

A regulação de proteção
de dados e seu impacto
para a publicidade online:

UM GUIA PARA A LGPD



A REGULAÇÃO DE PROTEÇÃO DE DADOS E SEU IMPACTO PARA A PUBLICIDADE ONLINE: UM GUIA PARA A LGPD

Pedro H. Ramos

Sócio do Baptista Luz Advogados

Mestre em Direito e Desenvolvimento pela FGV/SP

SOBRE O AUTOR



Pedro Henrique Soares Melo Ramos

Advogado empresarial, com mais de 10 anos de experiência no atendimento a empresas de tecnologia, publicidade, telecomunicações e *mobile*, com foco nas áreas de Transações de Tecnologia, Publicidade e Proteção de Dados. Com graduação pela Universidade de São Paulo e Mestrado pela Fundação Getúlio Vargas, foi pesquisador associado do InternetLab e professor visitante da Stanford Law School, onde atuou junto com a equipe de pesquisa do *Center of Internet and Society* da universidade, desenvolvendo trabalhos sobre a regulação da internet, e que foram apresentados em fóruns como a *Telecommunications Policy and Research Conference* em 2014 e o *Internet Governance Forum* da ONU em 2015. Também foi professor convidado na Universidade de São Paulo, London School of Economics e Cornell Law School, sendo em 2017 um dos palestrantes do Mozilla Festival em Londres.

Com experiências anteriores na área de políticas públicas e na gestão de departamentos jurídicos de agências de publicidade online, integra desde 2010 o time do Baptista Luz Advogados, sendo atualmente sócio coordenador da equipe de Transações de Tecnologia, Mídia e Publicidade e Propriedade Intelectual, e co-coordenador da equipe de Proteção de Dados, atendendo grandes grupos de comunicação, empresas de tecnologia, fundos de investimento e empresas de telecomunicações. Entre 2015 e 2016, foi consultor do Ministério da Justiça na elaboração do decreto 8.771/16, que regulamentou o Marco Civil da Internet, e atualmente é membro do Subcomitê “Ambiente Normativo de Startups” do Comitê Interministerial para a Transformação Digital, instituído pelo Decreto n. 9.319/18.

Atualmente, é conselheiro do Grupo Dínamo, da Associação Brasileira de Startups e do Internet Advertising Bureau Brasil, onde também é coordenador dos cursos “Aspectos Jurídicas da Compra de Mídia Online” e “Influenciadores Digitais”. É autor dos livros “**Neutralidade da Rede: a regulação da arquitetura da internet no Brasil**” (Editora IASP) e “**Ambiente Regulatório: Manual de Boas Práticas em Políticas Públicas**” (Dínamo, em coautoria com Felipe Matos).

INTRODUÇÃO

A publicidade digital tem ganhado cada vez mais holofotes desde que a União Europeia aprovou, em 2016, a sua regulação geral de proteção de dados (conhecida mundialmente sob a sigla GDPR), e que entrou em vigor no ano passado. A GDPR motivou discursos de pânico e desinformação no setor de publicidade online desde sua publicação, em especial porque algumas de suas principais premissas [foram \(e tem sido\) mal interpretadas](#).

O fato de que algumas das ideias mais restritivas da GDPR foram transplantadas para diversas legislações do mundo, acabou aproximando essa tendência de desinformação também no Brasil, onde ano passado foi aprovada a nossa lei geral de proteção de dados (“LGPD”).

Nesse artigo, vamos esclarecer alguns desses mal-entendidos sobre proteção de dados e mídia digital, apresentando de que forma o mercado pode não só sobreviver, como também crescer e amadurecer muito com a legislação brasileira.

COMO A PUBLICIDADE DIGITAL FUNCIONA?

A mídia digital é um negócio complexo, baseado numa cadeia de *stakeholders* extensa e cheia de particularidades. No entanto, seus objetivos e premissas continuam sendo os mesmos de toda indústria de publicidade.

O modelo de negócio de toda e qualquer mídia sempre foi baseado em dados, desde o início. [Como até mesmo escritores como Noam Chomsky reconhecem](#), se jornais vivessem somente de assinaturas e o preço de venda, esses simplesmente faliriam. A publicidade direcionada, baseada em dados, sempre foi a forma mais eficiente de permitir que as pessoas tivessem acesso a conteúdo pagando menos, e pudessem ter acesso a anúncios mais relevantes e valiosos para cada perfil. Quando a mídia digital surge nos anos 1990, essa estrutura torna-se ainda mais radical, pois é nessa época em que se forma a ideia de [todo um setor baseado na premissa de que o acesso a conteúdo deve ser o mais aberto, livre e democrático possível](#), patrocinado por empresas que estivessem dispostas a pagar pela atenção dos usuários e oferecendo anúncios personalizados e relevantes.

Com o surgimento da internet comercial nos anos 1990, a publicidade contextual ganhou ainda mais importância: com sites de conteúdo cada vez mais especializados, agências e anunciantes buscavam *prever* o público desses sites, utilizando como referência o conteúdo de uma determinada página. Evidente, isso trazia um desafio: se o conteúdo de determinada página (como um portal de notícias) muda frequentemente, ou se o usuário consegue personalizar esse conteúdo através de sua interação com o site, como automatizar o processo de inserção de publicidade, evitando que agências precisem negociar pessoalmente, espaço por espaço, com cada veículo?

Como resposta a esse desafio, surgem ferramentas de tecnologia cujo objetivo principal é automatizar os processos de identificação de conteúdo nas páginas e entregar publicidade segmentada de acordo com o conteúdo identificado. Por meio de *cookies*, tags, gerenciadores de base de dados e outras tecnologias, essas ferramentas não buscavam redefinir o processo de negociação de publicidade, mas tão somente *automatizá-lo*. Surgem então tecnologias de **publicidade**

comportamental, que permitem a identificação do histórico de navegação do usuário e o processamento dessas informações em grandes bases de dados, de forma a segmentar a entrega de publicidade *especificamente* para aquele usuário que atende ao perfil de determinado anunciante.

Há, nesse momento, uma mudança paradigmática em relação ao valor da publicidade. A qualidade do espaço publicitário disponibilizado por determinado veículo para a inserção de um anúncio (ex. a capa de um site, o banner central, etc.) perde cada vez mais importância em precificação. De nada adianta um *banner* numa página importante de um site, se este anúncio não será relevante para a audiência. Essa transformação altera, inclusive, a forma como os valores são cobrados na publicidade online, que não são mais baseados na posição de determinado anúncio em um site, mas sim em modelos de monetização que contabilizam impressões (*cost per mile*, "CPM"), cliques (*cost per click*, "CPC") ou aquisições (*cost per acquisition*, "CPA"), mostrando cada vez mais a posição central que a audiência possui no processo de inserção de publicidade.

Quando esse processo começa a evoluir nos anos 2010, novos atores começam a surgir para além da tríade anunciante/agência/veículo. Esse novo ecossistema, formado por empresas que operam e distribuem **tecnologias hoje conhecidas como *adtechs***, oferece um conhecimento ainda mais preciso para garantir que os dados capturados da audiência possam

oferecer anúncios de maior relevância e úteis para os usuários, com uma redução de custo para anunciantes e aumento de receitas para veículos.

Em outras palavras, essas *adtechs* permitiram o que hoje chamamos de **compra de mídia programática**. Esse termo é, na verdade, um gênero para diversas espécies de modelos de negócio e protocolos técnicos para compra automatizada de espaços de mídia, sendo o mais conhecido deles o leilão em tempo real (*real time bidding*, "RTB").

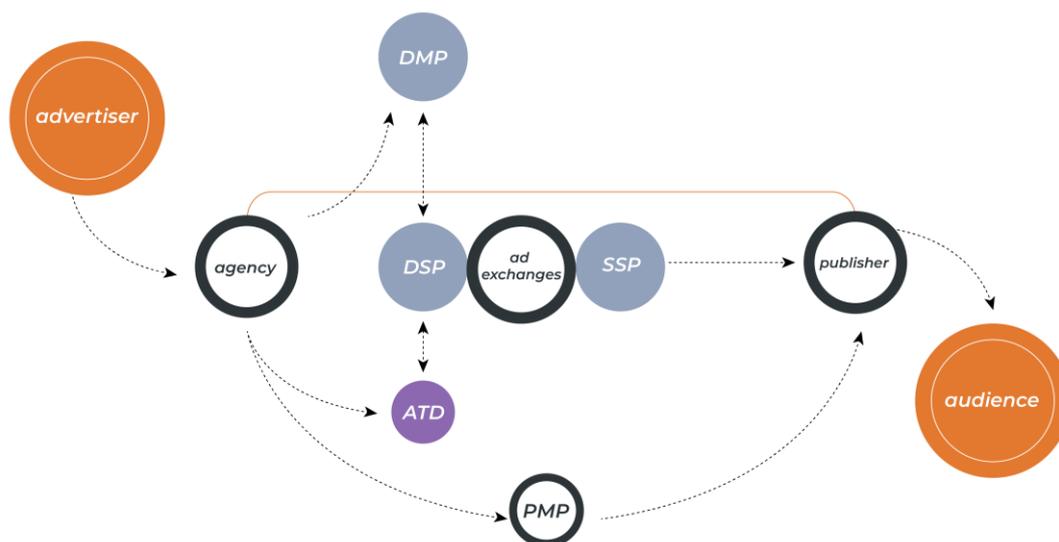
O RTB é um modelo transformador para o mercado, baseado em eficiência de custos e que ajudou o setor a ser mais assertivo e, ao mesmo tempo, garantir que os usuários pudessem receber anúncios melhores e mais atraentes. O modelo funciona, de forma bem simplificada, a partir de uma cadeia de dois lados, da seguinte forma:

- (i) no "**lado da oferta**", um veículo (como um site ou aplicativo) disponibiliza seu inventário de espaços publicitários por meio de soluções de software conhecidas como *supply-side platforms* ("SSP");
- (ii) essas SSPs vão enviar um pedido (conhecido como *bid request*), por conta e ordem do veículo, para um outro tipo de tecnologia, as *ad exchanges*;
- (iii) as *ad exchanges*, por sua vez, vão solicitar que compradores realizem uma oferta para aquele espaço publicitário;

- (iv) do outro lado da cadeia (o **“lado da demanda”**), possíveis compradores (anunciantes e agências de publicidade) vão enviar as suas ofertas de compra por meio de tecnologias conhecidas como *demand-side platforms* (“DSP”);
- (v) as DSPs também vão se conectar às *ad exchanges*, e vão analisar os *bid requests* enviados pelas SSPs;
- (vi) uma vez que todos estejam conectados nesse mesmo ambiente, as DSPs irão analisar os *bid requests* oferecidos pela SSPs, e apresentar uma proposta de preço (um lance) para inserir um anúncio naquele espaço publicitário
- (vii) a *ad exchange*, de maneira semelhante a um *leiloeiro*, irá coordenar a dinâmica entre os diferentes lances de DSPs para um determinado *bid request*;
- (viii) a DSP que oferecer o maior lance será vencedora, e as tecnologias irão trabalhar para que o anúncio vencedor seja inserido no espaço publicitário do *publisher* - todo esse processo dura apenas alguns milissegundos!

Além do gráfico e da explicação acima, o [Interactive Advertising Bureau \(“IAB”\)](#) possui [uma série de vídeos e cartilhas explicativas](#), que ajudam a entender bem esse modelo. Há também outros atores, como *agency trading desks*, *private marketplaces*, mas que não são relevantes para este estudo, além das *data management platforms*, que falaremos adiante. Há também diversas empresas que oferecem sistemas de RTB em ambientes fechados, isto é, ecossistemas que funcionam de maneira unificada, agregando duas ou mais tecnologias em uma única suíte de software – como a [Google](#) e a [Verizon Media](#).

Gráfico 1. O ecossistema de compra de mídia digital



Em suma, o modelo acima funciona como uma referência didática e ilustrativa para entendermos as questões de proteção de dados no ambiente de RTB, mas está longe de representar todo o ecossistema – que está em constante evolução. Atualmente, o investimento em publicidade online no Brasil representa cerca de [33% do mercado de](#)

[mídia – o equivalente a mais de 16 bilhões de reais](#). O modelo de compra direta, em que a agência negocia diretamente com o veículo, representa hoje pouco menos de 22% os investimentos de publicidade – ou seja, a grande maioria do mercado utiliza-se, direta ou indiretamente, de *adtechs* para realizar a compra de mídia digital.

GLOSSÁRIO - PRINCIPAIS EXPRESSÕES DO MERCADO

Ad Exchanges são plataformas de software que facilitam a compra e venda de inventário por meio de leilões, com várias partes envolvidas, que incluem: anunciantes, veículos, ad networks e plataformas de demanda (DSP).

Agency Trading Desks (ATDs) são empresas (ou uma divisão de uma empresa) focada na operação de tecnologias de compra de mídia.

Data Management Platforms (DMPs) são plataformas de software que permitem a anunciantes, agências e veículos gerenciarem dados de audiência, gerando informações que contribuem para a decisão de compra de mídia.

Demand Side Platforms (DSPs) são plataformas de software com foco no lado da demanda (anunciantes, trading desks e agências), e que automatizam a compra de mídia junto a Ad Exchanges e outras tecnologias.

Mídia Programática conjunto de processos automatizados para a compra e venda de mídia.

Private Marketplace (PMP) conjunto único de inventário privado de espaços publicitários, aberto a lances somente a DSPs cadastradas.

Real Time Bidding (RTB) é uma modalidade de mídia programática, que se utiliza de um protocolo para avaliação e realização de lances em impressões individuais em tempo real, no ambiente de Ad Exchanges.

Supply Side Platforms (SSPs) são plataformas de software com foco no lado da oferta (veículos), e que automatizam a venda de espaços publicitários junto a Ad Exchanges e outras tecnologias.

QUAL A RELAÇÃO ENTRE MÍDIA PROGRAMÁTICA E PROTEÇÃO DE DADOS?

Na mídia programática, embora as tecnologias em si sejam agnósticas e, por padrão, não necessariamente precisam usar dados pessoais de usuários, essas informações são importantes para garantir a publicidade direcionada e mais atraente para os usuários.

De um lado, SSPs vão informar, junto com sua oferta, qual usuário será impactado, naquele instante, por um anúncio veiculado em determinado espaço. Essas informações sobre o usuário são geralmente apresentadas e agrupadas por meio de um código, chamado "User ID". Do outro lado da cadeia, anunciantes, agências e DSPs podem utilizar tecnologias para gravar e tratar informações de usuários, com o objetivo de deduzir seus interesses e preferências. Essas informações podem ser, ainda, complementadas com outras tecnologias, como *Data Management Platforms* (DMPs), que integram diferentes fontes de dados e otimizam a criação desse *perfil de usuário*, agregando com outros dados, tornando-o mais completo, adequado e preciso.

O objetivo desse processo, naturalmente, é entender melhor que perfil de usuário está por trás daquele *User ID*, ajudar na decisão sobre o lance a ser realizado, reduzir custos da cadeia, e, em última instância, oferecer anúncios mais atraentes para os usuários (pagando menos por anúncios que determinado perfil provavelmente não irá achar tão atraente, e pagando mais por anúncios cujo perfil de audiência é mais adequado).

Os *User IDs* não são, em geral, informações pessoalmente identificadas, como um nome ou um CPF, até porque são marcados por meio de um número aleatório, gerado de acordo com o sistema utilizado. Ocorre que, em várias regulações recentes como a GDPR e a LGPD, o conceito de dado pessoal abrange não só a informação que identifica certo indivíduo, como aquela que *pode o identificar*, o que é exatamente o caso dos *User IDs*. Contudo, isso **não significa** que a GDPR ou a LGPD proibam a mídia programática. Esse tipo de argumento sensacionalista tem sido utilizado na Europa, com interesses econômicos, [pelos mesmos](#)

[atores que abusam do discernimento do usuário e tentam difamar a mídia online por meio de tecnologias de ad blocking.](#)

É importante ressaltar que, como já dito, as tecnologias de mídia programática são, *per se*, agnósticas. Por exemplo, o protocolo [OpenRTB](#) (principal protocolo técnico aberto utilizado no mercado) não exige que você inclua *User IDs* em nenhum lance. Se uma organização inclui informações em determinado *bid request* sem um fundamento legal que a autorize a fazer isso (“base legal”), isso não significa que a tecnologia em si é ilegal. Seria o mesmo de culpar o Microsoft Excel por permitir que um usuário faça uma planilha de caixa 2 com o programa. Da mesma forma, a cadeia de mídia programática não é uma “zona livre de proteção de dados”, pois diversas melhoras técnicas e operacionais tem sido implementadas pelas empresas, [com altos gastos](#), para proteger a privacidade dos usuários no ecossistema de mídia digital.

Evidente, é preciso reconhecer que há mações podres, que utilizam de [retargeting abusivo, pop-ups intrusivos e auto-plays irritantes](#) e que hoje estragam um pouco o valor da publicidade para os usuários. Todavia, é importante reconhecer [que essas são as ovelhas negras de uma indústria que já vem há muitos anos condenando essas práticas.](#)

No geral, o que temos visto é que há esforço grande da indústria em se adequar às

legislações de proteção de dados, e uma compreensão geral de que este momento é, na verdade, uma oportunidade para ganhar a confiança dos usuários, incentivar boas práticas e, ao final expurgar as práticas abusivas de alguns poucos *players*. **A publicidade direcionada, quando feita de forma responsável, gera uma melhor experiência para o usuário, um ganho efetivo para todo ecossistema de mídia e incentiva a criatividade e inovação na indústria.**

Alguns números mostram isso. Em pesquisa da *Data and Marketing Association* mostra que 71% dos profissionais de marketing do Reino Unido acreditam que a GDPR é uma [oportunidade para aumentar a criatividade de campanhas publicitárias](#). A mesma associação reportou que, após um ano da GDPR, houve um [aumento qualitativo nas métricas de e-mail marketing](#), com avanços significativos das taxas de abertura (74%) e cliques (75%) no último ano. Evidente, tudo isso não significa que se adequar às legislações de proteção de dados seja simples. [O custo e o tempo para adequação correta ainda são enormes.](#)

Nos próximos tópicos, vamos explorar alguns dos principais desafios para que anunciantes, agências, veículos e *adtechs* possam se adequar à LGPD, que entrará em vigor em agosto de 2020.

O QUE É BASE LEGAL PARA TRATAMENTO DE DADOS?

De maneira bem objetiva, toda entrega de anúncio publicitário que utilize dados pessoais precisa ter uma base legal, isto é, uma autorização prevista na LGPD para que o tratamento daqueles dados seja realizado. A LGPD enumera dez diferentes possibilidades de bases legais, mas duas delas são as mais importantes para o setor de publicidade: o **consentimento** e o **legítimo interesse**.

Obtendo o Consentimento

O **consentimento** significa uma *manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*. As palavras são importantes na LGPD, então vale atentar que o consentimento genérico, sem uma finalidade específica, não é considerado válido pela nossa lei. Além disso, outros pontos dessa frase merecem atenção:

(i) **manifestação livre:** o usuário deve concordar afirmativamente – no jargão

da indústria, é um regime de *opt-in*, e não *opt-out*;

(ii) **manifestação informada:** deve haver meios para que o usuário compreenda de que forma serão tratados seus dados e para quais finalidades;

(iii) **manifestação inequívoca:** ainda que a manifestação não precise ser expressa (como anteriormente – e equivocadamente – exigido pelo Marco Civil da Internet), deve haver meios para comprovar que não há dúvidas da escolha do usuário a respeito do tratamento de dados;

Logo, obter e documentar o consentimento pode ser desafiador no contexto da mídia programática, mas há algumas alternativas possíveis:

(i) Se você é um site, aplicativo ou rede social e requer que o usuário realize um cadastro antes de usar o seu serviço, você pode obter o consentimento por

meio de um *opt-in* em uma **política de privacidade**, que deve ter disposições razoáveis, claras e bem escritas sobre como e para que finalidades específicas você irá utilizar os dados do usuário, incluindo como o usuário pode exercer seus direitos. [O consentimento, nesse caso, pode ser documentado de forma granular](#), o que garantiria ainda mais transparência para o usuário;

- (ii) Agora, se você é um portal e, em geral, não exige que os usuários realizem um cadastro para usar seu site, você pode obter o consentimento por meio de um **aviso de cookies** (cookies são considerados dados pessoais tanto pela LGPD quanto pela GDPR, assim como qualquer outra tecnologia que atribua um identificador único, mesmo que aleatório, a um usuário). Sim, [esses avisos costumam ser pouco atraentes para o usuário](#) e, com poucas exceções, não podem ser mecanismos meramente de

opt-out, mas há referências interessantes no mercado de avisos consistentes com a legislação e que criam uma [boa experiência de usuário](#), incluindo o uso de plataformas de gestão de consentimento (*consent management platforms* – *CMPs*), sobre as quais vamos falar mais pra frente. O [próprio IAB disponibiliza gratuitamente protocolos](#) para implementação de um aviso de cookies com ferramentas que permitem a adequação a leis de proteção de dados – padrão semelhante ao que tem sido adotado pela própria [autoridade britânica de proteção de dados](#).

Não se deve começar a coletar dados pessoais antes do consentimento do usuário, e não se deve coletar dados além daqueles para os quais foi dado o consentimento. A tabela abaixo resume alguns dos principais cuidados que o setor de mídia deve ter ao obter o consentimento dos usuários:

OBTENDO O CONSENTIMENTO	<p>A política de privacidade e os avisos de cookies devem ser explícitos, claros e detalhando as finalidades específicas de seus usos</p> <hr/> <p>O modelo sempre deve ser opt-in, ou seja, o usuário deve concordar afirmativamente com aquela política</p>
DANDO TRANSPARÊNCIA AO USUÁRIO	<p>As finalidades devem ser o mais específicas possíveis, deixando claro os limites de uso e os direitos do usuário</p> <hr/> <p>Os tipos de dados utilizados devem estar sempre bem descritos, e restritos ao estritamente necessário para as finalidades pretendidas</p>
RESPEITANDO OS DIREITOS DO TITULAR	<p>Os usuários devem ter fácil acesso e controle sob o uso de seus dados, respeitando seus direitos a acesso, correção, portabilidade, exclusão e revogação do consentimento</p>

Além dos cuidados acima, é importante destacar que a experiência europeia, embora mais rígida que o modelo brasileiro, pode também trazer algumas reflexões práticas importantes para *publishers*, como por exemplo:

- (i) o consentimento implícito – aquele aviso de *cookies* em que o usuário “ao navegar pelo site/aplicativo, aceita automaticamente” – dificilmente será considerado uma boa prática adequada, salvo para **cookies essenciais** – aquelas *tags* que são estritamente necessárias para o funcionamento da aplicação, como por exemplo identificadores que otimizam performance de vídeos ou que previnem fraudes online;
- (ii) mesmo no caso de cookies essenciais, é importante que o aviso de cookies descreva claramente para o usuário que esses identificadores serão utilizados ao utilizar o site ou aplicativo, de forma a permitir o direito de escolha do usuário em não acessar determinada aplicação;
- (iii) embora cookies de publicidade sejam essenciais para financiar as atividades de certos sites e aplicativos e, logo permitir o acesso gratuito pelos usuários, várias [autoridades europeias já se posicionaram](#) no sentido de que identificadores de marketing não podem ser considerados cookies essenciais. Todavia, nada impede que os [publishers neguem acesso a](#)

[usuários que utilizem-se de *adblockers* ou que não aceitem cookies de publicidade](#), abordagem que tem sido adotada por grandes veículos como o [Washington Post](#);

O que é o legítimo interesse?

Obter o consentimento por meio de um cadastro prévio é, sem dúvidas, mais simples do que conseguir a atenção do usuário por meio de um aviso de cookies. Isso certamente dá uma vantagem competitiva a determinados competidores, em especial quando o usuário *precisa* passar pelo cadastro para utilizar determinado serviço que já é bem estabelecido e com boa reputação. Para portais e, em especial, novos competidores, obter um consentimento na forma acima pode ser mais desafiador, ainda mais porque o ecossistema de mídia digital é tão amplo e diverso que é praticamente impossível obter o consentimento para toda e qualquer empresa que faça parte da cadeia de valor.

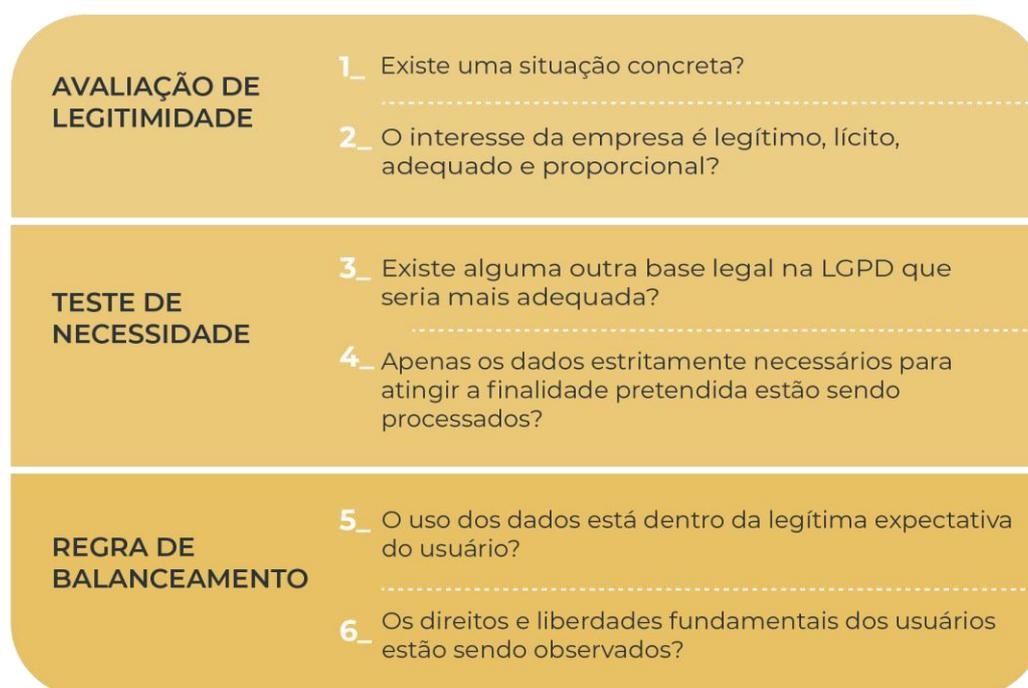
Se a indústria dependesse somente do consentimento, teríamos um cenário provavelmente pouco competitivo, de maior concentração entre os grandes atores do mercado e com baixa atratividade para o usuário. Todavia, há a base legal do **legítimo interesse**. Importante ressaltar que as bases legais não tem preponderância sobre a outra. Ou seja, o consentimento não vale mais do que

o legítimo interesse ou qualquer das outras oito bases. Ao fundamentar o tratamento dos dados com base no legítimo interesse, não é necessário obter o consentimento do usuário. Entretanto, é sempre necessário identificar a base legal mais adequada ao contexto do tratamento.

O legítimo interesse somente poderá fundamentar o tratamento de dados para finalidades legítimas, consideradas a partir de situações concretas, respeitadas as legítimas expectativas do usuário e os direitos previstos na LGPD. A lei brasileira é muito clara ao prever que o legítimo interesse pode, inclusive, legitimar e autorizar o tratamento de dados pessoais com os fins de apoio e promoção das atividades de uma empresa e, logo, a realização de publicidade – de forma mais

explícita que a GDPR, inclusive. Mas, naturalmente, a LGPD traz também todo um cuidado para que esse tratamento não seja feito de forma abusiva ou sem qualquer explicação ao usuário.

A base legal do legítimo interesse oferece a anunciantes uma maneira válida e legítima de garantir o tratamento de dados pessoais para fins de publicidade, em especial nas situações em que o consentimento é pouco viável. Ainda, essa base legal, após um teste de proporcionalidade, permite o uso dos dados para propósitos diferentes para os quais os dados foram originalmente coletados ou criados, enquanto o consentimento sempre vai exigir que as finalidades sejam previamente apresentadas e acordadas com o usuário.



Para o leitor atento, o teste acima traz uma inferência importante: o legítimo interesse da empresa deve ser balanceado com as legítimas expectativas do usuário no uso dos seus dados e justificá-lo pode ser mais simples quando o controlador dos dados já possui uma relação pré-estabelecida com o usuário, e mais complexo quando não há essa relação. Na Europa, reguladores de proteção de dados tem usado as expressões [marketing direto e marketing indireto](#) para diferenciar essas situações (ainda que, no mundo da publicidade, esses conceitos sejam aplicados de maneira bem diferente).

Isso ocorre, em especial, quando vamos analisar a legítima expectativa do usuário. Se já existe uma relação pré-estabelecida (marketing direto), há uma série de situações concretas em que parece ser razoável defender a base legal do legítimo interesse na LGPD por esta situação favorecer que haveria legítimas expectativas do usuário que seus dados poderiam ser utilizados para fins de marketing, como por exemplo:

- (i) um usuário já é consumidor de determinado site de e-commerce, e este deseja enviar, por meio de e-mail marketing, ofertas de produtos semelhantes ao histórico de compra do usuário;
- (ii) um usuário é assinante de um canal de vídeo online, costuma assistir os vídeos do canal com frequência, e o detentor do canal deseja impactar este usuário com

publicidade própria em uma rede social, comunicando que um novo vídeo já está disponível no canal;

- (iii) determinado usuário realizou, nas duas últimas semanas, diversas pesquisas de preço em um mesmo site de passagens aéreas; o site, identificando que o preço da passagem desejada pelo usuário caiu consideravelmente, resolve impactar o usuário com publicidade sobre essa passagem, por meio de uma rede de anúncios.

Isso não significa dizer que toda e qualquer prática de marketing indireto seria considerada inválida dentro da LGPD – até porque o teste de legítimo interesse acima descrito não exige esse relacionamento prévio. Muito pelo contrário. Há diversas situações em que seria razoável vislumbrar, no contexto do tratamento dos dados, que dados pessoais poderiam ser tratados para finalidades de marketing indireto, especialmente nos casos em que o controlador dos dados não possui interface direta com o cliente – algo que ocorre frequentemente em situações de prospecção comercial e, claro, na mídia programática.

Mais especificamente sobre esse campo, parece-nos haver fortes argumentos para sustentar o legítimo interesse como uma base legal válida para fins de entrega de mídia direcionada no âmbito da LGPD, ainda que não haja um relacionamento prévio:

- (i) **Legitimidade.** Anunciantes, agências, *adtechs* e veículos possuem um claro

interesse no uso de dados pessoais como parte dos *bid requests*, já que, caso não houvesse esse uso, o retorno sobre investimento seria certamente menor. E tal prática de marketing não é vedada pela legislação, sendo, portanto, lícita;

- (ii) **Necessidade.** O consentimento, como vimos acima, nem sempre será possível obter; entretanto, sem dados pessoais, as empresas não seriam capazes de entender as preferências dos usuários, e isso resultaria em um ciclo vicioso em que os anúncios seriam menos relevantes para os usuários, gerando menos cliques e conversões, o que levaria a menores receitas com publicidade e, potencialmente, menos conteúdo gratuito à disposição dos usuários; portanto, é necessário tratar tais dados pessoais para uma efetiva entrega de conteúdo direcionado;
- (iii) **Balanceamento.** Há uma razoável expectativa dos usuário de que portais e aplicativos gratuitos são sustentados pela publicidade (na Inglaterra, [somente 13% dos usuários são contra a publicidade online como contrapartida ao acesso gratuito a sites](#); nos EUA, [85% dos usuários preferem acessar sites gratuitamente, suportados por publicidade, do que sites pagos](#)). Além disso, como veremos adiante, a indústria já desenvolveu diversas ferramentas para garantir a observância dos direitos dos usuários.

Evidente, o quadro acima não justifica a inclusão de *todo e qualquer* dado pessoal em um *bid request*, já que a quantidade e os tipos de dados utilizados devem ser sempre balanceados com os direitos e liberdades dos titulares, devendo ser coletados e tratados apenas os dados estritamente necessários para atingir as finalidades almejadas pelo empresa (princípio da necessidade), além de ser simplista afirmar que toda e qualquer situação concreta seria *certamente* válida dentro do regime do legítimo interesse. Da mesma forma, é um desafio de anunciantes e agências criarem anúncios relevantes, criativos e que revertam a [impressão negativa que compras indiscriminadas de base de dados e algumas tecnologias de retargeting desqualificado e intrusivo criaram junto a usuários](#), e pensarem em formas claras e suficientes para descrever para seus usuários, de forma transparente, como funciona a cadeia de valor do mercado de mídia digital.

É exatamente por isso que o legítimo interesse é desafiador, pois oferece uma oportunidade de autorreflexão em toda cadeia da indústria, um momento para deixar definitivamente de lado o hype do *Big Data* e focar no *Good Data* para entender melhor quais dados que estão sendo capturados e que realmente agregam valor para os usuários, assim como uma chance para repensar conceitos de transparência e controle, como veremos adiante

GARANTINDO A TRANSPARÊNCIA E O CONTROLE DO USUÁRIO

Com o objetivo de balancear os direitos dos titulares de dados com os interesses legítimos dos controladores, as empresas precisam endereçar melhor a questão da transparência, isto é, o que estão fazendo com os dados pessoais e o controle que os titulares possuem sobre essas decisões.

Essa é uma tendência que começou bem antes da GDPR, com a *Digital Advertising Alliance* (DAA) que, em 2010, lançou o [AdChoices](#), uma ferramenta acoplada a anúncios que permite ao usuário entender como o anúncio foi entregue a ele e, caso prefira, possa bloquear a entrega de anúncios semelhantes. Empresas como Google, Microsoft, Facebook e Verizon Media aderiram aos princípios regulatórios da DAA e utilizam ferramentas semelhantes ao Adchoices desde então. Outra organização é a [Trustworthy Accountability Group](#), que se esforça para promover recomendações de antifraude, transparência e *brand safety* na indústria, práticas que podem apresentar soluções e métodos que provavelmente colaborariam para um embasamento legal do tratamento no legítimo interesse das empresas e um

aumento das legítimas expectativas dos usuários. Finalmente, a *Direct Marketing Association* recentemente se uniu a *Association of National Advertisers* nos EUA para também atualizar seus [guias de melhores práticas para o setor](#).

Após a GDPR, diversas plataformas tem aumentado suas ferramentas de transparência e controle dos dados pessoais, incluindo [Facebook](#), [Google](#) e [Verizon Media](#). Muitas dessas ferramentas utilizam-se de dois conceitos desenvolvidos recentemente, que são os *privacy dashboards* e as *consent management platforms*.

Os *Privacy Dashboards* são [ferramentas oferecidas por controladores e operadores de dados pessoais para garantir o cumprimento de direitos previstos em regulações como GDPR e LGPD](#). Esses direitos incluem a confirmação da existência de tratamento, o acesso, correção, exclusão de dados, portabilidade e revogação do consentimento, entre outros. Diversos portais, software e aplicativos já oferecem seus próprios painéis de controle para seus usuários e há,

atualmente, empresas que também comercializam esses softwares para terceiros, oferecendo aos usuários uma interface amigável para o acesso e controle desses dados, como por exemplo:

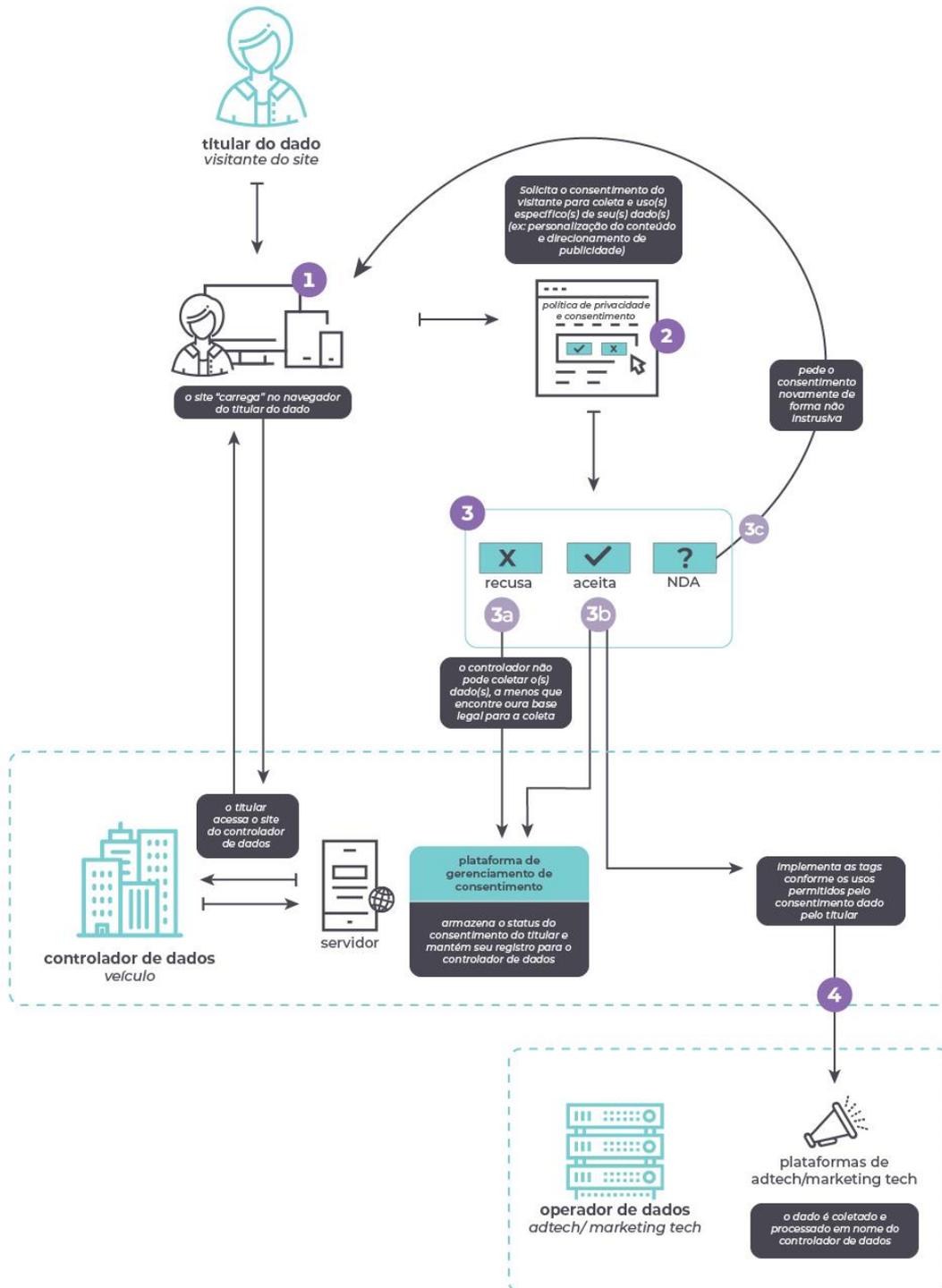
- (i) **acesso e explicação.** Os *privacy dashboards* permitem ao usuário acessar seus dados e entender como esses estão sendo utilizados, podendo inclusive entrar em contato direto com o controlador para solicitar informações;
- (ii) **retificação, oposição e cancelamento.** Essas ferramentas também permitem que o usuário controle a sua privacidade, altere dados e até mesmo cancele todo e qualquer tratamento realizado por aquele controlador; e
- (iii) **portabilidade.** Por fim, algumas dessas plataformas já estão se adaptando e permitindo o [download de seus dados](#) para o exercício do direito de portabilidade previsto na GDPR e também na LGPD.

Já as *Consent Management Platforms* (CMPs) são plataformas que podem ou não incluir ferramentas de *dashboards*, mas que possuem como principal diferencial configurar [cookie notices](#) em sites e aplicativos. Isso permite a obtenção do consentimento dos usuários em conformidade com as regulações aplicáveis –o IAB, por exemplo, tem disponibilizado gratuitamente [artigos e protocolos técnicos para que empresas possam desenvolver suas próprias CMPs](#).

O gráfico na página seguinte explica um pouco mais do fluxo típico dessas plataformas.

Finalmente o uso de **políticas de privacidade** claras, inteligentes e compreensíveis para a maioria da população é um outro desafio. Há abordagens interessantes, como aplicar [os conceitos da Creative Commons para privacidade](#), a aplicação de conceitos de [visual law, geradores automáticos de políticas que auxiliam startups](#) sem recursos suficientes e exemplos de políticas que misturam gráficos, imagens e textos de fácil compreensão para [auxiliar o entendimento do usuário](#). Aqui, mais uma oportunidade para não só a indústria da publicidade, mas também o setor de advocacia repensar como oferecer a seus clientes soluções fora do padrão *juridiquês* que impera nesse mercado.

Gráfico 2. Exemplo de fluxo de Consent Management Platforms



MITIGANDO RISCOS DE TRATAMENTO DE DADOS INVÁLIDOS

Pensando na complexa cadeia de atores envolvendo a mídia programática, por mais que uma empresa faça sua lição de casa e esteja com suas práticas adequadas dentro do cenário da LGPD, é sempre um desafio garantir que todos seus parceiros comerciais nesse ecossistema também estarão cumprindo as regulações de privacidade e proteção de dados.

Nesse sentido, um dos aspectos mais importantes da legislação brasileira é que, em caso de violação, a LGPD estabelece que controladores e operadores de dados pessoais podem ser *solidariamente* responsáveis. Trata-se de um regime semelhante ao que ocorre no Código de Defesa do Consumidor, em que qualquer agente da cadeia de tratamento pode vir a ser responsabilizado perante os titulares, ainda que não tenham sido diretamente responsáveis pelo dano.

No contexto de mídia programática, este é um assunto gravíssimo. Os dados passam por dezenas de empresas diferentes na cadeia, muitas delas que se quer possuem interface

com o usuário. Evidente, quem sofre mais exposição é o anunciante e os veículos, e é preciso desenvolver mecanismos de boas práticas para reduzir riscos de tratamentos não-autorizados. Sobre este ponto também é importante permitir que haja a responsabilização correta daqueles agentes que *realmente* causaram os danos aos usuários.

Um primeiro caminho que *mitiga* esses riscos é a elaboração de **acordos de tratamento de dados** (também conhecidos em inglês pela expressão *data processing agreements*). Esses acordos, que podem ser contratos autônomos ou mesmo anexos a outros contratos comerciais, estabelecem a relação entre controladores e operadores de dados pessoais. Assim, os *data processing agreements* limitam responsabilidades, estabelecem padrões de conduta e, em especial, estabelecem penalidades em caso de descumprimento das obrigações, permitindo o direito de regresso em caso de responsabilização solidária por terceiros.

Um bom contrato desse tipo deveria conter cláusulas como:

- (i) a obrigação do operador de somente tratar os dados em conformidade com as instruções recebidas pelo controlador;
- (ii) a obrigação de ambas as partes em manter os dados em sigilo e utilizando-se de padrões adequados de segurança da informação;
- (iii) a obrigação do operador em colaborar, na medida do possível, com o controlador no cumprimento de suas obrigações de proteção de dados;
- (iv) a obrigação do operador de devolver e/ou excluir os dados ao término do contrato.

Outras disposições importantes incluem cláusulas que garantem o **direito de auditoria** em parceiros comerciais. Essas auditorias podem focar tanto em aspectos

legais quanto técnicos, e possuem como objetivo verificar se os parceiros estão em conformidade com a legislação aplicável e com as boas práticas de mercado relacionadas com o tratamento de dados pessoais. A constatação de alguma falha no tratamento pode levar a penalidades e até a rescisão da relação comercial com esse parceiro.

Uma boa prática durante a negociação dos acordos é requisitar ao parceiro que apresente evidências de que está em conformidade com LGPD, ou está realizando seus melhores esforços para tanto, mas garante que os dados serão tratados em nível de segurança e proteção equivalente ao estabelecido pela legislação. Isso pode ser feito por meio de **documentos executivos** que resumem o trabalho previamente desenvolvido de análises de impacto de proteção de dados, metodologia comumente conhecida como **Data Protection Impact Assessment** ("DPIA"). Apesar do DPIA não ser obrigatório na LGPD, ele pode ser requisitado pelos reguladores, e já vem sendo requisitado pelo mercado.

CONCLUSÃO: UMA MENSAGEM PARA REGULADORES

Os números do mercado brasileiro de publicidade online são impressionantes. Em 2018, [mais de 16 bilhões de reais foram investidos em mídias digitais](#), o que já representa um terço do investimento em publicidade no país, e as previsões de crescimento para o mercado são de até 30% em 2019 – um número ainda mais expressivo se compararmos com a [previsão de crescimento do PIB](#).

Logo, o impacto de interpretações equivocadas da LGPD pode ter um efeito negativo muito maior para o setor de publicidade digital do que se observou na União Europeia, onde nasceu a principal inspiração da lei brasileira. Essa influência é evidente, a ponto de a lei brasileira ser chamada muitas vezes de uma versão *tropicalizada* da GDPR. Todavia, essa visão pode ser perigosa, não só pelas [diferenças existentes entre as legislações](#) (em que se vê claramente uma flexibilização maior da lei brasileira), mas também pelos problemas que o [transplante institucional](#) de outras regulações sem a devida adaptação de questões culturais pode ter no desenvolvimento social e econômico. Além

disso, após um ano de vigência da GDPR, já há críticas suficientes para argumentar que a GDPR criou [efeitos concorrenciais negativos, decisões equivocadas das principais autoridades nacionais](#) e riscos para o desenvolvimento de startups e novas tecnologias em campos de altíssima complexidade, como [inteligência artificial](#) – fora o fato de que nem [os próprios reguladores da GDPR estão se adequando corretamente à regulação](#), tamanha a distância entre o texto legal e a realidade do mercado de tecnologia.

Assim, em vez de importarmos indiscriminadamente a construção jurisprudencial e acadêmica europeia, **é o momento de empresas, academia, sociedade civil e, principalmente, reguladores desenvolverem suas próprias teses, baseadas na cultura e momento socioeconômico brasileiro**, e observando nas seguintes premissas:

- (i) é preciso entender a cadeia de valor da mídia interativa. É, sim, complexa e cheia de atores, mas isso não significa

que não agregue muito valor para os usuários e para a sociedade, gerando empregos, maior arrecadação de impostos e sendo um dos setores que mais cresce numa economia estagnada;

(ii) a mídia interativa tem um papel fundamental no caráter aberto e participativo da rede. Sem a publicidade online, a internet poderia ser muito mais restrita, fatiada e com custo muito mais alto para acesso ao conhecimento. Em um país em que os níveis de educação ainda são baixos e o custo de acesso à internet é alto em relação à renda, financiar portais e aplicativos por meio de publicidade ainda é um dos principais caminhos para redução de desigualdades no acesso à rede;

(iii) as associações e empresas do setor tem desenvolvido sólidos trabalhos de boas práticas e criação de padrões técnicos e operacionais de *privacy by design* e outras metodologias voltadas para a

proteção dos dados pessoais dos usuários; e

(iv) a publicidade online desempenha funções importantes para o desenvolvimento. No campo econômico, estimula a demanda, aumenta a concorrência, reduz custos de distribuição e introduz novos produtos e serviços no mercado com rapidez. No campo social, contribui para o desenvolvimento do país, informando sobre produtos e serviços de diferentes regiões de forma escalável e rompendo barreiras regionais e de renda.

Os próximos meses antes da vigência definitiva da LGPD serão desafiadores e marcantes na constituição do modelo regulatório de proteção de dados brasileiro. Nesta fase embrionária, é preciso responsabilidade de governos, empresas e sociedade civil em balancear todos esses aspectos, mas sempre com o objetivo comum de contribuir para o desenvolvimento econômico e social do país. Sem dúvidas, um grande desafio.
