está realizando uma operação de tratamento que demanda uma base legal robusta específica. Conforme aponta Faria (2023), é imperativo que a empresa tenha obtido o consentimento livre, informado e inequívoco desses titulares para essa finalidade específica de publicidade direcionada, ou que possa fundamentar o tratamento no legítimo interesse, após realizar a devida ponderação de riscos e direitos. A simples posse do dado, obtido para a finalidade de faturamento ou entrega de um produto, por exemplo, não autoriza, sob a ótica da LGPD e do princípio da finalidade, seu uso indiscriminado para publicidade. A empresa deve, portanto,

garantir total transparência, informando aos titulares, por meio de sua política de privacidade e de avisos claros no momento da coleta, que seus dados poderão ser compartilhados com plataformas como o Google para fins de publicidade personalizada, oferecendo-lhes a oportunidade de consentir ou se opor a tal tratamento (Faria, 2023). A falha em cumprir com esses deveres de transparência e de estabelecimento de uma base legal válida expõe o anunciante a um risco direto e substancial de responsabilização civil por eventuais danos, além de sanções administrativas por parte da ANPD.

O cenário se complexifica ao se considerar a solidariedade imposta pelo artigo 42 da LGPD, a qual cria uma interdependência de responsabilidades. Se um anunciante utiliza dados obtidos ilegalmente e causa dano a um titular, este poderá acionar judicialmente não apenas o anunciante (controlador), mas também o Google (operador). A defesa da plataforma provavelmente se basearia no artigo 43, II, da LGPD, que prevê a exclusão da responsabilidade quando o dano decorre de culpa exclusiva do titular ou de terceiro:

> **Art. 43.** Os agentes de tratamento só não serão responsabilizados quando provarem:
> [...]
> **II -** que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

Nesse caso, o Google poderia argumentar que a ilicitude na origem do tratamento foi ato exclusivo do anunciante (terceiro na relação entre a plataforma e o titular), e que a plataforma apenas executou as instruções recebidas. Todavia, a eficácia dessa defesa é incerta, pois os tribunais, orientados pelo princípio da reparação integral da vítima, podem entender que a plataforma, ao se beneficiar economicamente da atividade e ao deter um vasto poderio técnico, também possui um dever de vigilância e diligência que não pode ser completamente afastado. A solidariedade prevista na LGPD visa, primordialmente, garantir ao titular uma ampla possibilidade de reparação, permitindo-lhe demandar contra qualquer um dos agentes envolvidos na cadeia de tratamento que tenha contribuído para o evento danoso. Conforme lição doutrinaria, trata-se da decorrência onde concorrem para os fatos os múltiplos agentes envolvidos no tratamento de dados:

> As hipóteses descritas no §1º do art. 42 da LGPD asseguram ao titular dos dados, credor de uma indenização, o direito a exigir a receber de um ou de alguns dos devedores (controlador e operador, ou mais de um controlador, por exemplo), parcial ou totalmente, a dívida comum (Martins; Longhi; Faleiros Júnior, 2024, p. 430).

Portanto, a conformidade do Google Ads com a LGPD não depende apenas de suas próprias políticas e certificações, mas está intrinsecamente ligada à legalidade das práticas de

cada um dos milhares de anunciantes que utilizam seus serviços, criando um ecossistema de risco compartilhado e uma premência pela adoção de robusta prática de governança por parte de todos os envolvidos.

5. PRESTAÇÃO DE CONTAS E GOVERNANÇA NAS CAMPANHAS PUBLICITÁRIAS DO GOOGLE ADS

5.1. Responsabilidades e deveres de transparência nas campanhas segmentadas

A transição de uma economia industrial, centrada na produção de bens tangíveis, para uma economia pós-industrial e, subsequentemente, informacional, redefiniu o conceito de ativo de valor. Se outrora a terra e o capital fabril constituíam os principais motores da riqueza, hoje a informação e o conhecimento aplicado assumiram essa posição de protagonismo (Bioni, 2021, p. 4). A evolução tecnológica, notadamente a digitalização da informação da plataforma de átomos para a de bits, permitiu um processamento, armazenamento e transmissão de dados em uma escala e velocidade antes inimagináveis, virtualizando a informação e instaurando um novo padrão sócio-técnico-econômico (Bioni, 2020, p. 6-8).

Nesse novo paradigma, os dados pessoais emergiram como um ativo econômico de valor inestimável (Bioni, 2021, p. 12). A capacidade de coletar, processar e analisar informações sobre indivíduos, seus comportamentos, preferências e necessidades, tornou-se um fator crítico para a otimização de modelos de negócio em praticamente todos os setores. A dinâmica empresarial foi transformada, passando de modelos de produção em massa para sistemas flexíveis, capazes de se adaptar em tempo real às demandas do mercado. Empresas como a Zara, por exemplo, demonstram como o processamento de dados de vendas, retroalimentando o ciclo de design e produção, permite uma sintonia fina com os desejos dos consumidores, convertendo dados brutos em conhecimento estratégico aplicado (Bioni, 2021, p. 10). Essa lógica estende-se de maneira acentuada ao ambiente digital, onde as interações dos usuários geram um fluxo contínuo e exponencial de informações.

É nesse cenário que a figura do consumidor se transforma. De mero receptor passivo de produtos e mensagens, ele se torna um “prosumer”, um agente que simultaneamente consome e produz (Bioni, 2021, p. 13). Cada clique, cada busca, cada curtida em uma rede social, cada avaliação de produto é um ato de produção de dados valiosos (Bioni, 2021, p. 12). Essas informações, quando agregadas e analisadas, formam um rico retrato dos hábitos de consumo e das predileções individuais, permitindo que as empresas modelem não apenas seus produtos, mas também suas estratégias de comunicação e marketing de forma cirúrgica. A publicidade, consequentemente, abandona seu caráter estandardizado de comunicação em massa para adotar uma abordagem direcionada, que busca alcançar o indivíduo certo, com a mensagem certa, no momento certo (Bioni, 2021, p. 15). Este é o alicerce sobre o qual se ergue o ecossistema de plataformas como o Google Ads, cuja eficiência e rentabilidade estão intrinsecamente ligadas

à capacidade de segmentar audiências com base no vasto manancial de dados pessoais disponíveis.

A prevalência da publicidade comportamental está diretamente ligada ao modelo de negócio dominante na internet, conhecido como zero-price advertisement business model (Bioni, 2021, p. 23). Nesse arranjo, a grande maioria dos serviços e produtos digitais — redes sociais, mecanismos de busca, serviços de e-mail, portais de notícias — é oferecida aos usuários de forma aparentemente "gratuita", sem uma contraprestação pecuniária direta. A monetização não ocorre na transação entre a plataforma e o usuário, mas sim no mercado secundário, onde a atenção e os dados desse usuário são comercializados para anunciantes. O usuário, portanto, não é o cliente final, mas o produto, e a contraprestação pelo serviço recebido é o fornecimento contínuo de seus dados pessoais, que alimentam a engrenagem da publicidade direcionada (Bioni, 2021, p. 23).

Essa dinâmica subverte a relação bilateral tradicional do consumo, instaurando um ecossistema plurilateral e complexo (Bioni, 2021, p. 22). O fluxo de dados não se limita à interação entre o usuário e o website que ele visita. Por trás da interface visível, opera uma intrincada rede de atores que agem cooperativamente para a entrega da mensagem publicitária. As redes de publicidade (ad networks) conectam milhares de anunciantes (advertisers) a milhares de publicadores de conteúdo (publishers), gerenciando os espaços publicitários e o rastreamento dos usuários através de múltiplos sites (third-party tracking) (Bioni, 2021, p. 26). Essa prática permite a construção de perfis ainda mais ricos e abrangentes, que não se limitam ao comportamento do usuário em um único domínio (Bioni, 2021, p. 26).

A complexidade é amplificada pelas trocas de dados entre as próprias redes (ad exchanges) e pela atuação dos data brokers, empresas especializadas em agregar informações de inúmeras fontes, tanto online quanto offline, para criar, enriquecer e comercializar perfis detalhados de consumidores para as mais diversas finalidades (Bioni, 2021, p. 26). O resultado é um fluxo informacional abundante e de difícil mapeamento para o titular dos dados, que frequentemente desconhece a vasta gama de entidades que têm acesso às suas informações e as utilizam para fins comerciais (Bioni, 2021, p. 29). A percepção de que os mesmos anúncios "perseguem" o usuário por diferentes sites é um sintoma visível dessa arquitetura de vigilância distribuída. Essa opacidade e a multiplicidade de agentes envolvidos tornam a atribuição de responsabilidades e a garantia de transparência desafios centrais para a regulação, exigindo uma análise cuidadosa dos papéis de cada ator sob a égide da LGPD.

A LGPD instituiu um novo marco jurídico para o tratamento de dados pessoais no Brasil, estabelecendo um conjunto de princípios, direitos e deveres que incidem diretamente

sobre as práticas de publicidade segmentada. O objetivo da lei, conforme seu artigo 1º, é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Para tanto, o artigo 6º elenca dez princípios que devem nortear toda e qualquer operação de tratamento de dados, servindo como vetores interpretativos e balizas para a conduta dos agentes de tratamento.

O princípio da finalidade (art. 6º, I) exige que o tratamento seja realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sendo vedado o tratamento posterior de forma incompatível com essas finalidades. No contexto do Google Ads, isso significa que a coleta de dados para a segmentação de anúncios não pode ser justificada por finalidades genéricas como "melhorar a experiência do usuário". O anunciante e a plataforma devem ser capazes de especificar para quais campanhas ou tipos de segmentação os dados serão utilizados. O princípio da adequação (art. 6º, II) complementa o anterior, determinando que o tratamento deve ser compatível com as finalidades informadas. Já o princípio da necessidade (art. 6º, III) impõe a minimização dos dados, limitando o tratamento ao mínimo necessário para a realização de suas finalidades. Este princípio desafia diretamente a lógica do Big Data, que muitas vezes se baseia na coleta massiva de informações na expectativa de usos futuros ainda não determinados (Bioni, 2021, p. 229).

A transparência (art. 6º, VI) é um pilar central, garantindo aos titulares informações claras, precisas e facilmente acessíveis sobre o tratamento e os respectivos agentes. Não basta a existência de uma política de privacidade; esta deve ser compreensível e acessível, algo que, como demonstram estudos, raramente ocorre na prática (Bioni, 2021, p. 168). Os princípios da prevenção (art. 6º, VIII) e da segurança (art. 6º, VII) impõem aos agentes o dever de adotar medidas para prevenir a ocorrência de danos e para proteger os dados de acessos não autorizados e de situações acidentais ou ilícitas (Martins; Faleiros Júnior, 2020, p. 351). O princípio da não discriminação (art. 6º, IX) veda o tratamento de dados para fins discriminatórios ilícitos ou abusivos, uma preocupação especialmente relevante em práticas de perfilamento que podem levar à estigmatização ou exclusão de indivíduos (Vainzof, 2019, p. 161). Por fim, o princípio da responsabilização e prestação de contas (accountability), previsto no artigo 6º, X, exige que os agentes de tratamento demonstrem a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados (Flumignan; Flumignan, 2020, p. 137). Em conjunto, esses princípios formam uma malha de proteção que redefine as obrigações dos participantes do ecossistema de publicidade digital.

A efetiva atribuição de responsabilidades sob a LGPD depende da correta identificação dos papéis desempenhados pelos diferentes atores no tratamento de dados. A lei define duas

figuras centrais: o controlador (art. 5º, VI) e o operador (art. 5º, VII). O controlador, conforme o artigo 5º, VI, é a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais. O operador (art. 5º, VII) é aquele que realiza o tratamento em nome do controlador. A distinção é indispensável, pois ao controlador recai a maior parte das obrigações, incluindo a demonstração de conformidade, o atendimento aos direitos dos titulares e a responsabilidade primária por danos.

No ecossistema do Google Ads, essa definição se torna complexa e multifacetada. O anunciante — a empresa que contrata a plataforma para veicular suas campanhas — atua inequivocamente como controlador. É ele quem define a finalidade da campanha (promover um produto, gerar leads), o público-alvo (através da seleção de critérios de segmentação como interesses, demografia, comportamento) e, portanto, toma as decisões essenciais sobre o porquê e como os dados pessoais dos usuários serão tratados para aquele fim específico. A plataforma, por sua vez, pode atuar em diferentes capacidades. Em certas atividades, como o processamento técnico dos dados conforme as instruções diretas do anunciante para a exibição de um anúncio, o Google poderia ser visto como um operador.

Contudo, na maioria das situações, a plataforma transcende o papel de mero executor de ordens. O Google coleta dados de forma independente através de seus múltiplos serviços (Busca, YouTube, Gmail, Android), enriquece perfis de usuários e utiliza esses perfis para oferecer suas próprias ferramentas de segmentação e otimização de anúncios, definindo, assim, os meios e, em grande medida, as finalidades do tratamento que vão além das instruções de um anunciante específico. Nesse cenário, o Google também atua como controlador de um vasto ecossistema de dados. Frequentemente, a relação entre anunciante e plataforma se configura como uma controladoria conjunta (ou co-controladoria), prevista implicitamente na LGPD através da solidariedade na reparação de danos (art. 42, §1º). Nesta modalidade, dois ou mais controladores determinam conjuntamente as finalidades e os meios do tratamento. O anunciante decide quais perfis alcançar, e o Google, com base em seu próprio acervo de dados e algoritmos, decide como encontrar e impactar esses perfis, tornando-se ambos responsáveis perante o titular dos dados. Essa caracterização impõe a necessidade de um arranjo claro entre as partes para delimitar suas respectivas responsabilidades, especialmente no que tange ao fornecimento de informações e ao atendimento dos direitos dos titulares, solidificando a responsabilidade compartilhada no complexo fluxo da publicidade segmentada.

A LGPD estabelece, em seu artigo 7º, um rol de hipóteses que autorizam o tratamento de dados pessoais. Para as atividades de publicidade segmentada, duas bases legais se destacam como as mais pertinentes e, ao mesmo tempo, mais controversas: o consentimento e o legítimo

interesse. A escolha da base legal adequada é uma decisão fundamental do controlador e impacta diretamente o escopo do tratamento e os direitos do titular.

O consentimento, definido no artigo 5º, XII, como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", é a base legal historicamente associada à autodeterminação informacional. Contudo, a LGPD estabelece um padrão elevado para sua validade. A manifestação deve ser genuinamente livre, o que é questionável em ambientes digitais onde o acesso a serviços é frequentemente condicionado à aceitação de termos de uso que preveem a coleta de dados para publicidade, numa lógica de "pegar ou largar" que se assemelha mais a uma resignação do que a uma escolha autônoma (Bioni, 2021, p. 167). Deve ser informada, o que exige transparência sobre o complexo fluxo de dados no ecossistema publicitário, incluindo o compartilhamento com múltiplos parceiros, algo que as longas e obscuras políticas de privacidade raramente conseguem prover de forma eficaz (Bioni, 2021, p. 167). E deve ser inequívoca e para finalidades determinadas, invalidando autorizações genéricas e exigindo mecanismos claros de aceite, como caixas de seleção não pré-marcadas (Bioni, 2021, p. 190). A prática comum de cookie banners que induzem ao aceite ou dificultam a recusa dificilmente se sustenta sob uma análise rigorosa desses requisitos (Utz *et al*., 2019, p. 981).

Como alternativa, os agentes de tratamento podem recorrer ao legítimo interesse do controlador ou de terceiro (art. 7º, IX). Esta base legal permite o tratamento de dados sem o consentimento, desde que para finalidades legítimas e com base em situações concretas, e quando prevalecerem os direitos e liberdades fundamentais do titular. A sua aplicação, contudo, não é um cheque em branco. O artigo 10 da LGPD exige a realização de um teste de ponderação, conhecido como Relatório de Impacto à Proteção de Dados (no contexto europeu, LIA - Legitimate Interest Assessment), que deve balancear o interesse do controlador com as legítimas expectativas do titular e seus direitos (Bioni, 2021, p. 242-248). Embora a publicidade direta seja frequentemente citada como um exemplo de legítimo interesse, sua aplicação à publicidade comportamental, que envolve o monitoramento pervasivo, a criação de perfis detalhados e o compartilhamento de dados em larga escala, é altamente questionável. A expectativa razoável de um usuário que visita um site não necessariamente inclui ser rastreado por dezenas de terceiros desconhecidos por toda a internet (Bioni, 2021, p. 260). O impacto sobre a privacidade e o potencial para manipulação e discriminação são significativos, fazendo com que, em muitos casos, a balança penda em favor da proteção dos direitos do titular, tornando o legítimo interesse uma base legal de alto risco para as formas intrusivas de publicidade segmentada.

A efetivação do princípio da transparência, pilar da LGPD (art. 6º, VI), representa um dos maiores desafios para o ecossistema da publicidade segmentada. A complexidade do fluxo de informações, envolvendo uma miríade de atores, desde o anunciante, passando pela plataforma de anúncios como o Google Ads, até redes de publicidade e data brokers, torna a tarefa de fornecer informações "claras, precisas e facilmente acessíveis" (art. 6º, VI) uma empreitada hercúlea (Bioni, 2021, p. 142). A solução tradicionalmente adotada pelo mercado, a publicação de extensas e legalistas políticas de privacidade, tem se mostrado amplamente ineficaz. Estudos demonstram que os usuários raramente leem esses documentos, e, quando o fazem, a linguagem técnica e a extensão dos textos impedem uma compreensão real das práticas de tratamento de dados (Mcdonald; Cranor, 2008, p. 565). A sobrecarga de informação, paradoxalmente, gera desinformação e uma sensação de impotência que leva à resignação, em vez de uma tomada de decisão informada (Marzagão, 2005[3], p. 198, *apud* Bioni, 2021 , p. 185).

Para cumprir genuinamente com o dever de transparência, os agentes de tratamento precisam ir além do modelo estático das políticas de privacidade. A LGPD, em seu artigo 9º, detalha as informações que devem ser disponibilizadas ao titular, incluindo a finalidade específica do tratamento, a forma e a duração, a identificação do controlador e as informações sobre o uso compartilhado de dados. A implementação prática desse dever exige a adoção de mecanismos mais dinâmicos e amigáveis ao usuário, como painéis de controle de privacidade (privacy dashboards), onde o titular possa visualizar de forma centralizada quais dados estão sendo coletados, para quais finalidades e com quem são compartilhados, além de exercer seus direitos (Bioni, 2021, p. 186). Ferramentas como o "Minha Central de Anúncios" do Google representam um passo nessa direção, mas a transparência deve ser ainda mais granular, explicando não apenas os interesses inferidos, mas também as fontes de dados utilizadas para essa inferência. A utilização de notificações em camadas (layered notices) e avisos "just-in-time", que fornecem informações contextuais no momento da coleta do dado, são outras estratégias que podem tornar a informação mais digestível e relevante para o usuário, transformando a transparência de uma obrigação formal em uma ferramenta efetiva para o exercício da autodeterminação informacional (Kelley *et al*., 2009, p. 4-7).

A publicidade segmentada, em sua essência, baseia-se em decisões tomadas de forma automatizada. Algoritmos analisam o perfil de um usuário para decidir se ele se enquadra no público-alvo de uma campanha e, em sistemas de leilão em tempo real (real-time bidding), decidem automaticamente qual anúncio exibir e a que preço. Essas decisões, embora muitas

[3] MARZAGÃO, Nelcina C. de O. Tropardi. **Da informação e dos efeitos do excesso de informação no direito do consumidor**. 2005. Tese (Doutorado) – Universidade de São Paulo, São Paulo, 2005.

vezes percebidas como triviais, podem ter impactos significativos, influenciando os produtos e serviços aos quais um indivíduo é exposto, os preços que lhe são oferecidos (price discrimination) e até mesmo as informações e oportunidades que chegam ao seu conhecimento, podendo levar a práticas discriminatórias ilícitas (Bioni, 2021, p. 220).

Reconhecendo os riscos inerentes a essa prática, a LGPD, em seu artigo 20, confere ao titular o direito de "solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses" (Brasil, 2018). Essa disposição inclui as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito, ou os aspectos da personalidade do titular. A lei garante, ainda, o direito do titular a obter, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e procedimentos utilizados na decisão automatizada (Brasil, 2018). A operacionalização desse direito no contexto da publicidade digital é complexa. O que constitui uma "revisão" significativa de uma decisão que ocorre em milissegundos? Como fornecer uma explicação sobre a "lógica" de algoritmos complexos de machine learning sem revelar segredos comerciais e de uma forma que seja compreensível para o cidadão comum?

Apesar dos desafios, o direito à revisão impõe aos controladores, como anunciantes e plataformas, a obrigação de desenvolver mecanismos que permitam, no mínimo, que um ser humano reavalie os critérios que levaram à inclusão (ou exclusão) de um indivíduo em um determinado segmento de audiência. Exige, também, um nível de explicabilidade dos sistemas algorítmicos (algorithmic explainability), forçando as empresas a irem além dos modelos de "caixa-preta" e a serem capazes de auditar e justificar os resultados de suas decisões automatizadas (Bioni, 2021, p. 77). Essa obrigação de explicabilidade é um poderoso instrumento contra a discriminação, pois obriga os agentes a confrontarem os vieses que podem estar embutidos em seus dados e algoritmos, promovendo um tratamento de dados mais justo e responsável.

O princípio da responsabilização e prestação de contas (accountability), consagrado no artigo 6º, X, da LGPD, representa uma mudança de paradigma na regulação de privacidade (Brasil, 2018). Ele desloca o ônus da conformidade, exigindo que os agentes de tratamento não apenas cumpram a lei, mas sejam capazes de demonstrar o seu cumprimento (Flumignan; Flumignan, 2020, p. 137). Isso implica uma postura proativa na gestão da proteção de dados, que vai desde a implementação de políticas internas até a realização de auditorias e a manutenção de registros detalhados das operações de tratamento (Flumignan; Flumignan, 2020, p. 137).

No contexto de campanhas segmentadas, essa obrigação se materializa na necessidade de uma governança de dados robusta, compartilhada entre anunciantes e plataformas. Para atividades que apresentam alto risco aos direitos dos titulares, como a criação de perfis em larga escala ou o tratamento de dados sensíveis para segmentação, a LGPD exige a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme previsto no artigo 38 (Brasil, 2018). Esse relatório é uma ferramenta de gestão de riscos que obriga o controlador a descrever os processos de tratamento, avaliar a necessidade e a proporcionalidade da operação e identificar e mitigar os riscos aos direitos dos titulares (Alves, 2018, p. 186). A realização de um RIPD para campanhas de publicidade comportamental complexas torna-se uma prática essencial para demonstrar a devida diligência (Alves, 2018, p. 186).

Adicionalmente, a accountability se manifesta na adoção de medidas de segurança, técnicas e administrativas, aptas a proteger os dados (art. 46) (Martins; Faleiros Júnior, 2020, p. 350). A metodologia de privacidade desde a concepção (privacy by design) e por padrão (privacy by default), embora não explícita no texto da LGPD, é um corolário desses princípios. Ela preconiza que a proteção de dados deve ser integrada na concepção de tecnologias e modelos de negócio desde o início, e não adaptada posteriormente (Jimene, 2018, p. 174). Isso significa, por exemplo, que as plataformas de anúncios devem ser desenhadas para coletar o mínimo de dados necessários por padrão e oferecer aos usuários controles de privacidade granulares e fáceis de usar (Bioni, 2021, p. 191). A responsabilidade, portanto, não é apenas reativa, manifestando-se após um incidente de segurança, mas fundamentalmente preventiva, exigindo uma cultura de proteção de dados que permeie todas as etapas do ciclo de vida da informação no complexo e dinâmico ecossistema da publicidade digital (Martins; Faleiros Júnior, 2020, p. 351).

5.2. Implementação de boas práticas de governança em campanhas segmentadas

A arquitetura de negócios embasados na capacidade de coletar, processar e analisar dados pessoais para a segmentação de anúncios, intrinsecamente dependente do fluxo de informações pessoais, instaura uma tensão fundamental com os novos paradigmas jurídicos de proteção da pessoa humana. A LGPD impacta diretamente a operacionalização de ferramentas como o Google Ads, exigindo uma reavaliação das práticas de mercado e impondo a necessidade de estruturas de governança de dados que transcendam a mera conformidade formal (Faria, 2023). O antigo modelo, pautado em políticas de privacidade de difícil compreensão e em consentimentos genéricos, revela-se anacrônico e insuficiente diante de um arcabouço legal que preza pela autodeterminação informacional do titular dos dados.

Para compreender a profundidade das implicações da LGPD sobre as campanhas no Google Ads, é imperativo diagnosticar a reconfiguração socioeconômica impulsionada pela tecnologia digital, que reposicionou o dado pessoal como um ativo de primeira ordem. A transição de uma economia baseada em átomos para uma baseada em bits não apenas alterou os modos de produção, mas fundamentalmente transformou a natureza das relações de consumo e a própria percepção do indivíduo no circuito econômico (Bioni, 2021, p. 6). A "virtualização da informação" permitiu que as interações, preferências e comportamentos dos cidadãos fossem convertidos em dados passíveis de processamento, armazenamento e de monetização, estabelecendo as fundações para o que se convencionou chamar de "economia de vigilância".

Na economia da informação, o consumidor transcende seu papel passivo de mero receptor de bens e serviços. A interatividade das plataformas digitais, como redes sociais, blogs e fóruns, conferiu-lhe voz ativa, permitindo-lhe compartilhar experiências, avaliar produtos e influenciar as decisões de seus pares em uma escala antes inimaginável. Esse fenômeno, descrito por Bioni (2021, p. 13) com base na figura do prosumer, representa a fusão dos atos de produzir (production) e consumir (consumption), na medida em que o feedback e os dados gerados pelo consumidor retroalimentam e condicionam a própria confecção, distribuição e segmentação dos bens de consumo. As informações sobre hábitos, preferências, desejos e insatisfações, expressas direta ou indiretamente, tornam-se a matéria-prima para a inovação e para a otimização de estratégias comerciais, convertendo o dado pessoal em um fator vital para a engrenagem econômica.

Neste cenário, a observação contínua do comportamento dos indivíduos se consolida como um modelo de negócio em si, uma "economia de vigilância" na qual a geração de riqueza depende da extração e comodificação sistemática de informações pessoais (Bioni, 2021, p.12). Cada clique, cada busca, cada interação social é "datificada", gerando um dossiê digital que permite a construção de perfis detalhados. Essa biografia digital, por sua vez, torna o cidadão um "consumidor de vidro", cujas predileções e vulnerabilidades se tornam transparentes para os atores do mercado, que utilizam esse conhecimento para maximizar a eficiência de suas operações e, principalmente, de suas estratégias publicitárias.

O Google Ads, nesse contexto, posiciona-se como uma das mais sofisticadas e difundidas ferramentas para a materialização da economia de vigilância, sendo o principal motor da publicidade digital (Faria, 2023). A plataforma opera para além da publicidade meramente contextual, que correlaciona um anúncio ao tema de uma página, ou da segmentada, que se foca em características demográficas amplas. Seu maior diferencial reside na publicidade comportamental, uma prática que se utiliza de tecnologias de rastreamento, como os cookies,

para monitorar a jornada de navegação do usuário através de múltiplos websites e aplicações (Bioni, 2021, p. 15). Esse rastreamento persistente possibilita a inferência de interesses, intenções de compra e até mesmo de estados emocionais, permitindo que os anúncios sejam direcionados com uma precisão cirúrgica ao perfil do potencial consumidor.

A operacionalização dessa publicidade personalizada não se restringe à relação bilateral entre anunciante e Google. Ela é sustentada por um ecossistema complexo e opaco, composto por redes de publicidade (ad networks), bolsas de anúncios (ad exchanges) e corretores de dados (data brokers), que atuam de forma cooperativa para agregar e transacionar bases de dados, enriquecendo os perfis dos usuários e maximizando o alcance e a precisão das campanhas (Bioni, 2021, p. 25). Essa intricada rede de atores torna o fluxo informacional exponencialmente complexo, dificultando sobremaneira que o titular dos dados compreenda, e consequentemente controle, quem tem acesso às suas informações e para quais finalidades elas estão sendo utilizadas, um desafio central que a LGPD busca endereçar.

A LGPD ancora-se no fundamento da "autodeterminação informacional", que consagra o direito do titular de ter controle sobre o fluxo de suas informações pessoais (Bioni, 2021, p. 98). Esse paradigma se manifesta, primordialmente, através da exigência do consentimento como uma das bases legais centrais para o tratamento de dados. Contudo, a efetividade desse modelo é profundamente questionada quando confrontada com a realidade da economia de vigilância, marcada pela complexidade técnica, pela assimetria de poder e por vieses cognitivos que limitam a capacidade do indivíduo de exercer uma escolha verdadeiramente autônoma.

A LGPD estabelece requisitos rigorosos para a validade do consentimento, que deve ser uma manifestação livre, informada e inequívoca, para uma finalidade determinada (Faria, 2023). A intenção do legislador é garantir que o titular dos dados compreenda plenamente as implicações de sua autorização. Todavia, a arquitetura do mercado digital subverte essa premissa. A complexidade do ecossistema de publicidade do Google Ads, com seus múltiplos atores e fluxos de dados transfronteiriços, torna a tarefa de "informar" de maneira clara e completa uma quimera. O titular é confrontado com políticas de privacidade extensas, redigidas em linguagem jurídica e técnica, que obscurecem mais do que esclarecem, resultando em um consentimento que é, na prática, cego.

Adicionalmente, a relação entre o usuário e as plataformas digitais é estruturalmente assimétrica. O acesso a serviços e conteúdos muitas vezes é condicionado à aceitação integral dos termos, configurando uma lógica de "pegar ou largar" que anula a liberdade de escolha. Diante da onipresença de tais plataformas na vida social e econômica, a recusa em consentir pode significar a exclusão digital, um custo social desproporcional. Essa dinâmica, somada a

vieses cognitivos como a tendência de valorizar benefícios imediatos (o acesso ao serviço) em detrimento de riscos futuros e abstratos (a perda de privacidade), conduz a um estado de "resignação", no qual o indivíduo aquiesce não por vontade, mas por sentir-se impotente para alterar as regras do jogo (Bioni, 2021, p. 154). A autorização, nesse contexto, deixa de ser um ato de autodeterminação para se tornar um mero rito de passagem, uma formalidade que legitima a contínua extração de dados.

A superação dos limites do consentimento exige uma compreensão do bem jurídico tutelado pela LGPD. Conforme a doutrina, a proteção de dados pessoais transcende a noção tradicional de privacidade, historicamente associada ao direito de ser deixado só e à proteção de uma esfera íntima. Ela se consolida como um direito autônomo da personalidade, que resguarda não apenas o sigilo, mas a própria identidade, a dignidade e a capacidade do indivíduo de se desenvolver livremente e de participar da vida social sem ser indevidamente condicionado ou discriminado (Bioni, 2021, p. 55, 87).

As campanhas segmentadas no Google Ads, ao criarem perfis detalhados e utilizá-los para tomar decisões automatizadas sobre quais oportunidades, informações e preços são apresentados a cada indivíduo, interferem diretamente nesta esfera. O processo de analisar dados ou comportamentos para criar um perfil ou padrão que possa ser usado para entender ou prever algo pode levar à estigmatização e a práticas discriminatórias, parametrizando as oportunidades de vida do cidadão com base em inferências sobre sua condição financeira, estado de saúde ou convicções pessoais. A agregação de dados aparentemente triviais pode, inclusive, revelar dados sensíveis, como orientação sexual ou filiação política, expondo o titular a riscos de preconceito e exclusão (Bioni, 2021, p. 83). Portanto, a governança de dados no uso do Google Ads não pode se limitar a obter um consentimento formal; ela deve incorporar uma análise substantiva dos impactos do tratamento sobre os direitos fundamentais do titular, reconhecendo que o fluxo informacional deve ser governado por limites que assegurem o respeito à pessoa humana em sua integralidade.

A conformidade com a LGPD no uso de ferramentas complexas como o Google Ads não se esgota na revisão de uma política de privacidade ou na implementação de um banner de cookies. Exige-se a estruturação de um programa de governança em privacidade, um conjunto coordenado de políticas, processos, controles internos e medidas técnicas que assegurem, de forma contínua e demonstrável, o tratamento lícito, justo e transparente dos dados pessoais. Essa abordagem proativa possibilita gerenciar os riscos e para materializar o princípio da responsabilização e prestação de contas (accountability), um dos pilares da lei.

Uma premissa fundamental para a construção de um programa de governança eficaz é a compreensão das distintas responsabilidades dos agentes de tratamento. A documentação fornecida pelo próprio Google evidencia um modelo de responsabilidade compartilhada, no qual a plataforma oferece ferramentas e proteções contratuais, mas atribui ao anunciante a responsabilidade primária pela conformidade legal das suas campanhas (Google, 2023). Sob a ótica da LGPD, o anunciante que utiliza o Google Ads atua, na maioria dos cenários, como controlador, pois é ele quem toma as decisões referentes ao tratamento dos dados pessoais, definindo as finalidades da campanha e o público-alvo. Ao utilizar dados de sua própria base de clientes para criar listas de remarketing ou ao direcionar anúncios com base em critérios por ele definidos, o anunciante exerce o poder de decisão que caracteriza o controlador.

O Google, por sua vez, pode atuar como operador, tratando os dados em nome do controlador e de acordo com suas instruções, ou como co-controlador, quando toma decisões conjuntas com o anunciante sobre as finalidades e os meios do tratamento. Os "Termos de Proteção de Dados entre Controladores do Google Ads" são um instrumento que busca delimitar essas relações, mas não eximem o anunciante de sua própria diligência (Google, 2023). Um programa de governança robusto deve, portanto, mapear detalhadamente cada fluxo de dados dentro das campanhas do Google Ads, identificar os papéis de cada agente em cada contexto específico e garantir que as obrigações contratuais e legais de cada parte estejam claramente definidas e sejam devidamente cumpridas.

A implementação de uma governança efetiva para campanhas no Google Ads deve ser sustentada por pilares que enderecem os princípios e direitos previstos na LGPD de forma integrada e operacional. O primeiro pilar é a transparência efetiva, que vai muito além de textos genéricos. A empresa deve fornecer informações claras, precisas e facilmente acessíveis sobre como os dados são coletados por meio de suas propriedades digitais, quais tecnologias de rastreamento são utilizadas, para quais finalidades específicas os dados são tratados nas campanhas do Google Ads, e com quem são compartilhados dentro do ecossistema publicitário. Ferramentas como o "Por que este anúncio?" oferecidas pelo Google são um passo, mas a responsabilidade principal de informar recai sobre o controlador, que deve garantir que seus avisos de privacidade e banners de cookies sejam inteligíveis e completos (Google, 2023).

O segundo pilar é a gestão do consentimento e das bases legais. Um programa de governança maduro reconhece que o consentimento não é a única base legal disponível, mas também compreende que, para atividades de tratamento de alto impacto na privacidade, como a publicidade comportamental baseada em rastreamento entre sites, ele é, via de regra, indispensável. A governança deve incluir mecanismos para a coleta de um consentimento

válido, granular e livre de vícios, bem como para a sua gestão, permitindo que o titular o revogue de forma simples e gratuita. Ademais, para cada atividade de tratamento, a base legal apropriada deve ser identificada e documentada, seja ela o consentimento, o legítimo interesse do controlador ou a execução de contrato.

O terceiro pilar é a incorporação dos princípios de minimização de dados e finalidade, o que se traduz no conceito de Privacy by Design (privacidade desde a concepção). Antes de iniciar uma campanha, a governança exige que se defina um propósito legítimo, específico e explícito, e que o tratamento de dados se limite ao estritamente necessário para alcançar essa finalidade. Isso significa não apenas evitar a coleta de dados excessivos, mas também utilizar os recursos de proteção de dados oferecidos pela plataforma do Google, como os controles de retenção de informações, para garantir que os dados não sejam mantidos por mais tempo do que o necessário (Faria, 2023).

O quarto pilar é a segurança da informação e a gestão de incidentes. O controlador tem o dever de adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. A governança deve prever um plano de resposta a incidentes que inclua procedimentos para detecção, contenção, análise e notificação à ANPD e aos titulares, conforme exigido pela LGPD. O compromisso do Google com certificações como a ISO 27001 reforça a segurança da plataforma, mas a segurança "de ponta a ponta", incluindo a forma como o anunciante gerencia o acesso às suas contas e armazena os dados que coleta, é de responsabilidade do controlador (Google, 2023).

Finalmente, o quinto e mais abrangente pilar é o empoderamento do titular, que consiste em garantir o exercício pleno de seus direitos. A governança deve estabelecer canais de comunicação claros e eficientes para que os titulares possam solicitar a confirmação da existência do tratamento, o acesso aos seus dados, a correção de informações, a anonimização, o bloqueio ou a eliminação de dados desnecessários, a portabilidade e a revisão de decisões automatizadas. A capacidade de responder a essas requisições de forma tempestiva e completa não é apenas uma obrigação legal, mas um indicador da maturidade do programa de proteção de dados de uma organização e de seu respeito para com os indivíduos.

A jornada pela governança de dados em campanhas segmentadas no Google Ads, sob a perspectiva da LGPD, revela que a conformidade transcende a mera aplicação de um checklist legal. Ela demanda uma mudança cultural profunda, que reposiciona a proteção de dados pessoais não como um obstáculo à inovação, mas como um pilar para a construção de uma economia digital justa, transparente e sustentável. A análise da "economia de vigilância" demonstra que os modelos de negócios que prosperaram na ausência de uma regulação robusta

agora enfrentam o imperativo de se reinventarem, equilibrando seus legítimos interesses comerciais com o respeito inegociável aos direitos fundamentais dos cidadãos.

A crítica ao paradigma da autodeterminação informacional, centrada na figura fragilizada do consentimento, evidencia que a responsabilidade pela proteção de dados não pode recair exclusivamente sobre os ombros do titular. Em um ambiente de notória assimetria informacional, técnica e econômica, a governança corporativa emerge como o principal mecanismo para internalizar os princípios da LGPD nas operações cotidianas. O anunciante, na qualidade de controlador, detém o dever primordial de garantir que suas estratégias de marketing digital sejam concebidas e executadas de forma a respeitar a privacidade desde a concepção, limitando a coleta ao essencial, sendo transparente sobre suas finalidades e assegurando que o titular dos dados permaneça no controle de suas informações.

O modelo de responsabilidade compartilhada com o Google não dilui, mas reforça a necessidade de uma diligência ativa por parte dos anunciantes. A utilização das ferramentas e das garantias contratuais oferecidas pela plataforma deve ser parte de uma estratégia de governança ampla, que inclua políticas internas claras, treinamento de equipes, gestão de riscos, um plano de resposta a incidentes e, fundamentalmente, canais acessíveis para o exercício dos direitos dos titulares. Em última análise, a governança em proteção de dados no contexto do Google Ads é um processo contínuo de avaliação, adaptação e demonstração de compromisso, cujo sucesso se mede não apenas pela ausência de sanções, mas pela capacidade de construir relações de confiança com os consumidores que hoje valorizam as empresas que tratam seus dados com o respeito que sua dignidade exige.

6. CONCLUSÃO

Ao encerrar a jornada investigativa proposta por esta monografia, que se debruça sobre a intrincada relação entre as práticas publicitárias na plataforma Google Ads e o regime jurídico inaugurado pela LGPD, emerge um panorama de transformações e de desafios para os atores envolvidos no ecossistema da publicidade digital. A pesquisa, assim, parte de uma problemática central acerca da identificação, na política de tratamento de dados pessoais do Google Ads, de boas práticas de conformidade que permitam aos anunciantes a utilização das sofisticadas ferramentas de segmentação em coerência com os direitos de privacidade.

O percurso trilhado explora pilares da LGPD e realiza o exame da operacionalidade do Google Ads e das exigências de suas práticas de governança. A articulação teórico-documental demonstra, em primeiro lugar, a consolidação de um panorama socioeconômico no qual dados pessoais se convertem em ativo valioso que alimenta a chamada economia da vigilância. Com efeito, as práticas de publicidade comportamental, cerne da eficiência do Google Ads, são a manifestação mais visível dessa nova lógica, que se fundamenta na extração e análise massiva de informações para a criação de perfis detalhados e para a predição de hábitos de consumo.

Este estudo corrobora, também, que o modelo técnico-publicitário em apreço, embora economicamente poderoso, gera uma tensão entre princípios consagrados pela LGPD, especialmente a autodeterminação informativa, com os expedientes de direcionamento publicitário com base em estratégias de segmentação. A lei, portanto, representa um reforço antagônico à lógica extrativista, exigindo que o tratamento de dados, inclusive para fins publicitários, seja pautado pela finalidade, necessidade, transparência e pela não discriminação.

Em tudo o que fica exposto, parece destacar-se a constatação da fragilidade do consentimento como pilar isolado para a legitimação das práticas de publicidade segmentada. A análise evidencia que, em contextos de notória assimetria informacional, técnica e econômica que caracteriza a relação entre usuários e as grandes plataformas digitais, o consentimento tende a se degradar, convertendo-se em uma mera formalidade desprovida de substância. Essa realidade sugere que o consentimento se transforma em uma aquiescência resignada diante da complexidade dos fluxos de dados e da lógica de "pegar ou largar" para o acesso a serviços que foram travestidos como essenciais.

Diante do caso eleito para escrutínio, percebe-se a complexa distribuição de papéis e responsabilidades no âmbito do Google Ads. A figura do anunciante emerge, inequivocamente, como controlador na vasta maioria das operações, uma vez que é ele quem define as finalidades da campanha e as características do público-alvo, tomando as decisões essenciais sobre o

tratamento dos dados. A plataforma, por sua vez, transita entre os papéis de operadora e, em muitas circunstâncias, de co-controladora, dado seu poder de definir os meios formais e técnicos para articular seu próprio e vasto acervo de dados para otimizar os anúncios.

Esse importante achado desmistifica a falácia de que o anunciante, ao contratar o serviço, isenta-se de responsabilidade, que reside exclusivamente na esfera da plataforma. Pelo contrário, o modelo de responsabilidade compartilhada imposto pela LGPD exige diligência ativa e uma governança coordenada, na qual o anunciante também tem o dever inafastável de compreender e supervisionar o modo como os dados de seus potenciais clientes são tratados em toda a cadeia de valor publicitário. O Google Ads parece trilhar esse caminho.

Respondendo diretamente à questão central que norteia o trabalho, conclui-se que o conjunto de boas práticas para a conformidade no uso do Google Ads materializa-se na implementação de um programa de governança em privacidade robusto e integrado. Tal programa pode transcender a elaboração de documentos e se traduz em uma cultura organizacional que incorpora a proteção de dados em todas as suas fases, incentivando, assim, os demais atores do processo a absorverem a cultura proposta.

Logo, a pauta de governança presente na documentação do Google Ads contempla, mas não se limita, por exemplo, à adoção do princípio de Privacy by Design (privacidade desde a concepção), buscando assegurar que as campanhas sejam planejadas para utilizar o mínimo de dados necessários para finalidades específicas, legítimas e explícitas, mantendo-se, desde o princípio, uma postura de tratamento de dados mínimo, restrito e conservador. Também se verificam a implementação de mecanismos de transparência efetiva, por meio de avisos de privacidade claros e em camadas, que expliquem de forma inteligível o fluxo de dados na publicidade segmentada; a gestão criteriosa das bases legais, com a coleta de um consentimento válido e granular para as atividades de maior impacto; a realização de testes de ponderação (Relatórios de Impacto à Proteção de Dados) para o uso do legítimo interesse; a implementação de medidas de segurança técnicas e administrativas para proteger os dados em todo o seu ciclo de vida; e, por fim, o estabelecimento de canais pretensamente acessíveis e eficientes para garantir que os titulares possam exercer seus direitos, incluindo o direito à revisão de decisões automatizadas que definem seus perfis.

Diante dessa realidade, a monografia conclui que a conformidade com a LGPD, embora não se esgote nas previsões clausulares de políticas de tratamento de dados pessoais, possui relevância quando abordados e ostentados por documentos dessa sorte, que, em alguma medida, podem incentivar a ascensão de protocolos de responsabilização e prestação de contas

(accountability) por parte de anunciantes. Afinal, a aptidão de um anunciante em demonstrar, por meio de medidas concretas e auditáveis, que adota postura proativa de proteção de dados pessoais reforça a natureza substantiva de documentos que elaboram as políticas relacionadas.

Então, confirma-se a hipótese inicial de que, apesar da complexidade inerente, parece ser possível identificar um arcabouço normativo autorregulatório coerente com a LGPD, no caminho da preconização de condutas que harmonizem os arquétipos do mercado publicitário com a adequada proteção de diretos dos titulares de dados pessoais. É preciso reconhecer, contudo, as limitações inerentes a este estudo. A análise, de cunho predominantemente teórico-dogmático e focada no Google Ads, constitui um retrato de um cenário tecnológico e regulatório em constante evolução, além de circunscrito a uma das plataformas de segmentação publicitária. Sugerem-se, para futuras pesquisas, a realização de estudos empíricos que avaliem a percepção e o nível de compreensão dos titulares de dados diante das ferramentas de transparência oferecidas; análises comparativas com outras grandes plataformas de publicidade digital; o aprofundamento sobre os desafios práticos da efetivação do direito à revisão de decisões algorítmicas no contexto dos leilões de anúncios em tempo real. A atuação da ANPD na fiscalização do mercado publicitário, igualmente, revela-se campo fértil para investigações vindouras.

Em síntese final, a monografia conclui que a Lei Geral de Proteção de Dados vem sendo absorvida e considerada, ao menos em termos de documentação de política de tratamento de dados de importante plataforma de segmentação de anúncios operante em âmbito nacional, para a adequação das práticas de publicidade. Adicionalmente, afere-se que tal documentação descortina incentivos para que anunciantes se comprometam com um modelo de governança de dados coordenado, haja vista que as responsabilidades são compartilhadas.

A conclusão a que se chega, portanto, não é a de uma incompatibilidade insuperável entre publicidade segmentada e privacidade, mas sim a de que, pelo menos no âmbito das políticas autorregulatórias de tratamento de dados, cabe (e se identificam ações para) a promoção de uma reinvenção cultural e operacional, na qual o respeito à LGPD deixa de ser um mero requisito formal para se converter em um pilar estratégico na construção de um mercado mais ético, transparente e responsável.

REFERÊNCIAS

ADBUTLER. **Publishers vs Advertisers: What's the difference?** [*S.l.*], 1 jun. 2021. Disponível em: https://www.adbutler.com/blog/article/publishers-vs-advertisers-differences-explained. Acesso em: 7 jul. 2025.

ALICEDA, Rodolfo Ignácio; TEIXEIRA, Tarcisio. A responsabilidade do Google Ads por danos oriundos de conteúdo gerado por seus anunciantes. **Scientia Iuris**, Londrina, v. 25, n. 2, p. 107-130, jul. 2021. DOI: 10.5433/21788189.2021v25n2p107. ISSN: 2178-8189.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados-LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, p. 26-45, 2022. Disponível em: https://www.scielo.br/j/pci/a/tb9czy3W9RtzgbWWxHTXkCc/. Acesso em: 3 jun. 2025.

ALVES, Fabrício da Mota. Avaliação de impacto sobre a proteção de dados. *In*: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **Comentários ao GDPR: regulamento geral de proteção de dados da União Européia**. São Paulo: Reuters Brasil, 2018.

BIONI, Bruno R. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento** - 3ª Edição 2021. 3. ed. Rio de Janeiro: Forense, 2021. E-book. ISBN 9788530994105. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530994105/. Acesso em: 5 abr. 2025.

BIONI, Bruno R.; KITAYAMA, Marina; RIELLI, Mariana. **O Legítimo Interesse na LGPD**: quadro geral e exemplos de aplicação. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021.

BIONI, Bruno R; SILVA, Paula G. F. da; MARTINS, Pedro B. L. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso. **Cadernos Técnicos da CGU**, v. 1, p. 8-19, 2022. Disponível em: https://repositorio.ucp.pt/entities/publication/beac0e25-4bc9-4f3b-9484-107304a91d67. Acesso em: 4 abr. 2025.

BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito proativo. **Civilistica.com**, Rio de Janeiro, v. 8, n. 3, p. 1–6, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/448.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

CARIBÉ, João Carlos Rebello. Uma perspectiva histórica e sistêmica do capitalismo de vigilância. **Revista Inteligência Empresarial**, v. 41, p. 5-13, 2019. Disponível em: http://www.crie.ufrj.br/destaque/revista-inteligencia-empresarial-n-41/541.

FARIA, Wellington L. **Google Ads e LGPD: Proteja os Dados e Otimize Campanhas.** [*S.l.*], 2023. Disponível em: https://becompliance.com/google-ads-e-lgpd/. Acesso em: 4 abr. 2025.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes. Princípios que Regem o Tratamento de Dados no Brasil. *In*: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à lei geral de proteção de dados**: Lei 13.709/2018. São Paulo: Almedina, 2020.
GENEROSO, André Mesquita; SILVA, Michael César; NOGUEIRA, Roberto Henrique Porto. Publicidade ilícita e mecanismos tecnológicos de direcionamento. **Revista Jurídica Luso-Brasileira**, n. 4, 2022, p. 393-422. Disponível em: https://www.cidp.pt/revistas/rjlb/2022/4/2022_04_0393_0422.pdf.

GOOGLE. **Responsabilidade sobre os dados da empresa.** [*S.l.*], 2023. Disponível em: https://business.safety.google/intl/pt-BR/lgpd/. Acesso em: 4 abr. 2025.

GOOGLE. **Termos de Tratamento de Dados de Publicidade do Google**. [*S.l.*], 2024. Disponível em: https://business.safety.google/adsprocessorterms/.

GOOGLE. **Google Ads — Diretrizes e políticas — Central de Transparência**. [*S.l.*], [*s.d.*], Disponível em: https://transparency.google/intl/pt-BR/our-policies/product-terms/google-ads/. Acesso em: 4 abr. 2025.

JIMENE, Camila do Vale. Reflexões sobre privacy by design e privacy by default: da idealização à positivação. *In*: BLUM, Renato Opice; MALDONADO, Viviane Nóbrega (Coord.). **Comentários ao GDPR: regulamento geral de proteção de dados da União Européia**. São Paulo: Reuters Brasil, 2018.

KURBALIJA, Jovan. **Uma introdução à Governança da Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2016.

LADEIRA GARBACCIO, Grace; LUBIESKA N. KISCHELEWSKI , Flávia. Governança e boas práticas na Lei Geral de Proteção de Dados por meio da conformidade, da gestão de riscos e da accountability. **Revista Brasileira de Estudos Políticos**, v. 128, 15 jul. 2024. Disponível em: https://doi.org/10.9732/2024.V128.894.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Segurança, boas práticas, governança e compliance. *In*: LIMA, Cíntia Rosa Pereira de (Coord.). **Comentários à lei geral de proteção de dados**: Lei 13.709/2018. São Paulo: Almedina, 2020.

MARTINS, Guilherme Magalhães; LONGHI, João Victor; FALEIROS JÚNIOR, José Luiz de Moura. **Comentários à Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Editora Foco, 2024.

MCDONALD, Aleecia M; CRANOR, Lorrie Faith. The Cost of Reading Privacy Policies. **Journal of Law and Policy for Information Society**, v. 4, p. 543-570, 2008. Disponível em: https://kb.osu.edu/server/api/core/bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/content. Acesso em: 4 jul. 2025.

OLIVEIRA, Angélica Pires de. **O impacto da Lei Geral de Proteção de Dados no marketing digital**. 38f. 2021. Monografia (MBA em Tecnologias Digitais e Inovação Sustentável) Escola Politécnica da Universidade de São Paulo. 2021.

PAVANELLI, Stéfani Thaís. **Marketing digital: uma análise do impacto do tráfego pago em pequenas empresas**. 50f. 2022. Trabalho de Conclusão de Curso (Graduação em

Publicidade e Propaganda) - Centro Universitário Sagrado Coração, UNISAGRADO, Bauru, 2022. p. 15-20

SANI, Eduardo. **Papel dos publishers na Mídia Programática**. [*S.l.*], [*s.d.*]. ADSPLAY. Disponível em: https://adsplay.com.br/papel-dos-publishers-na-midia-programatica/. Acesso em: 7 jul. 2025.

TREVISAN, Nanci M. *et al*. **Publicidade on-line**. Porto Alegre: SAGAH, 2020. E-book. p. 77-100 ISBN 9786556900247. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556900247/. Acesso em: 4 abr. 2025.

UTZ, Christine *et al*. (Un) informed consent: Studying GDPR consent notices in the field. *In*: **Proceedings of the 2019 acm sigsac conference on computer and communications security**. 2019. p. 973-990. Disponível em: https://dl.acm.org/doi/epdf/10.1145/3319535.3354212. Acesso em: 4 jun. 2025.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of information technology**, v. 30, n. 1, p. 75-89, 2015. Disponível em: https://journals.sagepub.com/doi/abs/10.1057/jit.2015.5.

APÊNDICE A - RESPONSABILIDADE SOBRE OS DADOS DA EMPRESA.

SUMÁRIO

LGPD

A Lei Geral de Proteção de Dados (“LGPD”) é uma nova lei de privacidade que está prevista para entrar em vigor em 16 de agosto de 2020. A LGPD se aplica a empresas (dentro e fora do Brasil) que processam dados pessoais de usuários localizados nesse país.. Uma autoridade de proteção de dados (DPA) brasileira será estabelecida e fornecerá diretrizes sobre como interpretar e implementar os requisitos da LGPD. Como isso ainda não aconteceu, a abordagem atual do Google está sujeita a alterações.

Termos e proteções contratuais

O Google já oferecia termos de proteção de dados para os produtos do Google Ads de acordo com o Regulamento geral de proteção de dados (GDPR) europeu e a Lei de Privacidade do Consumidor da Califórnia (CCPA) antes de a LGPD entrar em vigor. Depois de atualizar os termos de proteção de dados do Google Ads para adicionar termos específicos da LGPD em meados de agosto de 2020, o Google consolidou recentemente as obrigações da LGPD no corpo principal dos termos de proteção de dados de anúncios, substituindo os termos específicos da LGPD. Para esclarecer, essa não foi uma mudança significativa dos compromissos do Google sob a LGPD, mas uma expansão dos compromissos que já se aplicavam consistentemente em conexão com a legislação europeia de proteção de dados, a LGPD brasileira e as leis de privacidade dos estados dos EUA a todos os clientes, independente da jurisdição.

Mais informações sobre a LGPD

Além dos termos de proteção de dados do Google Ads, oferecemos controles de produtos que nossos clientes de anúncios podem utilizar como parte da própria estratégia de conformidade com a LGPD. Se você acredita que está no escopo dessa lei, fale com seu advogado para determinar o que fazer para obedecê-la, incluindo como usar as opções que oferecemos.

Termos e políticas

> Termos de Proteção de Dados entre Controladores do Google Ads
>
> Termos de Processamento de Dados de Publicidade do Google
>
> Termos de Proteção de Dados entre Controladores de Métricas do Google
>
> Detalhamento dos produtos de publicidade do Google para controladores e processadores
>
> Publicidade e cookies

Recursos para editores e anunciantes

Recursos para editores:

 Google Ad Manager

 Google AdMob

 Google AdSense:

 Google Analytics

Recursos para anunciantes:

APÊNDICE B - TERMOS DE TRATAMENTO DE DADOS DE PUBLICIDADE DO GOOGLE.

Termos de Tratamento de Dados de Publicidade do Google

O Google e a contraparte que aceita estes termos (o "**Cliente**") celebraram um contrato de prestação de Serviços de Operador (conforme periodicamente alterado, o "**Contrato**").

Estes Termos de Tratamento de Dados de Publicidade do Google (juntamente com os apêndices, os "**Termos de Tratamento de Dados**") são celebrados pelo Google e pelo Cliente e complementam o Contrato. Estes Termos de Tratamento de Dados entrarão em vigor e substituirão quaisquer termos anteriormente aplicáveis relativos ao objeto em questão (incluindo quaisquer adendos ou alterações ao tratamento de dados com relação aos Serviços de Operador), a partir da data de Início da Vigência dos Termos.

Se você está aceitando estes Termos de Tratamento de Dados em nome do Cliente, você garante que: (a) tem plenos poderes legais para vincular o Cliente a estes Termos de Tratamento de Dados; (b) leu e entendeu estes Termos de Tratamento de Dados; e (c) aceita estes Termos de Tratamento de Dados, em nome do Cliente. Se você não tem poderes legais para vincular o Cliente, não aceite estes Termos de Tratamento de Dados.

1. Introdução

Estes Termos de Tratamento de Dados refletem o acordo celebrado entre as partes sobre os termos que regem o tratamento de Dados Pessoais do Cliente.

2. Definições e interpretação

2.1 Nestes Termos de Tratamento de Dados:

"**Afiliada**" significa uma entidade que, direta ou indiretamente, controla, é controlada por ou está sob controle comum de uma parte.

"**Certificação ISO 27001**" significa a certificação ISO/IEC 27001:2013 ou qualquer certificação equivalente para os Serviços de Operador.

"**Dados Pessoais do Cliente**" significa os dados pessoais tratados pelo Google em nome do Cliente no âmbito da prestação dos Serviços de Operador por parte do Google.

"**Data de Início da Vigência dos Termos**" significa a data em que o Cliente clicou para aceitar ou a data em que as partes, de outra forma, aceitaram estes Termos de Tratamento de Dados.

"**Documentação de Segurança**" significa o certificado emitido para a Certificação ISO 27001 e qualquer outra certificação ou documento de segurança que o Google possa disponibilizar relativamente aos Serviços de Operador.

"**Endereço de E-mail para Recebimento de Notificações**" significa o endereço de e-mail designado pelo Cliente, na interface do usuário dos Serviços de Operador ou em outros meios fornecidos pelo Google, para receber notificações do Google relacionadas a estes Termos de Tratamento de Dados.

"**Entidade do Google**" significa a Google LLC, a Google Ireland Limited ou qualquer outra Afiliada da Google LLC.

"**FDPA da Suíça**" significa, conforme aplicável, a Lei Federal de Proteção de Dados de 19 de junho de 1992 (Suíça) (com a Portaria da Lei Federal de Proteção de Dados de 14 de junho de 1993) ou a Lei Federal de Proteção de Dados revisada de 25 de setembro de 2020 (com a Portaria da Lei Federal de Proteção de Dados de 31 de agosto de 2022).

"**Ferramenta dos Titulares dos Dados**" significa uma ferramenta (se houver) disponibilizada por uma Entidade do Google aos titulares dos dados que permite ao Google responder direta e padronizadamente a determinadas solicitações feitas pelos titulares dos dados com

relação aos Dados Pessoais do Cliente. Por exemplo, configurações de publicidade on-line ou desativação do plug-in de um navegador.

"**GDPR**" significa, conforme aplicável: (a) o GDPR da UE; e/ou (b) o GDPR do Reino Unido.

"**GDPR da União Europeia**" significa o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE.

"**GDPR do Reino Unido**" significa o GDPR da UE conforme alterado e incorporado na legislação do Reino Unido, de acordo com os termos da Lei de Saída do Reino Unido da União Europeia de 2018 (UK European Union (Withdrawal) Act 2018), e a legislação secundária aplicável elaborada de acordo com essa lei.

"**Google**" significa a Entidade do Google que é uma parte do Contrato.

"**Incidente com Dados**" significa uma violação de segurança do Google que gera destruição, perda, alteração, divulgação não autorizada ou acesso acidentais ou ilegais a Dados Pessoais do Cliente em sistemas gerenciados ou controlados pelo Google. "Incidentes com Dados" não incluem atividades ou tentativas malsucedidas que não comprometam a segurança dos Dados Pessoais do Cliente, incluindo tentativas não concretizadas de login, pings, verificação de portas, ataques de negação de serviço e outros ataques de rede em firewalls ou sistemas de rede.

"**Instruções**" tem o significado atribuído na Seção 5.2 (Instruções do Cliente).

"**Legislação Aplicável em matéria de Proteção de Dados**" significa, conforme aplicável ao tratamento de Dados Pessoais do Cliente, qualquer lei ou regulamento sobre privacidade, segurança de dados ou proteção de dados, a nível nacional, federal, da UE, estadual, provincial ou outros, incluindo a Legislação Europeia em matéria de

Proteção de Dados, a LGPD e as Leis Estaduais de Privacidade dos EUA.

"**Legislação Europeia em matéria de Proteção de Dados**" significa, conforme aplicável, (a) o GDPR; e/ou (b) a FDPA da Suíça.

O conteúdo das "**Leis de privacidade dos estados nos EUA**" pode ser conferido em business.safety.google/usdataprotectionlaws.

"**LGPD**" significa a Lei Geral de Proteção de Dados Pessoais brasileira.

"**Medidas de Segurança**" tem o significado definido na Seção 7.1.1 (Medidas de Segurança do Google).

"**Novo Sub-Operador**" tem o significado atribuído na Seção 11.1 (Autorização para Engajamento de Sub-operadores).

"**Período de Vigência**" significa o período entre a Data de Início da Vigência dos Termos e o final do fornecimento dos Serviços de Operador por parte do Google ao abrigo do Contrato.

"**Produto Adicional**" significa um produto, serviço ou aplicativo fornecido pelo Google ou por um terceiro que: (a) não faz parte dos Serviços de Operador; e (b) está acessível para uso na interface do usuário dos Serviços de Operador ou, de alguma forma, integrado a eles.

"**Serviços de Operador**" significa os serviços aplicáveis listados em business.safety.google/adsservices.

"**Sub-operadores**" significa os terceiros autorizados por estes Termos de Tratamento de Dados a ter acesso lógico e a tratar Dados Pessoais do Cliente a fim de fornecer partes dos Serviços de Operador e qualquer suporte técnico relacionado.

"**Termos Adicionais**" significa os termos adicionais mencionados no Apêndice 3, que refletem o acordo entre as partes sobre os termos que regem o tratamento dos Dados Pessoais do Cliente ao abrigo de determinada Legislação de Proteção de Dados Aplicável.

2.2 Os termos "**controlador**", "**titular dos dados pessoais**", "**dados pessoais**", "**processamento**"/"**tratamento**" e "**operador**" usados

nestes Termos de Tratamento de Dados terão os significados atribuídos a eles (a) na Legislação Aplicável em matéria de Proteção de Dados ou, (b) se não houver descrição do significado ou lei, no GDPR.

2.3 As palavras "**incluir**" e "**incluindo**" significam "incluindo, mas não se limitando a". Todos os exemplos nestes Termos de Tratamento de Dados são ilustrativos, e não exemplos únicos de um conceito específico.

2.4 Qualquer referência a um regime legal, estatuto ou outro ato legislativo é uma referência a ele conforme periodicamente alterado ou promulgado.

2.5 Em caso de inconsistência entre a versão traduzida e a versão em inglês destes Termos de Tratamento de Dados, a versão em inglês terá precedência.

3. Duração destes Termos de Tratamento de Dados

Estes Termos de Tratamento de Dados entrarão em vigor na Data de Início da Vigência dos Termos. Não obstante a rescisão ou expiração do Contrato, estes Termos de Tratamento de Dados permanecerão em vigor até a eliminação de todos os Dados Pessoais do Cliente por parte do Google e expirarão automaticamente após esse fato, conforme descrito nesses Termos.

4. Aplicação destes Termos de Tratamento de Dados

4.1 **Geral**. Estes Termos de Tratamento de Dados só serão aplicados aos Serviços de Operador no âmbito dos quais as partes aceitaram estes Termos de Tratamento de Dados, por exemplo, (a) os Serviços de Operador para os quais o Cliente tenha aceitado estes Termos de

Tratamento de Dados ou, (b) se o Contrato incorpora estes Termos de Tratamento de Dados por referência, os Serviços de Operador que são objeto do Contrato.

4.2 **Incorporação de Termos Adicionais**. Os Termos Adicionais complementam estes Termos de Tratamento de Dados.

5. Tratamento de Dados

5.1 **Funções e Conformidade Regulatória; Autorização**.

5.1.1 **Responsabilidades do Operador e do Controlador**. As partes confirmam e concordam que:

(a) o Apêndice 1 descreve o objeto e os detalhes do tratamento de Dados Pessoais do Cliente; o Google é um operador de Dados Pessoais do Cliente;

(b) o Cliente é um controlador ou um operador, conforme aplicável, de Dados Pessoais do Cliente; e

(c) cada parte cumprirá as obrigações que para si decorrem ao abrigo da Legislação Aplicável em matéria de Proteção de Dados no que diz respeito ao tratamento de Dados Pessoais do Cliente.

5.1.2 **Clientes Operadores**. Se o Cliente for um operador:

(a) o Cliente garante, de maneira contínua, que o controlador relevante autorizou: (i) as Instruções, (ii) a designação por parte do Cliente do Google como outro operador e (iii) o engajamento de Sub-operadores pelo Google, conforme descrito na Seção 11 (Sub-operadores);

(b) o Cliente encaminhará, imediatamente e sem qualquer atraso, ao controlador relevante qualquer notificação fornecida da parte do Google ao abrigo das Seções 7.2.1 (Notificação de Incidentes) ou 11.4

(Oportunidade para se Opor a Alterações aos Sub-operadores); e

(c) o Cliente pode disponibilizar ao controlador relevante qualquer informação disponibilizada pelo Google ao abrigo das Seções 7.4 (Certificação de Segurança), 10.2 (Informações do Data Center) e 11.2 (Informações sobre Sub-operadores).

5.2 **Instruções do Cliente**. Ao celebrar estes Termos de Tratamento de Dados, o Cliente instrui o Google a tratar os Dados Pessoais do Cliente somente de acordo com a legislação aplicável: (a) a fim de prestar os Serviços de Operador e qualquer outro suporte técnico relacionado; (b) como especificado mais detalhadamente através do uso pelo Cliente dos Serviços de Operador (inclusive nas configurações e em outras funcionalidades dos Serviços de Operador) e em qualquer outro suporte técnico relacionado; (c) conforme documentado no Contrato, incluindo estes Termos de Tratamento de Dados; e (d) conforme documentado mais detalhadamente em quaisquer outras instruções por escrito fornecidas pelo Cliente e reconhecidas pelo Google como constituindo instruções para efeitos destes Termos de Tratamento de Dados (coletivamente, as "**Instruções**").

5.3 **Cumprimento das Instruções pelo Google**. O Google cumprirá as Instruções, exceto quando tal seja proibido ao abrigo da legislação aplicável ou quando a legislação aplicável exigir outro tratamento.

5.4 **Produtos Adicionais**. Se o Cliente usar qualquer Produto Adicional, os Serviços de Operador poderão permitir que esse produto tenha acesso aos Dados Pessoais do Cliente quando necessário para a interoperação do Produto Adicional com os Serviços de Operador. Para fins de esclarecimento, estes Termos de Tratamento de Dados não se aplicam ao tratamento de dados pessoais relacionado ao fornecimento de qualquer Produto Adicional usado pelo Cliente, incluindo dados pessoais transmitidos para esse Produto Adicional ou por esse Produto Adicional.

6. Exclusão de Dados

6.1 **Exclusão Durante o Período de Vigência.**

6.1.1 **Serviços de Operador com Funcionalidades de Exclusão.** Se, durante o Período de Vigência:

(a) as funcionalidades dos Serviços de Operador incluírem a opção que permite ao Cliente excluir Dados Pessoais do Cliente;

(b) o Cliente usar os Serviços de Operador para excluir determinados Dados Pessoais do Cliente; e

(c) os Dados Pessoais do Cliente excluídos não puderem ser recuperados pelo Cliente (por exemplo, da "Lixeira"),

o Google excluirá esses Dados Pessoais do Cliente dos próprios sistemas assim que razoavelmente possível e dentro de um período máximo de 180 dias, exceto se a legislação aplicável exigir o armazenamento.

6.1.2 **Serviços de Operador sem Funcionalidades de Exclusão.** Durante o Período de Vigência, se as funcionalidades dos Serviços de Operador não incluírem a opção que permita ao Cliente excluir Dados Pessoais do Cliente, o Google cumprirá:

(a) com qualquer solicitação razoável do Cliente para agilizar essa exclusão, na medida em que isso seja possível considerando a natureza e as funcionalidades dos Serviços de Operador e exceto se a legislação aplicável exigir o armazenamento; e

(b) as práticas de retenção de dados descritas em policies.google.com/technologies/ads.

O Google poderá cobrar uma taxa (com base nos custos razoáveis que tenha) por qualquer exclusão de dados realizada de acordo com a Seção 6.1.2(a). O Google dará ao Cliente mais detalhes sobre as taxas aplicáveis e sobre a base de cálculo das taxas antes da exclusão dos dados em questão.

6.2 **Exclusão no Final do Período de Vigência**. O Cliente instrui o Google a excluir todos os Dados Pessoais do Cliente restantes (incluindo eventuais cópias) dos sistemas do Google no final do Período de Vigência, de acordo com a legislação aplicável. O Google cumprirá essa instrução assim que razoavelmente possível e dentro de um período máximo de 180 dias, exceto se a legislação aplicável exigir o armazenamento.

7. Segurança dos Dados

7.1 **Medidas e Assistência de Segurança do Google**.

7.1.1 **Medidas de Segurança do Google**. O Google implementará e manterá medidas técnicas e organizacionais para proteger os Dados Pessoais do Cliente contra destruição, perda, alteração, divulgação não autorizada ou acesso acidentais ou ilegais, conforme descrito no Apêndice 2 (as "**Medidas de Segurança**"). De acordo com o Apêndice 2, as Medidas de Segurança incluem ações para: (a) criptografar dados pessoais; (b) ajudar a garantir confidencialidade, integridade, disponibilidade e resiliência contínuas dos sistemas e serviços do Google; (c) ajudar a restaurar o acesso a dados pessoais em tempo hábil após um incidente; e (d) fazer testes de eficiência regulares. O Google pode atualizar ou modificar as Medidas de Segurança periodicamente, desde que tais atualizações e modificações não resultem na degradação da segurança geral dos Serviços de Operador.

7.1.2 **Acesso e Compliance**. O Google: (a) só autorizará os seus funcionários, contratados e Sub-operadores a acessar os Dados Pessoais do Cliente quando tal for estritamente necessário para cumprimento das Instruções; (b) tomará as providências cabíveis para garantir o cumprimento das Medidas de Segurança por parte dos funcionários, contratados e Sub-operadores na medida aplicável ao seu escopo de atuação; e (c) garantirá que todas as pessoas autorizadas a tratar Dados Pessoais do Cliente assumiram um

compromisso de sigilo e confidencialidade ou têm uma obrigação legal adequada de confidencialidade.

7.1.3 **Assistência de Segurança do Google**. O Google, considerando a natureza do tratamento dos Dados Pessoais do Cliente e as informações que dispõe, ajudará o Cliente a garantir o cumprimento das obrigações do Cliente (ou, caso o Cliente seja um operador, as obrigações do controlador relevante) em matéria de segurança e de violações de dados pessoais, de acordo com a Legislação Aplicável em matéria de Proteção de Dados, das seguintes formas:

(a) implementação e manutenção de Medidas de Segurança de acordo com o previsto na Seção 7.1.1 (Medidas de Segurança do Google);

(b) cumprimento dos termos previstos na Seção 7.2 (Incidentes com Dados); e

(c) disponibilização ao Cliente da Documentação de Segurança de acordo com o previsto na Seção 7.5 (Verificação de Compliance) e das informações contidas nestes Termos de Tratamento de Dados.

7.2 **Incidentes com Dados**.

7.2.1 **Notificação de Incidentes**. Caso tome conhecimento de um Incidente com Dados, o Google:

(a) notificará o Cliente imediatamente e sem qualquer atraso; e

(b) tomará providências razoáveis imediatas para minimizar os danos e proteger os Dados Pessoais do Cliente.

7.2.2 **Detalhes do Incidente com Dados**. As notificações feitas de acordo com o previsto na Seção 7.2.1 (Notificação de Incidentes) irão descrever: a natureza do Incidente com Dados, incluindo os recursos do Cliente afetados; as medidas que o Google tomou ou planeja tomar para resolver o

Incidente com Dados e mitigar o potencial risco do mesmo; as medidas, se houver, que o Google recomenda que o Cliente tome para resolver o Incidente com Dados; e detalhes de um ponto de contato para a obtenção de mais informações. Se não for possível fornecer todas essas informações ao mesmo tempo, a notificação inicial do Google terá as informações disponíveis no momento, e mais detalhes serão fornecidos sem atrasos indevidos assim que estiverem disponíveis.

7.2.3 **Envio da Notificação**. O Google enviará a notificação sobre um Incidente com Dados para o Endereço de E-mail para Recebimento de Notificações ou, a critério do Google (incluindo nos casos em que o Cliente não tenha fornecido esse endereço), por qualquer outro meio de comunicação direta (por exemplo, por telefone ou reunião presencial). O Cliente é a única parte responsável por fornecer o Endereço de E-mail para Recebimento de Notificações e garantir que esse endereço está atualizado e válido.

7.2.4 **Notificações a Terceiros**. O Cliente é a única parte responsável por cumprir o disposto nas leis em matéria de notificação de incidentes que sejam aplicáveis ao Cliente e por cumprir todas as obrigações de notificação a terceiros relacionadas a Incidentes com Dados.

7.2.5 **Não Reconhecimento de Falha por parte do Google**. A notificação ou resposta do Google a um Incidente com Dados nos termos desta Seção 7.2 (Incidentes com Dados) não será interpretada como um reconhecimento por parte do Google de qualquer falha ou responsabilidade relativamente ao Incidente com Dados em questão.

7.3 **Responsabilidades e Avaliação de Segurança do Cliente**.

7.3.1 **Responsabilidades de Segurança do Cliente**. O Cliente concorda que, sem prejuízo das obrigações do Google previstas nas Seções 7.1 (Medidas e Assistência de Segurança do Google) e 7.2 (Incidentes com Dados):

(a) o Cliente é responsável pelo uso que fizer dos Serviços de Operador, incluindo:

(i) pelo uso apropriado dos Serviços de Operador a fim de garantir um nível de segurança adequado ao risco no que diz respeito aos Dados Pessoais do Cliente; e

(ii) pela proteção das credenciais de autenticação de contas, sistemas e dispositivos que o Cliente usa para ter acesso aos Serviços de Operador; e

(b) o Google não tem a obrigação de proteger os Dados Pessoais do Cliente que o Cliente armazenar ou transferir para fora dos sistemas do Google ou dos sistemas dos Sub-operadores do Google.

7.3.2 **Avaliação de Segurança do Cliente**. O Cliente reconhece e concorda que as Medidas de Segurança implementadas e mantidas pelo Google, nos termos previstos na Seção 7.1.1 (Medidas de Segurança do Google), oferecem um nível de segurança apropriado ao risco no que diz respeito aos Dados Pessoais do Cliente, considerando as tecnologias atuais, os custos de implementação e a natureza, o escopo, o contexto e as finalidades do tratamento dos Dados Pessoais do Cliente, bem como os riscos para as pessoas físicas.

7.4 **Certificação de Segurança**. Para avaliar e ajudar a garantir a eficiência contínua das Medidas de Segurança, o Google manterá a Certificação ISO 27001.

7.5 **Verificação de Compliance**. Para demonstrar o cumprimento pelo Google das respectivas obrigações ao abrigo destes Termos de Tratamento de Dados, e para auxiliar o Cliente a verificar o cumprimento pelo Google (i) das Instruções do Cliente; (ii) das obrigações do Google de acordo com estes Termos de Tratamento de Dados; e (iii) das obrigações do Google de acordo com a Legislação Aplicável em matéria de Proteção de Dados, o Google:

(a) disponibilizará a Documentação de Segurança para análise por parte do Cliente;

(b) fornecerá as informações contidas nos Termos de Tratamento de Dados; e

(c) fornecerá ou disponibilizará, de acordo com as práticas padrão do Google, outros materiais relacionados à natureza dos Serviços de Operador e do tratamento de Dados Pessoais do Cliente (por exemplo, materiais da Central de Ajuda).

O Cliente também pode verificar o cumprimento por parte do Google das respectivas obrigações ao abrigo destes Termos de Tratamento de Dados através da análise do certificado emitido para a Certificação ISO 27001 (que reflete o resultado de uma auditoria realizada por um auditor terceirizado).

8. Relatórios de Impacto e Consultas

O Google (levando em conta a natureza do tratamento e as informações disponíveis para o Google) auxiliará o Cliente a garantir o cumprimento das obrigações do Cliente (ou, caso o Cliente seja um operador, das obrigações do controlador relevante) relacionadas a relatórios de impacto à proteção de dados e consultas regulatórias prévias previstas na Legislação Aplicável em matéria de Proteção de Dados, das seguintes formas:

(a) fornecimento da Documentação de Segurança prevista na Seção 7.5 (Verificação de Compliance);

(b) fornecimento das informações contidas no Contrato (incluindo estes Termos de Tratamento de Dados); e

(c) fornecimento ou disponibilização, de acordo com práticas padrão do Google, de outros materiais referentes à natureza dos Serviços de Operador e do tratamento de Dados Pessoais do Cliente (por exemplo, materiais da Central de Ajuda).

9. Direitos do Titular dos Dados

9.1 **Respostas a Solicitações dos Titulares dos Dados**. Se o Google receber uma solicitação de um titular dos dados relacionada a Dados Pessoais do Cliente, o Cliente autoriza o Google a (e o Google desde já notifica o Cliente que irá):

(a) responder diretamente à solicitação do titular dos dados de acordo com a funcionalidade padrão da Ferramenta do Titular dos Dados (quando a solicitação tenha sido feita através dessa ferramenta); ou

(b) aconselhar o titular dos dados a enviar a sua solicitação ao Cliente e o Cliente será responsável por responder a tal solicitação (se a solicitação não for feita em uma Ferramenta do Titular dos Dados).

9.2 **Assistência por parte do Google a Solicitações dos Titulares dos Dados**. O Google ajudará o Cliente a cumprir as respectivas obrigações (ou, se o Cliente for um operador, as obrigações do controlador relevante) previstas na Legislação Aplicável em matéria de Proteção de Dados no sentido de responder às solicitações para exercício dos direitos dos titulares dos dados, tendo em conta, em todo caso, a natureza do tratamento dos Dados Pessoais do Cliente e, se aplicável, o disposto no Artigo 11.º do GDPR, das seguintes formas:

(a) fornecendo a funcionalidade dos Serviços de Operador;

(b) cumprindo os compromissos definidos na Seção 9.1 (Respostas a Solicitações dos Titulares dos Dados); e

(c) disponibilizando as Ferramentas dos Titulares dos Dados, se aplicáveis aos Serviços de Operador.

9.3 **Retificação**. Se o Cliente tomar conhecimento de que os Dados Pessoais do Cliente estão incorretos ou desatualizados, ele será responsável por retificar ou excluir esses dados, se tal for exigido pela Legislação Aplicável em matéria de Proteção de Dados, usando, inclusive, a funcionalidade dos Serviços de Operador (quando a mesma se encontrar disponível).

10. Transferências de Dados

10.1 **Instalações de Armazenamento e Tratamento de Dados**. O Google pode tratar Dados Pessoais do Cliente em qualquer país em que o Google ou seus Sub-operadores tenham instalações, sujeito a quaisquer disposições aplicáveis à transferência de dados determinadas nos Termos Adicionais.

10.2 **Informações do Data Center**. As informações sobre os locais onde estão instalados os data centers do Google estão disponíveis em www.google.com/about/datacenters/locations/.

11. Sub-operadores

11.1 **Autorização para Engajamento de Sub-operadores**. O Cliente autoriza especificamente o engajamento, como Sub-operadores, das entidades que, na Data de Início da Vigência dos Termos, se encontram listadas no URL especificado na Seção 11.2 (Informações sobre Sub-operadores). Além disso, sem prejuízo do disposto na Seção 11.4 (Oportunidade para se Opor a Alterações em Sub-operadores), o Cliente autoriza, de modo geral, o engajamento de outros terceiros como Sub-operadores ("**Novos Sub-operadores**").

11.2 **Informações sobre Sub-operadores**. As informações relativas aos Sub-operadores estão disponíveis em business.safety.google/adssubprocessors.

11.3 **Requisitos para o Engajamento de Sub-operadores**. Ao engajar qualquer Sub-operador, o Google:

(a) garantirá, através de um contrato escrito que o Sub-operador só acessa e utiliza os Dados Pessoais do Cliente na medida do necessário para cumprir as obrigações subcontratadas ao mesmo, e o faz em conformidade com o Contrato (incluindo estes Termos de Tratamento de Dados); e

(b) permanecerá totalmente responsável por todas as obrigações subcontratadas e por todos os atos e omissões do Sub-operador.

11.4 **Oportunidade para se Opor a Alterações em Sub-operadores**.

(a) Quando um novo Sub-operador for engajado durante o Período de Vigência, o Google informará ao Cliente do engajamento (incluindo o nome e a localização do respectivo Novo Sub-operador e as atividades que ele realizará), pelo menos 30 dias antes de o Novo Sub-operador tratar quaisquer Dados Pessoais do Cliente, através do envio de um e-mail para o Endereço de E-mail para Recebimento de Notificações.

(b) O Cliente poderá opor-se a qualquer novo Sub-operador rescindindo unilateralmente o Contrato com efeitos imediatos, mediante notificação por escrito ao Google, desde que o Cliente envie essa notificação em um prazo de até 90 dias após ter sido informado sobre o engajamento do novo Sub-operador, nos termos previstos na Seção 11.4(a).

12. Contato com o Google; Registros do Tratamento

12.1 **Contato com o Google**. O Cliente pode entrar em contato com o Google relativamente ao exercício de seus direitos previstos nestes Termos de Tratamento de Dados usando os meios descritos em privacy.google.com/businesses/processorsupport ou quaisquer outros meios que possam ser periodicamente disponibilizados pelo Google. O Google fornecerá assistência imediata e razoável para responder às dúvidas do Cliente recebidas por esses meios e que sejam referentes ao tratamento de Dados Pessoais do Cliente no âmbito do Contrato.

12.2 **Registros do Tratamento pelo Google**. O Google manterá uma documentação apropriada das suas atividades de tratamento,

conforme exigido pela Legislação Aplicável em matéria de Proteção de Dados.

12.3 **Solicitações de Controladores**. Se o Google receber uma solicitação ou instrução pelos meios descritos na Seção 12.1 (ou qualquer outro meio) de um terceiro que se apresente como controlador dos Dados Pessoais do Cliente, o Google orientará o terceiro a entrar em contato com o Cliente.

13. Limitação de responsabilidade

Se o Contrato for regido pela legislação de:

(a) um estado dos Estados Unidos da América, sem prejuízo de qualquer disposição no Contrato, a responsabilidade total de qualquer uma das partes em relação à outra parte decorrente ou relacionada a estes Termos de Tratamento de Dados será limitada ao valor monetário máximo ou ao valor baseado em pagamento a que a responsabilidade dessa parte está limitada ao abrigo do Contrato, não se aplicando, portanto, nenhuma exclusão de pedidos de indenização da limitação de responsabilidade prevista no Contrato a pedidos de indenização efetuados no âmbito do Contrato ao abrigo da Legislação Aplicável em matéria de Proteção de Dados; ou

(b) uma jurisdição que não seja um estado dos Estados Unidos da América, a responsabilidade das partes decorrente ou relacionada a estes Termos de Tratamento de Dados estará sujeita às exclusões e limitações de responsabilidade previstas no Contrato.

14. Efeitos destes Termos de Tratamento de Dados

14.1 **Ordem de Precedência**. Em caso de qualquer conflito ou inconsistência entre os Termos Adicionais, as restantes disposições destes Termos de Tratamento de Dados e/ou as restantes disposições do Contrato, será aplicada a seguinte ordem de precedência:

(a) os Termos Adicionais (se aplicável);

(b) as restantes disposições destes Termos de Tratamento de Dados; e

(c) as restantes disposições do Contrato.

Sujeito às alterações introduzidas por estes Termos de Tratamento de Dados, o Contrato permanece em vigor e a produzir efeitos.

14.2 **Não Produção de Efeitos sobre os Termos Aplicáveis a Controladores**. Estes Termos de Tratamento de Dados não afetarão os termos independentes celebrados entre o Google e o Cliente que reflitam uma relação controlador-controlador para um serviço diferente dos Serviços de Operador.

15. Alterações nestes Termos de Tratamento de Dados

15.1 **Alterações de URLs**. O Google pode periodicamente alterar qualquer URL mencionado nestes Termos de Tratamento de Dados e o conteúdo desses URLs. No entanto, o Google só pode mudar a lista de potenciais Serviços de Operador disponível em business.safety.google/adsservices:

(a) para refletir uma mudança no nome de um serviço;

(b) para adicionar um novo serviço; ou

(c) para remover um serviço (ou um recurso de um serviço) quando: (i) todos os contratos para a prestação desse serviço forem rescindidos; ou (ii) o Google tenha autorização da parte do Cliente; ou (iii) o serviço, ou um determinado recurso do serviço, foi recategorizado como um serviço de controlador.

15.2 **Alterações nos Termos de Tratamento de Dados**. O Google poderá modificar estes Termos de Tratamento de Dados se a alteração:

(a) for expressamente permitida por estes Termos de Tratamento de Dados, inclusive conforme descrito na Seção 15.1 (Alterações de URLs);

(b) refletir uma alteração no nome ou no tipo de uma entidade legal;

(c) for necessária para cumprir com o disposto numa lei ou regulamento aplicável, numa ordem judicial ou numa orientação expedida por um órgão regulador ou agência do governo, ou para refletir o uso por parte do Google de uma Solução de Transferência Alternativa (conforme definido no Apêndice 3A); ou

(d) não: (i) resultar em degradação da segurança geral dos Serviços de Operador; (ii) ampliar o escopo nem remover qualquer restrição sobre, (x) no caso dos Termos Adicionais, os dados incluídos no escopo dos Termos Adicionais ou, (y) no caso das restantes disposições destes Termos de Tratamento de Dados, o tratamento de Dados Pessoais do Cliente por parte do Google, conforme descrito na Seção 5.3 (Comprimento das Instruções pelo Google); e (iii) tiver um impacto negativo significativo sobre os direitos do Cliente ao abrigo destes Termos de Tratamento de Dados, conforme razoavelmente determinado pelo Google.

15.3 **Notificação de Alterações**. Caso o Google tenha a intenção de alterar estes Termos de Tratamento de Dados de acordo com o disposto na Seção 15.2(c) ou (d), o Google informará o Cliente pelo menos 30 dias antes de a alteração entrar em vigor, ou em um período menor, quando tal seja exigido por lei ou regulamento aplicável ou por uma ordem judicial ou orientação expedida por um órgão regulador ou agência do governo. Isso precisa ser feito (a) enviando uma mensagem para o Endereço de E-mail para Recebimento de Notificações ou (b) alertando o Cliente na interface do usuário dos Serviços de Operador. Caso o Cliente se oponha a qualquer uma dessas alterações, ele poderá rescindir unilateralmente o Contrato, com efeitos imediatos, enviando uma notificação por

escrito ao Google até 90 dias após ter sido informado de tal alteração.

Apêndice 1: Objeto e Detalhes do Tratamento de Dados

Objeto

A Prestação dos Serviços de Operador e de qualquer suporte técnico relacionado pelo Google ao Cliente.

Duração do Tratamento

O Período de Vigência, mais o tempo entre o fim desse período e a data de exclusão de todos os Dados Pessoais do Cliente pelo Google de acordo com estes Termos de Tratamento de Dados.

Natureza e finalidade do Tratamento

O Google tratará os Dados Pessoais do Cliente com a finalidade de prestar os Serviços de Operador e qualquer suporte técnico relacionado ao Cliente de acordo com estes Termos de Tratamento de Dados. O tratamento inclui a coleta, registro, organização, estruturação, armazenamento, alteração, recuperação, uso, divulgação, combinação, exclusão e destruição, conforme aplicável aos Serviços de Operador e às Instruções.

Tipos de dados pessoais

Os Dados Pessoais do Cliente podem incluir os tipos de dados pessoais descritos em business.safety.google/adsservices.

Categorias de titulares dos dados

Os Dados Pessoais do Cliente serão referentes às seguintes categorias de titulares dos dados:

- titulares dos dados sobre os quais o Google coleta dados pessoais ao prestar os Serviços de Operador e/ou

- titulares dos dados cujos dados pessoais são transferidos para o Google no âmbito dos Serviços de Operador, quer pelo Cliente, por instrução dele ou em nome dele.

Dependendo da natureza dos Serviços de Operador, esses titulares dos dados podem incluir indivíduos: (a) a quem tenha sido, ou venha a ser direcionada publicidade on-line; (b) que tenham visitado websites ou aplicativos específicos no âmbito dos quais o Google presta os Serviços de Operador; e/ou (c) que sejam clientes ou usuários dos produtos ou serviços do Cliente.

Apêndice 2: Medidas de Segurança

A partir da Data de Início da Vigência dos Termos, o Google implementará e manterá as Medidas de Segurança definidas neste Apêndice 2. O Google pode atualizar ou modificar essas Medidas de Segurança periodicamente, desde que essas atualizações e modificações não resultem na degradação da segurança geral dos Serviços de Operador.

1. Data Center e Segurança de Rede

(a) **Data centers.**

Infraestrutura. O Google mantém data centers distribuídos geograficamente. Ele armazena todos os dados de produção em data centers fisicamente protegidos.

Redundância. Os sistemas da infraestrutura foram criados para eliminar pontos únicos de falha e minimizar o impacto de riscos ambientais previsíveis. Circuitos duplos, interruptores, redes ou outros dispositivos necessários ajudam a proporcionar essa redundância. Os Serviços de Operador foram criados para permitir que o Google execute certos tipos de manutenção preventiva e corretiva sem interrupções. Todos os equipamentos e instalações ambientais têm procedimentos de manutenção preventiva documentados que detalham o processo e a frequência de desempenho de acordo com as especificações internas ou do fabricante. A manutenção preventiva ou corretiva dos equipamentos dos data centers é agendada por um processo padrão, de acordo com procedimentos documentados.

Energia. Os sistemas de energia elétrica dos data centers são desenvolvidos para serem redundantes e poderem passar por manutenção sem afetar as operações contínuas, 24 horas por dia, 7 dias por semana. Na maioria dos casos, é fornecida uma fonte de energia principal e uma alternativa, cada uma delas com a mesma capacidade, para componentes essenciais da infraestrutura do data center. Uma alimentação de reserva é fornecida por vários mecanismos como, por exemplo, baterias de fonte de alimentação ininterrupta (UPS, na sigla em inglês), que oferecem proteção elétrica consistentemente fiável durante blecautes parciais da concessionária de serviços públicos, blecautes, sobretensão/subtensão e condições de frequência fora da tolerância. Se a energia for interrompida, a alimentação de reserva fornecerá energia momentânea ao data center, na capacidade total, por um período de até 10 minutos, até que os sistemas de geradores de reserva sejam acionados. Os geradores de reserva podem ser inicializados de forma automática, em segundos, para fornecer energia elétrica de emergência suficiente para alimentar o data center na capacidade total normalmente por um período de dias.

Sistemas Operacionais dos Servidores. Os servidores do Google usam sistemas operacionais robustos que são customizados para as necessidades exclusivas dos servidores da atividade. Os dados são armazenados através de algoritmos exclusivos para aumentar a segurança e redundância dos dados. O Google emprega um processo de revisão de código para aumentar a segurança do código usado para prestar os Serviços de Operador e melhorar os produtos de segurança em ambientes de produção.

Continuidade do Negócio. O Google replica dados em vários sistemas para ajudar a protegê-los contra a sua destruição ou perda acidental. O Google desenvolveu, e planeja e testa regularmente os programas para recuperação de desastres/planejamento de continuidade do negócio.

Tecnologias de Criptografia. As políticas de segurança do Google exigem a criptografia em repouso para todos os dados do usuário, incluindo os dados pessoais. Os dados são geralmente

criptografados em vários níveis na pilha de armazenamento de produção do Google em data centers, inclusive no nível do hardware, sem necessidade de nenhuma ação por parte dos clientes. O uso de várias camadas de criptografia oferece proteção redundante aos dados e permite que o Google selecione a abordagem ideal com base nos requisitos do aplicativo. Todos os dados pessoais são criptografados quando são armazenados, geralmente usando AES256. O Google usa bibliotecas criptográficas comuns que incorporam o módulo FIPS 140-2 do Google para implementar a criptografia de forma consistente em todos os Serviços de Operador.

(b) **Redes e Transmissão**.

Transmissão de Dados. Os data centers são geralmente conectados através de links privados de alta velocidade que proporcionam uma transferência de dados segura e rápida entre os data centers. Além disso, o Google criptografa os dados transmitidos entre data centers para evitar que os dados sejam lidos, copiados, alterados ou removidos sem autorização durante o transporte eletrônico. O Google transfere dados através de protocolos padrão da Internet.

Superfície de Ataque Externo. O Google emprega várias camadas de dispositivos de rede e detecção de intrusão para proteger sua superfície de ataques externos. Ele considera os possíveis vetores de ataques e incorpora tecnologias específicas adequadas a sistemas externos.

Detecção de Intrusões. A detecção de intrusões tem o objetivo de fornecer informações sobre atividades de ataque em andamento e informações adequadas para responder a incidentes. A detecção de intrusão do Google consiste em:

1. Controlar de forma rigorosa o tamanho e a composição da superfície de ataque do Google com medidas preventivas;

2. Empregar controles de detecção inteligentes nos pontos de entrada de dados; e

3. Empregar tecnologias que resolvem automaticamente certas situações perigosas.

Resposta a Incidentes. O Google monitora uma variedade de canais de comunicação para incidentes de segurança. O pessoal de segurança do Google reagirá prontamente a incidentes identificados.

Tecnologias de Criptografia. O Google disponibiliza uma criptografia HTTPS, também chamada de "conexão TLS". Os servidores do Google são compatíveis com troca de chaves criptográficas efêmeras Diffie Hellman com base em curvas elípticas assinadas com RSA e ECDSA. Esses métodos de perfect forward secrecy (PFS) ajudam a proteger o tráfego e a minimizar o impacto de uma chave comprometida ou de uma inovação criptográfica.

2. **Controles de Acesso e do Local**

(a) **Controles do Local**.

Operação de Segurança Local nos Data Centers. Os data centers do Google mantêm uma operação de segurança local responsável por todas as funções físicas de segurança do data center, 24 horas por dia, 7 dias por semana. A equipe da operação de segurança local monitora câmeras do circuito fechado de TV (ou CCTV, na sigla em inglês) e todos os sistemas de alarme. A equipe da operação de segurança local realiza rondas internas e externas regularmente no data center.

Procedimentos de Acesso aos Data Centers. O Google mantém procedimentos formais para permitir o acesso físico aos data centers. Os data centers estão alojados em instalações que exigem acesso através de cartão eletrônico, com alarmes que estão ligados à operação de segurança local. Todas as pessoas que entram no data center são obrigadas a se identificar e mostrar um comprovante de identidade para a equipe de operações de segurança local. Somente funcionários, contratados e visitantes autorizados têm permissão para entrar nos data centers. Somente funcionários e contratados autorizados têm permissão para solicitar acesso por cartão eletrônico a essas instalações. As solicitações de acesso por cartão eletrônico precisam ser feitas com antecedência e por escrito e exigem autorização da equipe autorizada do data center. Todas as outras pessoas que precisam de acesso temporário ao data center devem: (i) obter autorização prévia da equipe do data center específico e das

equipes das áreas internas que querem visitar; (ii) identificar-se em todas as operações de segurança local; e (iii) apresentar um registro de acesso ao data center que identifique a pessoa como aprovada.

Dispositivos de Segurança Local dos Data Centers. Os data centers do Google empregam um sistema de cartão eletrônico e um sistema de controle de acesso biométrico que está ligado a um alarme do sistema. O sistema de controle de acesso monitora e registra a chave eletrônica de cada indivíduo e quando ele acessa as portas do perímetro, a área de envio/recebimento e outras áreas críticas. As atividades não autorizadas e as tentativas frustradas de acesso são registradas pelo sistema de controle de acesso e investigadas, quando adequado. O acesso autorizado às operações comerciais e aos data centers é restrito de acordo com as zonas e as responsabilidades inerentes à função da pessoa em questão. As portas corta-fogo nos data centers estão equipadas com alarmes. As câmeras de CCTV estão em funcionamento tanto dentro como fora dos data centers. O posicionamento das câmeras foi pensado para cobrir áreas estratégicas, incluindo, entre outras, o perímetro, as portas de acesso ao edifício dos data centers e as áreas de envio/recebimento. A equipe de operações de segurança local gerencia os equipamentos de monitoramento, gravação e controle de CCTV. O equipamento de CCTV é conectado por cabos fixos instalados ao longo dos data centers. As câmeras gravam o local 24 horas por dia, 7 dias por semana por meio de filmadoras digitais. Os registros de vigilância são mantidos por pelo menos sete dias, dependendo da atividade.

(b) **Controle de Acesso**.

Equipe de Segurança da Infraestrutura. O Google tem e mantém uma política de segurança para seu pessoal e exige treinamento de segurança como parte do pacote de treinamento da equipe. A equipe de segurança da infraestrutura do Google é responsável pelo monitoramento contínuo dessa infraestrutura, pela análise dos Serviços de Operador e por responder a incidentes de segurança.

Gerenciamento de Privilégios e Controle de Acesso. Os administradores e usuários do Cliente devem se autenticar através de

um sistema de autenticação central ou por logon único para poder usar os Serviços de Operador.

Políticas e Processos Internos de Acesso a Dados — Política de Acesso. As políticas e os processos internos de acesso a dados do Google são criados para evitar que pessoas e/ou sistemas não autorizados tenham acesso aos sistemas usados para tratar dados pessoais. O Google pretende conceber os seus sistemas de forma a: (i) permitir que apenas pessoas autorizadas tenham acesso aos dados que elas têm autorização para acessar; e (ii) garantir que os dados pessoais não possam ser lidos, copiados, alterados nem removidos sem autorização durante o tratamento, uso e posterior gravação. Os sistemas são desenvolvidos para detectar qualquer acesso indevido. O Google emprega um sistema centralizado de gerenciamento de acesso para controlar o acesso da equipe aos servidores de produção e só o concede a um número limitado de pessoas autorizadas. O LDAP, o Kerberos e um sistema próprio e exclusivo que utiliza certificados foram desenvolvidos para fornecer ao Google mecanismos de acesso seguros e flexíveis. Estes mecanismos foram concebidos para só conceder os direitos de acesso aprovados aos anfitriões, registros, dados e informações de configuração do site. O Google exige o uso de códigos de usuários únicos, senhas fortes, autenticação de dois fatores e listas de acesso cuidadosamente monitoradas para minimizar a possibilidade de uso não autorizado de contas. A concessão ou modificação de direitos de acesso se baseia nas responsabilidades inerentes às funções da equipe autorizada, nos requisitos necessários para a execução de tarefas autorizadas e no princípio da necessidade de saber. A concessão ou modificação de direitos de acesso também precisa estar de acordo com as políticas e o treinamento em matéria da acesso a dados internos do Google. As aprovações são gerenciadas por ferramentas de fluxo de trabalho que mantêm registros de auditoria de todas as alterações. O acesso a sistemas é registrado para criar uma trilha de auditoria para efeitos de responsabilização. Sempre que as senhas são empregadas para autenticação (por exemplo, no login em estações de trabalho), são implementadas políticas de senha que seguem pelo menos as práticas padrão do

setor. Esses padrões incluem restrições sobre a reutilização e o nível de segurança das senhas.

3. **Dados**

(a) **Armazenamento, Isolamento e Autenticação de Dados**.

O Google armazena dados em um ambiente multilocatário em servidores pertencentes ao Google. Os dados, o banco de dados dos Serviços de Operador e a arquitetura do sistema de arquivos são replicados em vários data centers espalhados em diversas áreas geográficas. O Google isola os dados de cada cliente de forma lógica. É usado um sistema de autenticação central em todos os Serviços de Operador para aumentar a segurança uniforme dos dados.

(b) **Discos Desativados e Orientações para a Destruição de Discos**.

Alguns discos que contêm dados podem apresentar problemas de desempenho, erros ou falhas de hardware que fazem com que eles sejam desativados ("**Disco Desativado**"). Todos os Discos Desativados são submetidos a uma série de processos de destruição de dados (as "**Orientações para a Destruição de Dados**") antes de deixar as instalações do Google para reutilização ou destruição. Os Discos Desativados são apagados em um processo de várias etapas e verificados por pelo menos dois avaliadores independentes. Os resultados da limpeza são registrados para efeitos de rastreamento pelo número de série do Disco Desativado. Por fim, o Disco Desativado apagado é liberado para o inventário para reutilização e reimplementação. Se, devido a uma falha de hardware, o Disco Desativado não puder ser apagado, ele será armazenado em segurança até que possa ser destruído. Cada instalação é auditada regularmente para monitoramento da conformidade com as Orientações para a Destruição de Dados.

(c) **Dados Pseudonimizados**.

Os dados de publicidade on-line são geralmente associados a identificadores on-line que, por si só, são considerados "pseudonimizados", ou seja, não podem ser atribuídos a um indivíduo específico sem o uso de informações adicionais. O Google dispõe de um conjunto robusto de políticas e controles técnicos e

organizacionais em vigor para garantir a separação entre dados pseudonimizados e informações de identificação pessoal do usuário, ou seja, dados que possam ser usados para identificar ou contatar diretamente ou localizar com precisão um indivíduo, como é o caso dos dados da Conta do Google do usuário. As políticas do Google só permitem fluxos de informações entre dados pseudonimizados e dados pessoais em circunstâncias estritamente limitadas.

(d) **Análises de lançamento**.

O Google conduz análises antes do lançamento de novos produtos e funcionalidades. O que inclui uma análise de privacidade realizada por engenheiros de privacidade especialmente treinados. Nas análises de privacidade, os engenheiros de privacidade garantem que todas as políticas e diretrizes aplicáveis do Google foram seguidas, incluindo, mas não se limitando as políticas relacionadas à pseudonimização e à retenção e exclusão de dados.

4. Segurança da Equipe

A equipe do Google deve se comportar de maneira consistente com as orientações da empresa em matéria de confidencialidade, ética nos negócios, uso adequado e padrões profissionais. O Google realiza verificações de antecedentes razoavelmente apropriadas na medida do legalmente permitido e de acordo com a legislação trabalhista local e os regulamentos estatutários aplicáveis.

A equipe deve assinar um acordo de confidencialidade e confirmar o recebimento das Políticas de Privacidade e Confidencialidade do Google e que irá cumprir com elas. A equipe recebe treinamento de segurança. Aqueles que lidam com Dados Pessoais do Cliente precisam satisfazer outros requisitos adequados à respetiva função. A equipe do Google não tratará Dados Pessoais do Cliente sem autorização.

5. Segurança do Sub-operador

Antes da integração dos Sub-operadores, o Google realiza uma auditoria às práticas de segurança e privacidade dos Sub-operadores para garantir que eles fornecem um nível de segurança e privacidade adequado ao acesso deles a dados e ao escopo dos serviços que precisam prestar. Depois que o Google avalia os riscos apresentados pelo Sub-operador, este precisa assinar

termos contratuais em matéria de segurança, confidencialidade e privacidade adequados, sempre sujeitos aos requisitos definidos na Seção 11.3 (Requisitos para o Engajamento de Sub-operadores).

Apêndice 3: Termos Adicionais para Legislação Aplicável em matéria de Proteção de Dados

PARTE A - TERMOS ADICIONAIS PARA A LEGISLAÇÃO EUROPEIA EM MATÉRIA DE PROTEÇÃO DE DADOS

1. Introdução

Este Apêndice 3A será aplicado apenas quando a Legislação Europeia em matéria de Proteção de Dados for aplicável para o tratamento de Dados Pessoais do Cliente.

2. Definições Adicionais

2.1 Neste Apêndice 3A:

"**Autoridade Supervisora**" significa, conforme aplicável: (a) uma "autoridade supervisora" conforme definida no GDPR da UE; e/ou (b) o "Comissário" conforme definido no GDPR do Reino Unido e/ou na FDPA da Suíça.

"**EEE**" significa o Espaço Econômico Europeu.

"**Legislação Europeia**" significa, conforme aplicável: (a) a legislação da UE ou de um Estado-Membro da UE, caso o GDPR da UE seja aplicável ao tratamento de Dados Pessoais do Cliente; (b) a legislação do Reino Unido ou de uma parte do Reino Unido, caso o GDPR do Reino Unido seja aplicável ao tratamento de Dados Pessoais do Cliente; e (c) a legislação da Suíça, caso a FDPA da Suíça seja aplicável ao tratamento de Dados Pessoais do Cliente.

"**País Adequado**" significa:

(a) para dados tratados e sujeitos ao GDPR da UE: o EEE ou um país ou território que seja considerado como tendo proteções adequadas de acordo com o GDPR da UE;

(b) para dados tratados e sujeitos ao GDPR do Reino Unido: o Reino Unido ou um país ou território que seja considerado como tendo proteções adequadas de acordo com o GDPR do Reino Unido e a Lei de Proteção de Dados de 2018; e/ou

(c) para dados tratados e sujeitos à FDPA da Suíça: a Suíça ou um país ou território: (i) incluído na lista de estados cuja legislação garante a proteção de dados, conforme publicado pelo Comissário Federal de Proteção e Informação de Dados da Suíça; ou (ii) que cumpre a proteção de dados estabelecida pelo Conselho Federal da Suíça de acordo com a FDPA da Suíça; em todos os casos, exceto quando há uma estrutura opcional de proteção de dados.

"**SCCs**" são as Cláusulas Contratuais Padrão (SCCs, na sigla em inglês) do Cliente e/ou SCCs (Operador para Operador, Exportador do Google), conforme aplicável.

"**SCCs (Controlador para Operador)**" significa os termos disponíveis em business.safety.google/adsprocessorterms/sccs/c2p.

"**SCCs (Operador para Controlador)**" significa os termos disponíveis em business.safety.google/adsprocessorterms/sccs/p2c.

"**SCCs (Operador para Operador)**" significa os termos disponíveis em business.safety.google/adsprocessorterms/sccs/p2p.

"**SCCs (Operador para Operador, Exportador do Google)**" significa os termos disponíveis em business.safety.google/adsprocessorterms/sccs/p2p-intra-group.

"**SCCs do Cliente**" são as SCCs (Controlador para Operador), as SCCs (Operador para Controlado) e/ou as SCCs (Operador para Operador), conforme aplicável.

"**Solução de Transferência Alternativa**" significa uma solução, que não seja as Cláusulas Contratuais Padrão de Controlador, que permita

a transferência legal de informações pessoais para um terceiro país de acordo com a Legislação Europeia em matéria de Proteção de Dados, por exemplo, uma estrutura de proteção de dados que garanta que as entidades locais participantes forneçam a proteção adequada.

2.2 Os termos "**importador de dados**" e "**exportador de dados**" terão os significados atribuídos a eles nas SCCs aplicáveis.

3. **Clientes Operadores.** Se o Cliente for um operador, o Cliente encaminhará, imediatamente e sem qualquer atraso, ao controlador relevante quaisquer notificações referentes a todas as SCCs.

4. **Legislação Europeia.** Quando a Legislação Europeia em matéria de Proteção de Dados for aplicável ao tratamento pelo Google dos Dados Pessoais do Cliente, o termo "legislação aplicável" nas Seções 5.3 (Comprimento das Instruções pelo Google), 6.1.1 (Serviços de Operador com Funcionalidades de Exclusão), 6.1.2(a) (Serviços de Operador sem Funcionalidades de Exclusão) e 6.2 (Exclusão no Final do Período de Vigência), se refere à "Legislação Europeia".

5. **Notificações de Instrução.** O Google notificará imediatamente o Cliente se, na opinião do Google: (a) a Legislação Europeia proibir o Google de cumprir uma Instrução; (b) uma Instrução não estiver em conformidade com a Legislação Europeia em matéria de Proteção de Dados; ou (c) o Google não puder cumprir uma Instrução por qualquer motivo, a menos que essa notificação seja proibida pela Legislação Europeia. Se o Cliente for um operador, o Cliente encaminhará imediatamente ao controlador relevante quaisquer notificações disponibilizadas pelo Google, ao abrigo deste parágrafo. Este parágrafo 5 (Notificações de Instrução) não reduz os direitos e as obrigações das partes dispostas em outras seções do Contrato.

6. **Auditorias de Conformidade**

6.1 **Direitos de Auditoria do Cliente**.

(a) O Google permitirá que o Cliente ou um auditor terceirizado indicado pelo Cliente realize auditorias (incluindo inspeções) para verificar o cumprimento pelo Google das respectivas obrigações ao abrigo destes Termos de Tratamento de Dados, nos termos previstos no parágrafo 6.2 (Termos

Comerciais Adicionais para Auditorias) deste Apêndice 3A. Durante uma auditoria, o Google disponibilizará todas as informações necessárias para demonstrar esse cumprimento e contribuirá com as auditorias conforme descrito na Seção 7.4 (Certificação de Segurança) e no parágrafo 6 (Auditorias de Conformidade) deste Apêndice 3A.

(b) Se as SCCs forem aplicáveis, nos termos do disposto no parágrafo 7.1 (Transferências Europeias Restritas) deste Apêndice 3A, o Google permitirá que o Cliente, ou um auditor terceirizado indicado por ele, conduza auditorias nos termos previstos nas SCCs e disponibilizará, durante a auditoria, todas as informações exigidas pelas SCCs, de acordo com o disposto no parágrafo 6.2 (Termos Comerciais Adicionais para Auditorias) deste Apêndice 3A.

6.2 **Termos Comerciais Adicionais para Auditorias.**

(a) O Cliente enviará ao Google todas as solicitações para a realização de uma auditoria ao abrigo do parágrafo 6.1(a) ou 6.1(b) deste Apêndice 3A, nos termos previstos na Seção 12.1 (Contato com o Google).

(b) Depois de receber uma solicitação ao abrigo do parágrafo 6.2(a) deste Apêndice 3A, o Google e o Cliente conversarão entre si e chegarão a um acordo sobre a data de início, o escopo e duração razoáveis, bem como os controles de confidencialidade e segurança aplicáveis a qualquer auditoria prevista nos parágrafos 6.1(a) ou 6.1(b) deste Apêndice 3A.

(c) O Google poderá cobrar uma taxa, com base nos custos razoáveis que tenha, para qualquer auditoria prevista nos parágrafos 6.1(a) ou 6.1(b) deste Apêndice 3A. O Google fornecerá ao Cliente mais detalhes sobre qualquer taxa aplicável e sobre a base de cálculo antes da realização da auditoria em questão. O Cliente será responsável pelas taxas cobradas por um auditor terceirizado indicado pelo Cliente para a execução da auditoria.

(d) O Google poderá opor-se a qualquer auditor terceirizado indicado pelo Cliente para a realização das auditorias previstas nos parágrafos 6.1(a) ou 6.1(b) deste Apêndice 3A se, segundo opinião razoável do Google, o auditor não estiver devidamente qualificado, não for um auditor independente, for um concorrente do Google ou for claramente inadequado. Qualquer objeção por parte do Google exigirá que o Cliente indique outro auditor ou conduza a auditoria por conta própria.

(e) As disposições contidas nestes Termos de Tratamento de Dados não exigem que o Google dê acesso ou divulgue ao Cliente ou ao auditor independente: (i) dados de qualquer outro cliente de uma Entidade do Google; (ii) informações financeiras ou contábeis internas de uma Entidade do Google; (iii) segredos comerciais de uma Entidade do Google; (iv) informações que, na opinião razoável do Google, possam: (A) comprometer a segurança dos sistemas ou instalações de qualquer Entidade do Google; ou (B) fazer com que uma Entidade do Google incumpra as obrigações decorrentes da Legislação Europeia em matéria de Proteção de Dados ou as obrigações de segurança e/ou privacidade para com o Cliente ou com terceiros; ou (v) informações que o Cliente ou o auditor independente tentem acessar por qualquer motivo que não seja o cumprimento de boa-fé das obrigações do Cliente decorrentes da Legislação Europeia em matéria de Proteção de Dados.

7. Transferências de Dados

7.1 **Transferências Europeias Restritas**. As partes reconhecem que a Legislação Europeia em matéria de Proteção de Dados não exige as SCCs nem uma Solução de Transferência Alternativa para tratar Dados Pessoais do Cliente em um País Adequado ou para transferir Dados Pessoais do Cliente para um País Adequado. Se os Dados Pessoais do Cliente forem transferidos para qualquer outro país e a Legislação Europeia em matéria de Proteção de Dados se aplicar às transferências (**"Transferências Europeias Restritas"**):

(a) caso o Google adote uma Solução de Transferência Alternativa para as Transferências Europeias Restritas, o Google informará o Cliente da solução relevante e garantirá que as Transferências Europeias Restritas em questão sejam realizadas de acordo com essa mesma solução; e/ou

(b) caso o Google não tenha adotado, ou tenha informado o Cliente de que não iria mais adotar uma Solução de Transferência Alternativa para as Transferências Europeias Restritas:

(i) se o endereço do Google estiver em um País Adequado:

(A) as SCCs (Operador para Operador, Exportador do Google) serão aplicáveis relativamente a essas mesmas Transferências Europeias Restritas do Google para Sub-operadores; e

(B) além disso, se o Cliente não estiver em um País Adequado, as SCCs (Operador para Controlador) serão aplicáveis relativamente às Transferências Europeias Restritas entre o Google e o Cliente (independentemente de o Cliente ser um controlador e/ou um operador); ou

(ii) se o endereço do Google não for de um País Adequado, as SCCs (Controlador para Operador) e/ou as SCCs (Operador para Operador) serão aplicáveis (desde que o Cliente seja um controlador e/ou um operador) relativamente às Transferências Europeias Restritas em questão entre o Cliente e o Google.

7.2 **Informações e Medidas Complementares**. O Google fornecerá ao Cliente informações relevantes para as Transferências Europeias Restritas, incluindo informações sobre medidas complementares para a proteção dos Dados Pessoais do Cliente, conforme descrito na Seção 7.5 (Verificação de Compliance), no Apêndice 2 (Medidas de Segurança) e outros materiais relativos à natureza dos Serviços de Operador e do tratamento de Dados Pessoais do Cliente (por exemplo, artigos da Central de Ajuda).

7.3 **Rescisão**. Se o Cliente concluir, com base no seu uso atual ou pretendido dos Serviços de Operador, que a Solução de Transferência Alternativa e/ou as SCCs, conforme aplicável, não fornecem um nível de proteção adequada para os Dados Pessoais do Cliente, o Cliente poderá rescindir unilateralmente o Contrato com efeitos imediatos, mediante notificação por escrito ao Google.

7.4 **Uso e Certificação da Solução de Transferência Alternativa**. Informações sobre o uso de, ou certificação para, Soluções de Transferência Alternativas pelo Google e/ou os Afiliadas dele podem ser encontradas em https://business.safety.google/adsdatatransfers.

8. **Sub-operadores**. Ao engajar qualquer Sub-operador, o Google garantirá (por um contrato escrito) que, se o tratamento de Dados Pessoais do Cliente estiver sujeito à Legislação Europeia em matéria de Proteção de Dados, o Sub-operador fica sujeito às obrigações em matéria de proteção de dados previstas nestes Termos de Tratamento de Dados (conforme disposto no Artigo 28(3) do GDPR, se aplicável).

9. **Registros do Tratamento pelo Google.**

O Cliente reconhece que, de acordo com o GDPR, o Google está obrigado a:

(a) coletar e manter registros de determinadas informações, incluindo: (i) o nome e os detalhes de contato de cada operador e/ou controlador em nome do qual o Google está agindo e (se aplicável) do representante local e do oficial de proteção de dados desse operador ou controlador, e (ii) a Autoridade Supervisora do Cliente, se aplicável ao abrigo das SCCs do Cliente; e

(b) disponibilizar essas informações a qualquer Autoridade Supervisora. Da mesma forma, o Cliente, quando solicitado e se aplicável, fornecerá essas informações ao Google na interface do usuário dos Serviços de Operador ou por qualquer outro meio que possa ser disponibilizado pelo Google, e usará essa interface ou tais outros meios para garantir que todas as informações fornecidas sejam mantidas corretas e atualizadas.

10. **SCCs**

10.1 **Ordem de Precedência**. Em caso de qualquer conflito ou inconsistência entre as SCCs do Cliente e este Apêndice 3A, as restantes disposições destes Termos de Tratamento de Dados e/ou as restantes disposições do Contrato, as SCCs terão precedência.

10.2 **Não Introdução de Alterações nas SCCs**. O Contrato (incluindo estes Termos de Tratamento de Dados) não tem o objetivo de alterar ou contradizer as SCCs nem de prejudicar os direitos ou as liberdades fundamentais dos titulares dos dados previstos na Legislação Europeia em matéria de Proteção de Dados.

11. **Alterações nas SCCs**. O Google só pode alterar as SCCs de acordo com as seções 15.2(b) a 15.2(d) (Alterações aos Termos de Tratamento de Dados) ou para incorporar novas versões das SCCs que possam ser adotadas pela Legislação Europeia em matéria de Proteção de Dados. Em cada caso, isso só pode ser realizado de uma maneira que não afete a validade das SCCs sob a Legislação Europeia em matéria de Proteção de Dados.

PARTE B - TERMOS ADICIONAIS PARA AS LEIS ESTADUAIS DE PRIVACIDADE DOS EUA

1. **Introdução**

O Google pode oferecer e o Cliente pode habilitar determinadas configurações no produto, ajustes ou outras funcionalidades para os Serviços de Operador relacionados ao tratamento de dados restrito, conforme descrito na documentação de apoio disponível em business.safety.google/rdp e atualizada periodicamente ("**Tratamento de Dados Restrito**"). O Apêndice 3B reflete o acordo entre as partes para o tratamento de Dados Pessoais do Cliente e Dados Desidentificados (conforme definido abaixo) de acordo com o Contrato em conexão com as Leis Estaduais de Privacidade dos EUA e é vigente somente de acordo com a aplicabilidade de cada Lei Estadual de Privacidade dos EUA.

2. **Definições Adicionais e Interpretação**

Neste Apêndice 3B:

(a) "**Dados Desidentificados**" significa informações de dados que foram "desidentificados", de acordo com a definição do termo "deidentified"

no CCPA e do termo "de-identified" em outras Leis Estaduais de Privacidade dos EUA, quando divulgados de uma parte para outra.

(b) "**Instruções de RDP**" significa, coletivamente, as Instruções (conforme definidas nestes Termos de Tratamento de Dados) e as instruções do Cliente para o Google relacionadas ao tratamento de Dados Pessoais do Cliente conforme permitido pelas Leis Estaduais de Privacidade dos EUA para prestadores de serviços e operadores.

(c) "**Serviços de RDP**" significa os Serviços de Operador sujeitos ao Tratamento de Dados Restrito (RDP, na sigla em inglês).

(d) Os termos "**comercial**", "**cliente**", "**informações pessoais**", "**venda(s)**", "**vender**", "**prestador de serviço**" e "**compartilhamento**" conforme usados neste Apêndice 3B foram definidos nas Leis Estaduais de Privacidade dos EUA aplicáveis.

(e) O Cliente é o único responsável por cumprir cada uma das Leis Estaduais de Privacidade dos EUA ao usar os serviços do Google, incluindo o Tratamento de Dados Restrito.

3. Termos das Leis Estaduais de Privacidade Aplicáveis (sob o Tratamento de Dados Restrito).

3.1 Em relação aos Dados Pessoais do Cliente tratados sob o Tratamento de Dados Restrito, e na medida em que uma ou mais das Leis Estaduais de Privacidade dos EUA se aplique ao tratamento de Dados Pessoais do Cliente:

3.1.1 **Funções e Compliance Regulatória; Autorização.**

(a) **Responsabilidades do Operador e do Controlador.** As partes reconhecem e concordam que:

(i) o Apêndice 1 destes Termos de Tratamento de Dados descrevem o objeto e os detalhes do tratamento de Dados Pessoais do Cliente, sujeito às seguintes modificações:

(1) todas as referências aos "Serviços de Operador" são substituídas por "Serviços de RDP"; e

(2) a seção "Tipos de dados pessoais" é substituída pelos seguintes termos: "Os Dados Pessoais do Cliente podem incluir os tipos de dados pessoais descritos nas Leis Estaduais de Privacidade dos EUA."

(ii) o Google é um prestador de serviços e operador de Dados Pessoais do Cliente de acordo com as Leis Estaduais de Privacidade dos EUA; e

(iii) o cliente é um controlador ou operador, conforme aplicável, de Dados Pessoais do Cliente de acordo com as Leis Estaduais de Privacidade dos EUA.

(b) **Clientes Operadores.** Se o Cliente for um operador:

(i) O Cliente garante, de maneira contínua, que o controlador relevante autorizou: (A) as Instruções, (B) a designação do Google como outro operador por parte do Cliente e (C) o envolvimento do Google com subcontratados, conforme descrito no parágrafo 3.4 (Subcontratados) deste Apêndice 3B.

(ii) O Cliente encaminhará imediatamente ao controlador relevante qualquer notificação fornecida pelo Google de acordo com a Seção 7.2.1 (Notificação de Incidentes) destes Termos de Proteção de Dados e o parágrafo 3.4 (Subcontratados) deste Apêndice 3B.

(iii) O Cliente pode disponibilizar ao controlador relevante qualquer informação fornecida pelo Google de acordo com os parágrafos 3.2(b) (Direitos de Auditoria do Cliente) e 3.4 (Subcontratados) deste Apêndice 3B.

3.1.2 **Instruções do Cliente para Serviços de RDP**. Ao celebrar este Apêndice 3B, e relativamente aos Serviços de RDP, o Cliente instrui o Google a tratar Dados Pessoais do Cliente apenas de acordo com as Instruções de RDP.

3.1.3 **Compliance do Google com as Instruções de RDP**. Em relação aos Serviços de RDP, o Google cumprirá as Instruções de RDP, exceto quando proibido pelas Leis Estaduais de Privacidade dos EUA.

3.1.4 **Produtos Adicionais.** Se o Cliente usar qualquer produto, serviço ou aplicativo fornecido pelo Google ou terceiros que: (a) não faça parte dos Serviços de RDP; e (b) esteja acessível para uso em uma interface do usuário dos Serviços de RDP ou integrado de outra forma aos Serviços de RDP (um "**Produto Adicional**"), os Serviços de RDP podem permitir que o Produto Adicional acesse os Dados Pessoais do Cliente conforme necessário para interoperação do Produto Adicional com os Serviços de RDP. Para deixar claro, o Apêndice 3B não se aplica ao tratamento de dados pessoais relacionado ao fornecimento de qualquer Produto Adicional usado pelo Cliente, incluindo os dados pessoais transmitidos para o Produto Adicional ou pelo Produto Adicional.

3.2 **Segurança de dados**

3.2.1 **Responsabilidades e Avaliação de Segurança do Cliente.**

(a) **Responsabilidades de Segurança do Cliente.** Além das responsabilidades de segurança do Cliente descritas na Seção 7.3.1 destes Termos de Tratamento de Dados, o Cliente concorda que, sem prejuízo das obrigações do Google previstas nas Seções 7.1 (Medidas e Assistência de Segurança do Google) e 7.2 (Incidentes com Dados) destes Termos de Tratamento de Dados, o Cliente é responsável pelo próprio uso dos Serviços de RDP, incluindo: (1) pelo uso apropriado dos Serviços de RDP para garantir um nível de segurança adequado ao risco no que diz respeito aos Dados Pessoais do Cliente; e (2)

pela proteção das credenciais de autenticação de contas, sistemas e dispositivos que o Cliente usa para ter acesso aos Serviços de RDP.

(b) **Direitos de Auditoria do Cliente.**

(i) O Cliente pode realizar uma auditoria para verificar a compliance do Google com as obrigações segundo este Apêndice 3B. Ele fará isso solicitando e analisando (1) um certificado emitido para verificação de segurança que mostre o resultado de uma auditoria por um auditor independente (por exemplo, certificação SOC 2 Tipo II ou ISO/IEC 27001 ou outra certificação similar, ou outra certificação de segurança referente a uma auditoria realizada por um auditor independente aceito pelo Cliente e pelo Google) em até 12 meses a partir da data de solicitação do Cliente e (2) qualquer outra informação que o Google determinar que é razoavelmente necessária para o Cliente verificar a compliance.

(ii) Como alternativa, o Google pode, a seu único e exclusivo critério e em resposta à solicitação do Cliente, iniciar uma auditoria independente para verificar a compliance do Google com suas obrigações listadas neste Apêndice 3B. Durante tal auditoria, o Google disponibilizará ao auditor independente todas as informações necessárias para demonstrar a compliance. Quando o Cliente solicitar esse tipo de auditoria, o Google pode cobrar uma taxa (baseada nos custos razoáveis do Google). O Google fornecerá ao Cliente mais detalhes sobre qualquer taxa aplicável e sobre a base de cálculo antes da realização

da auditoria em questão. O Cliente será responsável por quaisquer taxas cobradas por um auditor independente indicado pelo Cliente para a execução da auditoria.

(iii) Nada neste Apêndice 3B requer que o Google dê acesso ou divulgue ao Cliente ou ao auditor independente:

(1) dados de outro cliente de uma Entidade do Google;

(2) informações internas financeiras ou contábeis de uma Entidade do Google;

(3) segredos comerciais de uma Entidade do Google;

(4) informações que, na opinião razoável do Google, possam: (A) comprometer a segurança dos sistemas ou instalações de qualquer Entidade do Google; ou (B) fazer com que uma Entidade do Google incumpra as obrigações decorrentes das Leis Estaduais de Privacidade dos EUA ou as obrigações de segurança e/ou privacidade para com o Cliente ou terceiros; ou

(5) informações que o Cliente ou o auditor independente tentem acessar por qualquer motivo que não seja o cumprimento de boa-fé das obrigações do Cliente decorrentes das Leis Estaduais de Privacidade dos EUA.

3.3 **Direitos dos Titulares dos Dados**. Para o cumprimento deste Apêndice 3B, o Google obedecerá aos procedimentos listados na

Seção 9 (Solicitações dos Titulares dos Dados) na medida em que tais solicitações, pedidos de ajuda ou retificações sejam aplicáveis aos Serviços de RDP.

3.4 **Subcontratados.**

(a) O Cliente autoriza, em geral, o Google a contratar outras entidades como subcontratados para o fornecimento dos Serviços de RDP. Nessas contratações, o Google:

(i) vai garantir em um contrato escrito que: (A) o subcontratado use e acesse os Dados Pessoais do Cliente apenas para o que for necessário para executar as obrigações contratadas, seguindo o Contrato (incluindo o Apêndice 3B); e, (B) se o tratamento dos Dados Pessoais do Cliente estiver sujeito às Leis Estaduais de Privacidade dos EUA, garantir que as obrigações de proteção de dados neste Apêndice 3B sejam impostas ao subcontratado;

(ii) ao envolver novos subcontratados, o Google avisará ao Cliente sobre essas contratações e fornecerá a oportunidade de se opor às contratações, quando e onde for exigido pelas Leis Estaduais de Privacidade dos EUA; e

(iii) continuará totalmente responsável por todas as obrigações passadas ao subcontratado e por todos os atos e omissões do subcontratado.

(b) O Cliente poderá opor-se a qualquer novo subcontratado rescindindo unilateralmente o Contrato imediatamente mediante notificação por escrito ao Google, sob a condição de fornecer essa notificação em um prazo de até 90 dias após ter sido informado sobre o envolvimento do novo subcontratado, conforme descrito no parágrafo 3.4(a)(ii).

4. Termos das Leis Estaduais de Privacidade Aplicáveis

4.1 **Dados Desidentificados.** Em relação aos Dados Pessoais do Cliente tratados com ou sem ativação do Tratamento de Dados Restrito, e na

medida em que uma ou mais das Leis Estaduais de Privacidade dos EUA se aplique ao tratamento de Dados Pessoais do Cliente, cada parte cumprirá os requisitos para o tratamento de Dados Desidentificados descritos nas Leis Estaduais de Privacidade dos EUA, respeitando todos os Dados Desidentificados recebidos da outra parte, de acordo com o Contrato. Para os propósitos deste parágrafo 4, os Dados Pessoais do Cliente são todos os dados pessoais tratados por uma das partes de acordo com este Contrato no âmbito da prestação ou do uso dos Serviços de Operador.

5. Obrigações do Google relacionadas à CCPA.

5.1 Em relação aos Dados Pessoais do Cliente tratados sob o Tratamento de Dados Restrito, e na medida em que a CCPA se aplique a tal tratamento, o Google agirá como prestador de serviços do Cliente e, portanto, a menos que permitido para prestadores de serviço pela CCPA, conforme razoavelmente determinado pelo Google:

(i) o Google não venderá ou compartilhará os Dados Pessoais do Cliente que forem recebidos do Cliente e relacionados ao Contrato;

(ii) o Google não armazenará, usará ou divulgará os Dados Pessoais do Cliente (incluindo fora do relacionamento comercial direto entre o Google e o Cliente), exceto para fins comerciais provisionados na CCPA em nome do Cliente e para o propósito específico de executar os Serviços de RDP, conforme descrito na documentação de apoio disponível em business.safety.google/rdp e atualizado periodicamente;

(iii) o Google não combinará Dados Pessoais do Cliente que o Google receber do Cliente ou em nome dele com (i) informações pessoais que o Google receber de outra(s) pessoa(s) ou em nome dela(s), ou (ii) informações pessoais coletados da própria interação do Google com um cliente, conforme descrito em mais detalhes na documentação de apoio disponível em business.safety.google/rdp , exceto no limite do permitido pela CCPA;

(iv) o Google tratará esses Dados Pessoais do Cliente para a finalidade específica de realizar os Serviços de RDP, conforme descrito no Contrato e na documentação de apoio (por exemplo, artigos da Central de Ajuda) ou conforme permitido pela CCPA, e as partes concordam que o Cliente está disponibilizando os Dados Pessoais do Cliente ao Google para tais fins;

(v) o Google permitirá auditorias para verificar a compliance do Google com suas obrigações de acordo com este Apêndice 3B, conforme descrito no parágrafo 3.2.1(b) (Direitos de Auditoria do Cliente) deste Apêndice 3B;

(vi) o Google notificará o Cliente se determinar que não pode mais cumprir suas obrigações de acordo com a CCPA. Este parágrafo 5.1(vi) não reduz os direitos e as obrigações das partes dispostas em outras seções do Contrato;

(vii) se o Cliente acreditar razoavelmente que o Google está tratando Dados Pessoais do Cliente de maneira não autorizada, o Cliente tem o direito de notificar o Google sobre tal crença usando os métodos descritos em privacy.google.com/businesses/processorsupport, e as partes trabalharão juntas em boa-fé para remediar as atividades de tratamento supostamente violadoras, se necessário; e

(viii) o Google cumprirá as obrigações aplicáveis de acordo com a CCPA e fornecerá o mesmo nível de proteção de privacidade exigido pela CCPA.

5.2 Em relação aos Dados Pessoais do Cliente tratados sem a ativação do Tratamento de Dados Restrito, e na medida em que a CCPA se aplica ao tratamento de Dados Pessoais do Cliente:

(i) o Google tratará esses Dados Pessoais do Cliente para a finalidade específica de realizar os Serviços de Operador, conforme descrito no Contrato e na documentação de apoio (por exemplo, artigos da Central de Ajuda) ou conforme permitido pela CCPA, e as partes concordam que o Cliente

está disponibilizando os Dados Pessoais do Cliente ao Google para tais fins;

(ii) o Google permitirá auditorias para verificar a compliance do Google com as obrigações de acordo com este Apêndice 3B, conforme descrito no parágrafo 3.2.1(b) (Direitos de Auditoria do Cliente);

(iii) o Google notificará o Cliente se determinar que não pode mais cumprir suas obrigações de acordo com a CCPA;

(iv) se o Cliente acreditar razoavelmente que o Google está tratando Dados Pessoais do Cliente de maneira não autorizada, o Cliente tem o direito de notificar o Google sobre tal crença usando os métodos descritos em privacy.google.com/businesses/processorsupport, e as partes trabalharão juntas em boa-fé para remediar as atividades de tratamento supostamente violadoras, se necessário; e

(v) o Google cumprirá as obrigações aplicáveis de acordo com a CCPA e fornecerá o mesmo nível de proteção de privacidade exigido pela CCPA.

6. Alterações no Apêndice 3B.

Além da Seção 15 dos Termos de Tratamento de Dados (Alterações nestes Termos de Tratamento de Dados), o Google pode alterar este Apêndice 3B sem aviso prévio se a alteração (a) for baseada na legislação aplicável, em regulamentos aplicáveis, numa ordem judicial ou numa orientação emitida por um órgão regulador ou agência do governo, ou (b) não tenha um impacto material adverso sobre o Cliente de acordo com as Leis Estaduais de Privacidade dos EUA, conforme determinado razoavelmente pelo Google.

Termos de Tratamento de Dados de Publicidade do Google, Versão 8.0

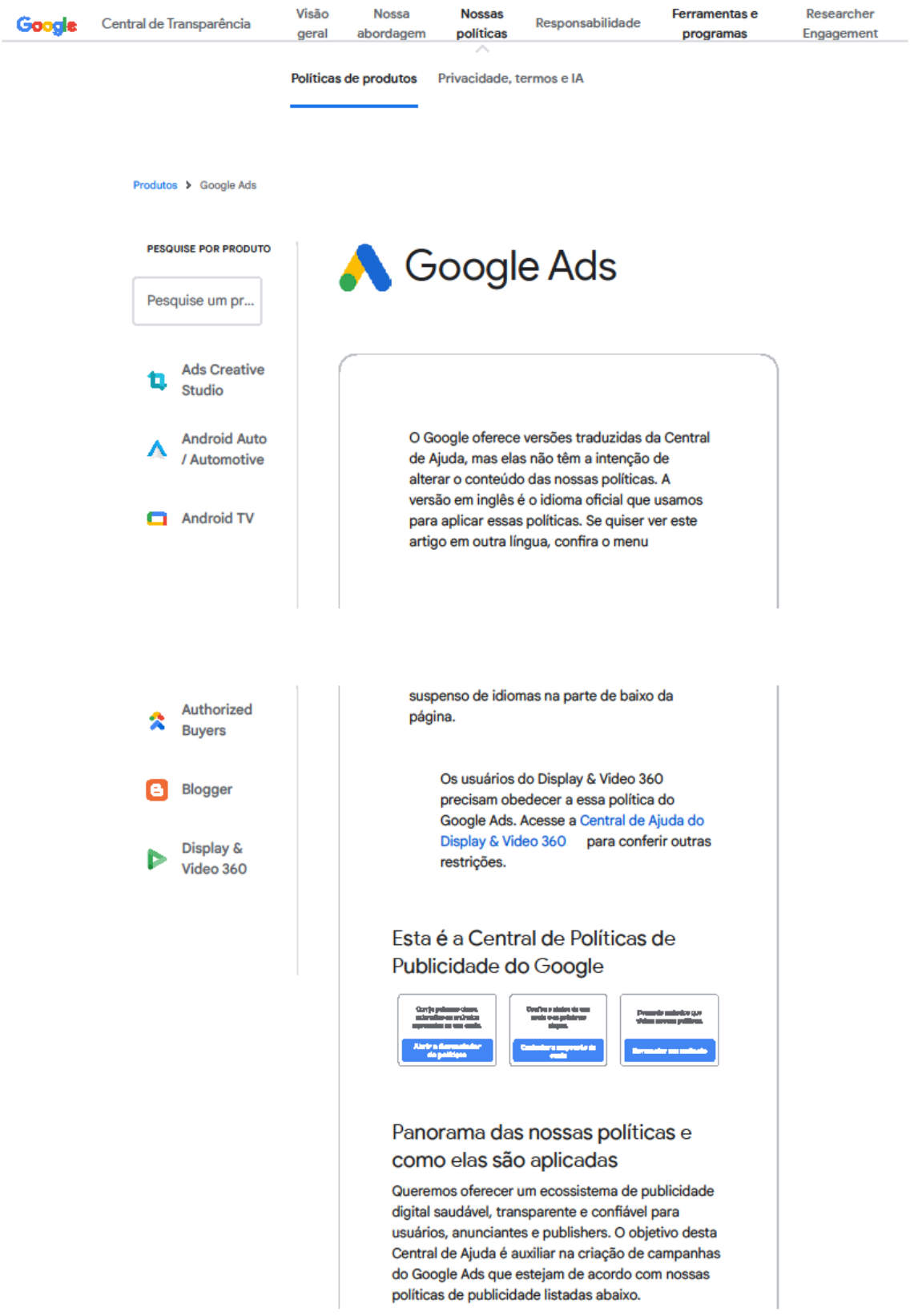
10 de setembro de 2024

Versões anteriores

- 1º de setembro de 2023

- 1º de julho de 2023
- 1º de janeiro de 2023
- 21 de setembro de 2022
- 16 de agosto de 2020
- 12 de agosto de 2020
- 1º de janeiro de 2020
- 31 de outubro de 2019
- 12 de outubro de 2017

APÊNDICE C - GOOGLE ADS — DIRETRIZES E POLÍTICAS — CENTRAL DE TRANSPARÊNCIA



Essas políticas foram estabelecidas para garantir uma experiência segura e positiva aos usuários, além de seguir as leis vigentes. Sendo assim, proibimos a veiculação de conteúdo que seja prejudicial aos usuários e ao ecossistema geral de publicidade.

Nossas políticas de publicidade abrangem quatro áreas amplas:

Conteúdo proibido: conteúdo que não pode ser anunciado na Rede do Google.

Práticas proibidas: ações que você não poderá realizar se quiser anunciar no Google.

Conteúdos e recursos restritos: conteúdo que pode ser anunciado, mas com limitações.

Requisitos editoriais e técnicos: padrões de qualidade para anúncios, sites e apps.

Para saber quais políticas estão incluídas nessas categorias amplas, clique no link de cada uma dessas categorias para ver o conteúdo abaixo. Clique no cabeçalho da seção para conferir mais detalhes sobre cada política.

Usamos uma combinação de IA do Google e avaliação humana para garantir que os anúncios obedeçam a essas políticas. Nossas tecnologias de restrição contam com a IA do Google, treinada nas decisões de revisores humanos, para proteger os usuários e manter a segurança das nossas plataformas de publicidade. Casos mais complexos, específicos ou graves costumam ser revisados e avaliados pelos nossos especialistas.

Nós tomamos as medidas necessárias quando o conteúdo viola as políticas. Isso inclui a reprovação de anúncios, o que impede a veiculação deles, e a suspensão de contas por violações repetidas ou graves. Levamos a sério as violações recorrentes das nossas políticas e continuamos ampliando o sistema de advertências para quem faz isso.

Vamos informar o motivo das nossas ações de fiscalização quando houver uma violação da política. Se um dos seus anúncios for reprovado, corrija o problema ou conteste a decisão . Também é possível contestar uma decisão de suspensão da conta . Para que esses links funcionem, faça login na sua conta do Google Ads.

Observação: no caso de reprovações de anúncios do DV360, saiba como encontrar e corrigir criativos rejeitados . Também é possível contestar uma suspensão de conta do DV360 .

Conteúdo proibido

Produtos falsificados

O Google Ads proíbe a venda ou promoção de produtos falsificados. Esses produtos contêm um logotipo ou uma marca registrada idêntica ou que possui diferenças mínimas em relação à marca verdadeira. Eles imitam as características da marca no produto em uma tentativa de se passar por produtos originais do proprietário da marca. Esta política se aplica ao conteúdo do seu anúncio e do seu site ou aplicativo.

Produtos ou serviços perigosos

Queremos proteger as pessoas on-line e off-line. Sendo assim, não permitimos a promoção de alguns produtos ou serviços que causam danos, prejuízos ou ferimentos.

Alguns exemplos de conteúdo perigoso: drogas recreativas (químicas ou à base de plantas); substâncias psicoativas; equipamentos para facilitar o uso de entorpecentes; armas, munições, materiais explosivos e fogos de artifício; instruções para a confecção de bombas ou outros produtos nocivos; derivados do tabaco.

Permissão de comportamento desonesto

Valorizamos a honestidade e a justiça. Por isso, não permitimos a promoção de produtos ou serviços que viabilizam comportamentos desonestos.

Alguns exemplos de produtos ou serviços que permitem comportamento desonesto: software ou instruções para invasões; serviços que aumentam artificialmente o tráfego do anúncio ou do site; documentos falsificados; serviços de fraude acadêmica.

Conteúdo inadequado

Valorizamos a diversidade e o respeito e não queremos ofender os usuários. Por isso, não permitimos anúncios ou destinos que mostram conteúdo chocante ou promovem ódio, intolerância, discriminação ou violência.

Alguns exemplos de conteúdo inadequado ou ofensivo: bullying ou intimidação de um indivíduo ou grupo; discriminação racial; conteúdo que promove grupos de ódio ou produtos relacionados; imagens explícitas de cenas de crimes ou de acidentes; crueldade com animais; assassinato; automutilação; extorsão ou chantagem; venda ou comércio de espécies ameaçadas de extinção; anúncios com linguagem obscena; e conteúdo que promova exploração sexual de menores.

Práticas proibidas

Abuso da rede de publicidade

Os anúncios em toda a Rede do Google precisam ser úteis, variados, relevantes e seguros para os usuários. O Google Ads não permite que os anunciantes veiculem publicidade, conteúdo ou destinos que tentem enganar ou burlar nossos processos de revisão.

Saiba mais sobre a política de abuso da rede de publicidade .

Alguns exemplos de abuso da rede de publicidade: promoção de conteúdo que contém malware; prática de cloaking ou outras técnicas para ocultar o verdadeiro destino dos usuários; arbitragem ou promoção de destinos com a finalidade exclusiva ou principal de mostrar anúncios; promoção de destinos intermediários ou gateway criados exclusivamente para enviar as pessoas a outros locais; publicidade com a intenção única ou principal de ganhar apoio público do usuário nas redes sociais; manipulação de configurações na tentativa de contornar nossos sistemas de análise de conformidade com a política.

Coleta e uso de dados

Queremos que os usuários confiem que as respectivas informações pessoais serão respeitadas e tratadas com os devidos cuidados. Sendo assim, nossos parceiros de publicidade não devem usar essas informações de modo inadequado nem fazer a coleta para fins pouco claros ou sem as medidas apropriadas de segurança ou divulgação.

Há políticas adicionais sobre o uso da publicidade personalizada, que inclui remarketing e públicos-alvo personalizados . Se você utiliza recursos de segmentação de publicidade personalizada, leia as políticas sobre coleta e uso de dados de anúncios personalizados.

Alguns exemplos de informações sobre o usuário que devem ser tratadas com cuidado: nome completo; e-mail; endereço de correspondência; número de telefone; carteira de identidade, pensão, Previdência Social, CPF/CNPJ, matrícula de convênio médico ou número da carteira de habilitação; data de nascimento ou nome de solteira da mãe, além de uma das informações mencionadas acima; situação financeira; filiação política; orientação sexual; raça ou etnia; religião.

Alguns exemplos de coleta e uso irresponsável de dados: coleta de informações de cartão de crédito em um servidor não seguro; promoções que afirmam conhecer a orientação sexual ou situação financeira de um usuário; violações das nossas políticas que se aplicam à publicidade com base em interesses e ao remarketing .

Deturpação

Queremos que os usuários confiem nos anúncios da nossa plataforma. Sendo assim, fazemos todo o possível para que eles sejam claros e verdadeiros, além de oferecerem as informações necessárias para que as pessoas tomem decisões fundamentadas. Não permitimos anúncios ou destinos que excluam informações relevantes dos produtos para tentar confundir os usuários ou que exibam conteúdo enganoso sobre produtos, serviços ou empresas.

Veja abaixo alguns exemplos de conteúdo que deve ser evitado nos seus anúncios. Saiba o que acontece quando nossas políticas são violadas .

Alguns exemplos de deturpação: omissão ou encobrimento de detalhes de faturamento (por exemplo, como, quanto e quando os usuários serão cobrados); omissão ou encobrimento de encargos associados aos serviços financeiros, como taxas de juros, tarifas e multas; não apresentação de números fiscais ou de licença, dados de contato ou endereço físico quando relevante; ofertas que não estão efetivamente disponíveis; afirmações enganosas ou irreais sobre perda de peso ou ganho financeiro; coleta de doações sob falsos pretextos; realizar phishing ou alegar falsamente ser uma empresa respeitável para fazer os usuários darem informações pessoais ou financeiras valiosas.

Conteúdo e recursos restritos

As políticas a seguir abrangem conteúdos que podem ser sensíveis em termos jurídicos ou culturais. A publicidade on-line pode ser uma maneira eficiente de alcançar clientes. Porém, em áreas sensíveis, também nos esforçamos para evitar que esses anúncios apareçam em contextos inadequados.

Por essa razão, permitimos a promoção do conteúdo abaixo, mas de forma limitada. Essas promoções podem não aparecer para todos os usuários em todos os locais. Além disso, podemos pedir que os anunciantes atendam a outros requisitos para que

seus anúncios sejam qualificados. Nem todos os produtos, recursos ou redes de publicidade aceitam esse conteúdo restrito. Confira mais detalhes no Gerenciador de políticas .

Proteções de veiculação de anúncios para crianças e adolescentes

Nossas políticas de anúncios para crianças e adolescentes, em conjunto com outras políticas do Google Ads (incluindo, mas não se limitando àquelas relacionadas a bebidas alcoólicas, jogos de azar e alimentos com alto teor de gordura, açúcar e sal), são combinadas para reforçar as proteções que incluem:

- Desativação da personalização de anúncios
- Restrição de categorias e conteúdo de anúncios sensíveis

Esperamos que todos os nossos anunciantes sigam os requisitos legais ao usar nossos produtos, incluindo todos os regulamentos sobre publicidade para usuários com menos de 18 anos e todas as políticas do Google Ads. Saiba mais sobre nossas proteções para crianças e adolescentes e políticas de anúncios relevantes, quando elas se aplicam e o que significam para os anunciantes.

Conteúdo sexual

Os anúncios precisam respeitar as preferências do usuário e obedecer aos regulamentos legais. Restringimos certos tipos de conteúdo sexual nos anúncios e destinos. Eles só serão exibidos em um número limitado de situações, com base nas consultas de pesquisa, na idade do usuário e na legislação vigente de onde o anúncio está sendo veiculado. Os anúncios não podem segmentar menores de idade.

Saiba mais sobre o que acontece quando nossas políticas são violadas .

Alguns exemplos de conteúdo sexual restrito: órgãos genitais e seios femininos expostos; encontros para sexo casual; brinquedos sexuais; clubes de striptease; chats ao vivo com conotação sexual; modelos em poses sexualizadas.

Bebidas alcoólicas

Respeitamos as leis de bebidas alcoólicas vigentes e os padrões do setor. Portanto, não permitimos determinados tipos de publicidade relacionados a qualquer tipo de bebidas alcoólicas. Alguns tipos de anúncio relacionados a bebidas alcoólicas são permitidos desde que atendam às políticas abaixo, não segmentem menores de idade e segmentem apenas os países que têm permissão explícita para exibi-los.

Alguns exemplos de bebidas alcoólicas restritas: cerveja; vinho; saquê; destilados; champanhe; vinho fortificado; cerveja, vinho e bebidas destiladas sem álcool.

Direitos autorais

Respeitamos as leis de direitos autorais vigentes e protegemos os detentores desses direitos. Portanto, não permitimos anúncios que não têm autorização para usar conteúdo protegido por direitos autorais. Se você tiver permissão legal para utilizar esse tipo de conteúdo, inscreva-se para receber uma certificação (ou então no DV360) e começar a anunciar. Se você encontrar conteúdo não autorizado, envie uma denúncia relacionada a direitos autorais .

Alguns exemplos de conteúdo restrito e protegido por direitos autorais: sites ou apps que facilitem a distribuição off-line não autorizada de conteúdo protegido por direitos autorais; sites ou softwares não autorizados que capturem, copiem ou deem acesso a esse tipo de conteúdo.

Jogos de azar

Apoiamos a publicidade responsável de jogos de azar e respeitamos a legislação de jogos de azar vigente e os padrões do setor. Portanto, não permitimos determinados tipos de publicidade

permitidos se o anunciante for certificado pelo Google e segmentar apenas locais aprovados. Consulte as regulamentações dos locais que você quer segmentar.

Para a maioria das políticas de saúde, se sua campanha publicitária segmenta locais permitidos e o domínio tem a certificação adequada, seu anúncio é rotulado como Qualificado (limitado) e pode ser veiculado em locais permitidos.

Alguns exemplos de conteúdo restrito de saúde: recrutamento para estudos clínicos; testes domésticos de HIV; serviços de reabilitação de drogas e álcool; serviços de prescrição de medicamentos.

Conteúdo político

Esperamos que todos os anúncios e destinos políticos obedeçam às leis eleitorais e de campanha vigentes das regiões segmentadas pelos anúncios. Essa política inclui os "períodos de silêncio" eleitorais exigidos por lei.

Alguns exemplos de conteúdo político: promoção de partidos ou candidatos políticos; defesa de questões políticas.

Produtos e serviços financeiros

Queremos que os usuários tenham informações adequadas para tomar boas decisões financeiras. O objetivo das nossas políticas é oferecer aos usuários informações para que eles considerem os custos associados aos produtos e serviços financeiros, além de proteger as pessoas contra práticas nocivas ou enganosas. Para os fins desta política, são considerados produtos e serviços financeiros aqueles que estão relacionados ao gerenciamento ou investimento de dinheiro e criptomoedas , incluindo consultorias personalizadas.

Ao promover produtos e serviços financeiros, você precisa obedecer às regulamentações estaduais e locais de todos os locais segmentados pelos seus anúncios (por exemplo, incluir as divulgações específicas exigidas pela legislação vigente). Os anunciantes devem pesquisar por conta própria sobre a regulamentação vigente nos locais segmentados pelos anúncios.

Veja a seguir alguns requisitos da política relacionados a serviços financeiros, empréstimos pessoais e determinados produtos financeiros restritos. Como a publicidade on-line e a regulamentação estão sempre mudando, atualizamos continuamente esta política com mais diretrizes específicas para cada produto. Saiba mais sobre o que acontece quando nossas políticas são violadas .

Alguns exemplos de produtos e serviços financeiros restritos: empréstimos pessoais; modificação dos termos do empréstimo; serviços de recuperação de crédito.

Criptomoedas e produtos relacionados

Devido à natureza complexa e em constante evolução das regulamentações associadas a criptomoedas e produtos e serviços relacionados, permitimos que determinadas categorias de produtos e serviços relacionados a criptomoedas sejam anunciados com e sem certificação pelo Google em alguns casos.

Embora a maioria dos anunciantes precise da certificação do Google, existem algumas circunstâncias em que a certificação não é obrigatória.

Alguns exemplos de empresas de criptomoeda que podem não exigir certificação: empresas que aceitam pagamento em criptomoeda; hardware de mineração de criptomoeda; jogos NFT em que os jogadores podem comprar itens, como roupas virtuais para os personagens, consumidos ou usados em um jogo para aprimorar a experiência do usuário ou ajudar a avançar no jogo.

Alguns exemplos de empresas de criptomoeda que exigem certificação: corretoras, carteiras e

fundos de criptomoedas.

Ao promover criptomoedas e produtos relacionados, você precisa obedecer à regulamentação estadual e local do país ou região que seus anúncios segmentam. Para mais informações, consulte nossa lista com alguns exemplos de requisitos locais específicos . No entanto, os anunciantes precisam pesquisar por conta própria as regulamentações vigentes dos locais segmentados pelos seus anúncios.

Marcas registradas

Existem vários fatores que determinam quando as marcas registradas podem ser usadas em anúncios do Google Ads. Junto aos fatores descritos na nossa Central de políticas, estas políticas se aplicam somente quando o proprietário de uma marca registrada envia uma reclamação válida ao Google.

Requisitos legais

Você é responsável por garantir conformidade com todas as leis e regulamentações aplicáveis, além das políticas de publicidade do Google, de todos os locais onde seus anúncios são veiculados.

Outros negócios restritos

Restringimos a publicidade de determinadas empresas para evitar a exploração do usuário, mesmo que ela esteja em conformidade com outras políticas. Revisões e feedback contínuos de usuários, reguladores e autoridades de proteção ao consumidor nos ajudam a identificar produtos ou serviços propensos a abusos. Podemos limitar ou interromper anúncios de empresas que representem um risco desarrazoado à segurança ou à experiência do usuário.

Restrição de recursos e formatos de anúncio

Existem vários fatores que determinam o acesso a recursos e formatos de anúncio avançados no Google Ads. Determinados recursos e formatos de anúncio só ficam disponíveis para todos os anunciantes depois que eles atendem aos nossos requisitos específicos ou concluem o processo de certificação.

Veiculação de anúncios limitada

Para proteger a integridade do nosso ecossistema do Google Ads, limitamos as impressões de anúncios com alto potencial de resultar em abuso ou em uma experiência insatisfatória para os usuários. Nesses casos, apenas anunciantes qualificados poderão mostrar publicidade sem limites de impressões.

Saiba em que casos a veiculação de anúncios limitada é válida e quem são os anunciantes qualificados.

Requisitos editoriais e técnicos

Queremos veicular anúncios envolventes que não sejam desagradáveis nem de difícil interação. Sendo assim, desenvolvemos requisitos editoriais para ajudar a melhorar a experiência dos usuários com os seus anúncios. Também especificamos requisitos técnicos para ajudar os usuários e anunciantes a aproveitar ao máximo a variedade de formatos de anúncios que oferecemos.

Requisitos editoriais

Para oferecer uma experiência de qualidade aos usuários, o Google exige que todos os anúncios, recursos e destinos sigam altos padrões profissionais e editoriais. Só permitimos anúncios claros, com aparência profissional e que apresentam conteúdo relevante, útil e de fácil interação.

Alguns exemplos de promoções que não seguem esses requisitos editoriais e profissionais: anúncios excessivamente genéricos com frases vagas, como "Compre produtos aqui"; uso extravagante de palavras, números, letras, pontuação ou símbolos, como GRÁTIS, g-r-á-t-i-s e GR@TI$!!.

Requisitos de destino

Nosso objetivo é oferecer uma boa experiência quando os consumidores clicam em um anúncio. Portanto, os destinos precisam agregar valor exclusivo, além de serem funcionais, úteis e fáceis de navegar.

Alguns exemplos de promoções que não atendem aos requisitos de destino: URLs de visualização que não refletem com precisão o URL da página de destino; sites ou apps em construção; sites que não podem ser acessados em navegadores comuns; sites que desativaram o botão "Voltar" do navegador.

Requisitos técnicos

Para oferecer uma experiência envolvente ao usuário, o Google exige que todos os anúncios, recursos e destinos cumpram determinados requisitos técnicos para garantir que a publicidade seja útil e atrativa. Os anúncios precisam ser claros,

funcionais e direcionar os usuários a um conteúdo relevante e de fácil interação.

Alguns exemplos de promoção que não seguem os requisitos técnicos: exceder os limites da conta relacionados a anúncios e outros tipos de conteúdo; anúncios ou conteúdo de destino em um idioma de segmentação não disponível; anúncios em HTML5 que não funcionam corretamente ou aparecem em branco.

Requisitos de formato do anúncio

Para oferecer uma ótima experiência ao usuário e veicular anúncios atraentes e profissionais, permitimos apenas promoções que obedeçam aos requisitos de cada formato. Confira os requisitos de todos os formatos de anúncio que você usa.

Não é permitido usar publicidade não indicada para menores em anúncios gráficos, em vídeo e em outros formatos que não sejam de texto. Consulte nossa política de conteúdo sexual .

Os anunciantes que participam de programas Beta de novos formatos de anúncio precisam entrar em contato com os representantes ou com o suporte ao cliente do Google Ads para saber mais sobre os requisitos de política para cada formato.

Alguns exemplos de requisitos de formato do anúncio: limites de caracteres para o título ou o corpo do anúncio; requisitos de tamanho da imagem; limites de tamanho de arquivo; limites de duração do vídeo; proporções.

Sobre nossas políticas

O Google Ads permite que empresas de todos os tamanhos, do mundo todo, promovam uma ampla variedade de produtos, serviços, aplicativos e sites no Google e na nossa rede. Queremos ajudar você a alcançar os clientes e públicos-alvo atuais e em potencial. No entanto, para criar uma experiência segura e positiva para os usuários, ouvimos os comentários e preocupações sobre os tipos de anúncios que eles veem. Também revisamos regularmente mudanças nas tendências e práticas on-line, normas e regulamentos do setor. E por fim, elaboramos as políticas pensando em nossos valores e cultura como uma empresa, além de considerar as questões operacionais, técnicas e comerciais. Como resultado, criamos um conjunto de políticas válidas para todas as promoções na Rede do Google.

O Google exige que os anunciantes cumpram todas as leis e regulamentações relevantes , além das políticas descritas acima. É importante que você se familiarize e acompanhe esses requisitos para os locais onde sua empresa atua, bem como quaisquer outros lugares onde seus anúncios são veiculados.

Quando encontramos algum conteúdo que viola esses requisitos, bloquearemos a veiculação e, em casos de violações repetidas ou graves, impediremos que você veicule anúncios conosco.

É de responsabilidade dos anunciantes não promover conteúdo nem apresentar comportamento que coloque nossos usuários, funcionários ou o ecossistema de anúncios em risco. Caso contrário, tomaremos medidas, incluindo, mas não se limitando a restringir ou bloquear seus anúncios ou suspender sua conta.

Precisa de ajuda?

Se você tiver dúvidas sobre nossas políticas, entre em contato com o suporte do Google Ads . Classifique o nível de utilidade desta página e deixe seu feedback abaixo: