CARTILHA DE PROTEÇÃO DE DADOS PESSOAIS

abooh
ASSOCIAÇÃO BRASILEIRA DE OUT OF HOME

SUMÁRIO

Sobre a ABOOH

ABOOH é a Associação Brasileira de *Out Of Home* (OOH), ou seja, a entidade que conecta diversos agentes que trabalham com mídias publicitárias externas no país, com o intuito de representar o setor, favorecer a troca de experiências e fomentar a adoção de boas práticas nesse mercado que cresce a cada ano, nacional e internacionalmente.

I. Introdução

Concretizando os objetivos da ABOOH de fomentar boas práticas no setor de mídias publicitárias externas, o Comitê de Privacidade da associação, desenvolveu a presente Cartilha de Proteção de Dados Pessoais, para difundir e esclarecer aspectos gerais da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais ("LGPD"), relacionando-os a atividades do setor de OOH.

II. Proteção de dados pessoais

1. O que é LGPD?

A Lei 13.709/2018, popularmente conhecida como “Lei Geral de Proteção de Dados” ou simplesmente “LGPD”, é a lei brasileira que regula o tratamento de dados pessoais. Desde a sua promulgação, toda atividade empresarial, inclusive aquela que lida com o digital, passou a ter que se adequar aos requisitos legais de proteção de dados pessoais, sempre de modo a garantir a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural, chamada pela Lei de titular de dados.

2. Mas, afinal, o que são dados pessoais?

A LGPD define os dados pessoais como todas as informações relacionadas a uma pessoa física identificada ou identificável. Dentre os dados pessoais, existe uma categoria especial à qual a Lei atribui maior proteção e exigências quanto ao seu tratamento. Essa categoria de dados pessoais a Lei denominou-se “dados pessoais sensíveis” - isto é, dados pessoais que dizem respeito à privacidade ou intimidade do titular de dados e têm maior risco de gerar discriminação.

Uma situação que demanda maior atenção, se refere ao tratamento de dados pessoais (ou dados pessoais sensíveis) de menores, sendo estes os dados de crianças (menores de 12 anos incompletos) e adolescentes (maiores de 12 e menores de 18 anos). Além do respeito à LGPD e às bases legais, o tratamento de dados de menores sempre deverá ser realizado em seu melhor interesse.

O quadro abaixo mostra as diferenças entre dados pessoais e dados pessoais sensíveis:

	DADOS PESSOAIS	**DADOS PESSOAIS SENSÍVEIS**
CONCEITO	Quaisquer informações sobre pessoa física identificada ou identificável.	Dados pessoais que podem gerar discriminação e/ou sejam invasivos à privacidade do titular.
EXEMPLOS	Nome completo, RG, CPF, endereço, telefone, celular, e-mail, endereço IP, geolocalização, etc.	Dados sobre origem racial ou étnica, religião, filiação a sindicato ou organização religiosa, filosófica ou política, dados de saúde, vida sexual, dados genéticos e

		biométricos.
PONTOS RELEVANTES	A jurisprudência formada, até então, é de que o dano moral por vazamento de dados pessoais exige prova do dano para concessão de indenização.	A jurisprudência formada, até então, é de que o vazamento de dados pessoais sensíveis gera um dano in re ipsa (dano presumido, que não requer prova).

3. Quando a LGPD é aplicada?

A LGPD é uma lei nacional, aplicável a qualquer pessoa natural ou pessoa jurídica, de direito público ou privado, que realize **operações de tratamento de dados pessoais.**[1]

Apesar de seu amplo escopo, é importante observar que **a LGPD não se aplica a dados anonimizados**, que consistem em dados de titular que, por si só, não possibilitam a identificação do titular pelo controlador através do uso de meios que se encontrem razoavelmente ao alcance deste.[2] Por outro lado, a **LGPD se aplica a dados pseudonimizados**, entendidos como dados que foram desassociados de seu titular pelo controlador, mas que podem ser novamente a ele associados pela conjunção de elementos que foram previamente afastados e ainda se encontram ao alcance do controlador.[3]

4. E a LGPD vale apenas para dados de brasileiros?

Não. A LGPD é aplicável a quatro situações em que há operações de tratamento de dados pessoais:

Operação de tratamento realizada **no território brasileiro.**	**Oferta e/ou fornecimento de bens e/ou serviços** a pessoas físicas localizadas no Brasil.	Tratamento de dados de **indivíduos localizados no Brasil.**	Dados coletados **no território nacional.**

[1] Ressalvadas as operações de tratamento realizadas para fins exclusivamente jornalísticos e artísticos, ou acadêmicos quando a LGPD não será aplicada.

[2] De acordo com a LGPD, dado anonimizado é o "dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento." (artigo 5º II).

[3] V. artigo 13 §4º da LGPD.

5. O que são operações de tratamento de dados pessoais?

São todas as atividades realizadas com dados pessoais, incluindo a coleta, produção, recepção, classificação, uso, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, disseminação ou extração de dados.

É importante ter o mesmo cuidado com os dados em cada uma das operações de tratamento, pois a LGPD determina que as organizações que intervenham em qualquer uma das fases são obrigadas a garantir **a segurança da informação destes, mesmo após o término do tratamento (eliminação ou descarte do dado)**.

6. Quem são os principais atores da LGPD?

A LGPD tem 4 atores principais, a saber, **o titular dos dados, o controlador, o operador e o encarregado de dados.**

Nesse cenário, **o titular** dos dados é uma pessoa física a quem os dados pessoais se referem. O titular, então, poderá ser um cliente, um empregado, um candidato ao emprego, um consumidor, ou qualquer outra pessoa que, direta ou indiretamente, poderá ser identificada a partir dos dados pessoais que são tratados.

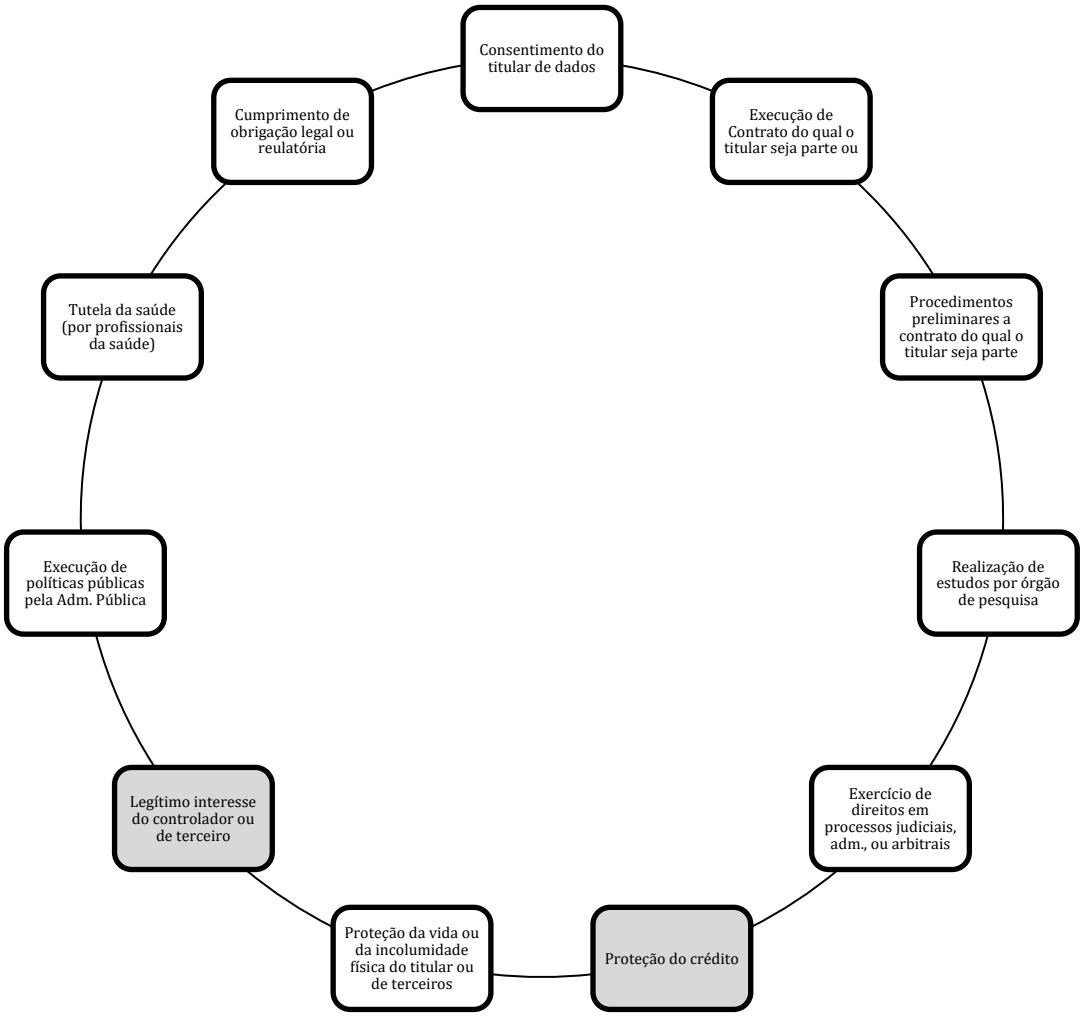
Por sua vez, **o controlador** é o responsável pelo tratamento, uma pessoa jurídica ou física que decide quais dados pessoais devem ser recolhidos e toma as decisões relativas ao tratamento dos dados. Já **o operador** é uma pessoa física ou jurídica, que trata dados pessoais por ordem do controlador. Esses dois atores, conforme definição da LGPD, são os **agentes de tratamento**. É essencial que se entenda qual é o papel exercido no tratamento de dados, pois a LGPD distribui de forma distinta as obrigações e as responsabilidades dos agentes de tratamento.

Por último, a LGPD cria a função de **encarregado de dados**, pessoa física ou jurídica, designada pelo controlador e responsável pela comunicação deste com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD), órgão público federal criado pela LGPD para garantir a

proteção dos titulares de dados.

7. Quando pode haver tratamento de dados pessoais?

O tratamento de dados pessoais somente poderá ocorrer legalmente quando houver respaldo de uma das hipóteses permitidas pela LGPD, chamadas de **bases legais**[4]. Essas bases legais são equivalentes, não havendo, como regra, prevalência de uma sobre as outras.



As bases legais para o tratamento de dados pessoais sensíveis diferem das bases legais acima mencionadas, e alguns esclarecimentos adicionais são fundamentais:

As bases legais de legítimo interesse e proteção ao crédito **NÃO** podem ser usadas para dados

[4] V. artigo 7º da LGPD.

pessoais sensíveis;

A base legal do consentimento, para os dados pessoais sensíveis, possui mais exigências: ele deve ser **específico e destacado.**

- **Específico:** os titulares de dados devem ser informados de forma específica todas as finalidades para os quais seus dados são tratados;
- **Destacado:** o consentimento deve aparecer em evidência no documento, como por exemplo em letras maiores, negrito ou sublinhado.

Os dados pessoais sensíveis, portanto, podem ser tratados com fundamento nas seguintes bases legais[5]:

A. Quando o titular ou seu responsável legal **consentir**, de forma **específica** e **destacada**, para finalidades específicas;

B. Sem fornecimento de consentimento do titular, nas hipóteses em que for **indispensável** para:

   i. Cumprimento de **obrigação legal** ou **regulatória** pelo controlador;

   ii. Tratamento compartilhado de dados necessários à execução, pela administração pública, de **políticas públicas** previstas em leis ou regulamentos;

   iii. Realização de **estudos** por **órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

   iv. **Exercício regular de direitos**, inclusive em contrato e em processo judicial, administrativo e arbitral;

   v. **Proteção da vida** ou **da incolumidade física** do titular ou de terceiros;

[5] V. artigo 11º da LGPD.

vi. **Tutela da saúde**, exclusivamente, em procedimento realizado por profissionais da saúde, serviços de saúde ou autoridade sanitária; ou

vii. Garantir a **prevenção à fraude e à segurança do titular**, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

8. Como os dados pessoais devem ser utilizados?

A conformidade com a LGPD deve ser orientada, primordialmente, por seus princípios. Assim, os seguintes **princípios específicos devem ser observados** quando houver atividades de tratamento de dados pessoais:

i. **Finalidade:** o tratamento de dados pessoais deve ser realizado apenas para fins legítimos, específicos, explícitos e informados ao titular dos dados.
ii. **Adequação:** o contexto do tratamento deve ser compatível com os fins para os quais o titular dos dados é informado.
iii. **Necessidade:** é o requisito da coleta mínima de dados pessoais levando em consideração as finalidades de processamento.
iv. **Livre Acesso:** dá direito aos titulares de dados um formulário de acesso fácil e gratuito sobre o conteúdo completo dos seus dados pessoais, seus meios e período de tratamento.
v. **Qualidade dos dados:** concede aos titulares dos dados garantia de exatidão, clareza, relevância e atualização dos dados pessoais.
vi. **Transparência:** garante aos titulares dos dados o direito de compreender de forma clara, precisa e simples as atividades e os agentes de tratamento, respeitando os segredos comerciais e industriais.
vii. **Segurança:** exige o uso de medidas técnicas e administrativas para proteger os dados pessoais contra acesso não autorizado e destruição, perda, alteração, comunicação ou disseminação acidental ou ilegal.
viii. **Prevenção:** requer a adoção de medidas para evitar danos aos titulares dos dados devido ao tratamento de dados pessoais.
ix. **Não discriminação:** proíbe a realização de atividades de processamento para fins discriminatórios ilícitos ou abusivos; e
x. **Responsabilidade e prestação de contas:** requer evidências sobre medidas eficazes que

foram tomadas para demonstrar a conformidade com os regulamentos de proteção de dados pessoais do controlador e do operador.

9. O que é e quando realizar um relatório de impacto à proteção de dados pessoais?

O relatório de impacto à proteção de dados pessoais ("RIPD") é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Segundo a LGPD, o relatório deve conter, no mínimo:

1. Descrição dos dados pessoais coletados;
2. A metodologia utilizada para a coleta e para a garantia das informações;
3. A análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

10. Quais são os direitos dos titulares dos dados pessoais?

Os direitos dos titulares de dados previstos na LGPD são os seguintes:

a. **Acesso:** Os titulares dos dados têm garantido o acesso aos seus dados pessoais, no sentido de que podem pedir informações aos controladores sobre os dados tratados.

a) **Retificação de dados incompletos, inexatos ou desatualizados**: um dos principais direitos dos titulares de dados pessoais é o direito de corrigir ou retificar qualquer informação sobre eles.

b) **Anonimização, bloqueio ou eliminação dos dados**: os titulares dos dados podem exigir que os dados pessoais considerados desnecessários, excessivos ou ilegalmente processados sejam tornados anônimos, bloqueados ou excluídos.

c) **Portabilidade:** o titular dos dados pode: (i) receber, a seu pedido, dados pessoais que um Controlador possui sobre eles de forma estruturada (geralmente em um formato interoperável legível por máquina ou usado rotineiramente que pode ser lido automaticamente por computadores) para ser dado a outro fornecedor de serviço ou produto; e / ou (ii) alternativamente, e se tecnicamente possível, exigir uma transferência

direta de tais dados pessoais para outro fornecedor de serviços ou produtos.

d) **Eliminação dos dados pessoais tratados com base no consentimento**: o titular dos dados pode solicitar a eliminação dos dados pessoais tratados com o seu consentimento, exceto nos casos previstos no artigo 16.º da LGPD.

e) **Informação das entidades públicas e privadas**: dá aos titulares de dados o direito de saber sobre o compartilhamento de seus dados pessoais pelos controladores.

f) **Informações sobre o consentimento e as consequências da recusa de consentimento:** impõe aos controladores que usam o consentimento como base legal para o tratamento de dados pessoais para informar os titulares dos dados: (i) a possibilidade de não fornecer consentimento, quando viável, e (ii) as consequências de uma recusa, que na maioria dos casos significará a impossibilidade de usar um determinado produto ou serviço; e

g) **Revogação do consentimento:** os controladores devem informar a pessoa em causa que têm o direito de revogar o seu consentimento a qualquer momento e devem fornecer um meio simples de exercer esse direito.

III. O que o OOH tem com isso?

Na condição de um segmento de alto valor agregado e elevado grau de digitalização, o setor de mídias publicitárias externas, a exemplo de outros mercados de ponta, depende de dados para a obtenção precisa de suas métricas e o aperfeiçoamento de seus resultados – acima de tudo, o alcance de público.

O setor de OOH, focado em mídias publicitárias externas, não oferece a personalização da publicidade digital consumida em meios pessoais como celulares ou navegadores, o que afasta a importância da identificação individual dos integrantes do público e diminui significativamente a utilização de dados pessoais. Isso se dá porque a importância do OOH está em atingir grandes públicos de uma só vez, de forma que o que importa para o setor é a identificação de grupos numerosos, não de indivíduos.

Ainda assim, ao utilizar recursos de alta tecnologia ao ar livre e/ou em espaços acessíveis ao público, não há dúvidas de que o OOH pode se beneficiar de boas práticas no que diz respeito a seus fluxos de dados, fortalecendo a preservação dos valores protegidos pela LGPD.

Desta maneira, os quesitos a seguir buscam jogar luz sobre o funcionamento do setor do ponto de vista dos dados, oferecendo-lhe algumas das melhores práticas no que concerne ao respeito à legislação de proteção de dados pessoais.

1. Quais são os agentes do OOH?

O núcleo do OOH é o **veículo**, isto é, o proprietário ou responsável pela estrutura física da mídia publicitária externa, que pode ter diversas formas (como grandes outdoors, mobiliário urbano, painéis digitais ou totens em shopping centers). No veículo, são afixados ou exibidos materiais publicitários gráficos do **anunciante**, que pode contratar a mídia externa diretamente ou por meio de uma **agência de publicidade** (ou outro tipo de **intermediário de anúncios**).

Para mensurar seu potencial de público, o veículo pode contratar serviços de um **fornecedor de dados**, que oferece um conjunto de dados, obtidos de fontes diversas, analisados ou em estado bruto, que dão conta de movimentações de pessoas não identificadas nas imediações da mídia publicitária externa. Alternativamente, o veículo também pode realizar suas próprias mensurações ou mesmo prescindir de realizá-las, nos casos em que o público seja considerado notório (por exemplo, quando a localização do anúncio sabidamente atinja público tão numeroso que a mensuração, a critério do veículo, deixar de ser realizada).

Neste contexto, a ABOOH se limita a representar veículos e fornecedores de dados.

2. Como os veículos devem usar dados?

Quando realizam por si mesmos a mensuração do potencial de público de suas mídias publicitárias externas, os veículos podem optar por dados próprios ou de terceiros. Nesse caso, dados próprios são dados obtidos de meios próprios (por exemplo, oferta de internet wi-fi a transeuntes), enquanto que dados de terceiros são todos os dados que podem ser obtidos de outras fontes, como fornecedores de dados ou fontes estatísticas oficiais. Em ambas as hipóteses, **os veículos devem privilegiar o tratamento de dados que não possam implicar na identificação individual dos transeuntes**.

Para a obtenção de dados próprios, **o veículo pode disponibilizar sinal de wi-fi sempre que os dados recebidos dos celulares dos transeuntes não possibilitem, por si só ou em conjunto, a**

identificação pelo veículo (por exemplo, endereços MAC, códigos alfanuméricos de Device IDs, modelo de celular, etc). No caso do transeunte optar por efetivamente utilizar a rede oferecida, o veículo pode solicitar dados pessoais para realização de registro e/ou uso da internet, mas deve informar, em linguagem clara e simples, o titular a respeito dos dados, modos e finalidades do tratamento, obtendo seu **consentimento para tratamento desses dados pessoais**. O veículo deve oferecer **soluções de segurança à conexão wi-fi**, como o uso de senhas fortes na configuração de sua infraestrutura e padrões elevados de criptografia, em especial o WPA2. Adicionalmente, em cumprimento ao Marco Civil da Internet, o veículo, equiparado a provedor de conexão de internet, deve guardar por 1 ano os registros de conexão de seus usuários (data e hora, duração e endereço IP).

Ao obter dados de terceiros, os veículos devem utilizar apenas bases de dados, de fontes públicas ou privadas, que estejam devidamente anonimizados – isto é, mais uma vez, que impossibilitem, por si ou em conjunto, a identificação individual dos titulares por parte dos veículos. Ainda, na relação com fornecedores de dados, os veículos devem contratar com agentes que demonstrem boas práticas de proteção de dados, de acordo com os critérios da próxima questão.

Adicionalmente, sugere-se que os veículos realizem e incentivem a seus parceiros atividades de qualificação e conscientização sobre privacidade e proteção de dados com seus empregados e colaboradores, garantindo a constante atualização sobre a normativa relevante e o estabelecimento de uma cultura de preservação destes direitos fundamentais.

3. Como os fornecedores de dados devem usar dados?

Para possibilitar a aferição de potencial de público de mídias publicitárias externas, os fornecedores de dados reúnem dados de movimentação geográfica a partir de diversas fontes, públicas e privadas. Estes dados devem ser obtidos anonimizados, de forma que seja impossível a identificação individual dos titulares por parte dos fornecedores (por exemplo, consistindo apenas de coordenadas de GPS e códigos alfanuméricos de Device IDs e Mobile Advertising IDs).

Quando os dados forem obtidos como dados pessoais, os fornecedores de dados devem realizar o tratamento utilizando-se de bases legais da LGPD - por exemplo, solicitando

consentimento de usuário de determinada aplicação de celular para usar seus dados anonimizados para a realização de análises de potencial de público para mídias publicitárias externas – embora esta não seja a única base legal permitida. Em seguida, antes da transmissão dos dados aos veículos, os fornecedores devem realizar **procedimento de pseudonimização**, **tornando os dados anonimizados do ponto de vista dos veículos**.

Quando se tratar de dados obtidos por **vídeo**, utilizando-se de câmera instalada nas mídias publicitárias externas, os fornecedores de dados devem evitar a captura de imagens que possibilitem a identificação dos transeuntes. Para isso, **é preciso que restrinjam o acesso e a análise dos vídeos a máquinas (notadamente, programas de computador de varredura de imagem), limitando-se a identificar número de transeuntes e a classificar o público de acordo com grandes grupos não discriminatórios e que não impliquem em identificação individual** (por exemplo, sexo, idade e velocidade). Além disso, os vídeos devem ser automaticamente eliminados assim que forem analisados por máquinas, impedindo o seu uso para outros fins.

Além disso, a exemplo dos veículos, sugere-se que os fornecedores de dados realizem e incentivem a seus parceiros atividades de qualificação e conscientização sobre privacidade e proteção de dados com seus empregados e colaboradores, garantindo a constante atualização sobre a normativa relevante e o estabelecimento de uma cultura de preservação destes direitos fundamentais.

4. Como os anunciantes e agências de publicidade devem usar dados?

Ainda que anunciantes e agências de publicidade não sejam representados pela ABOOH e disponham de autonomia dentro das regras de seus próprios setores, a ABOOH sugere que, em contexto de anúncio em mídia publicitária externa, estes agentes realizem campanhas que levem em conta a centralidade de dados anonimizados e/ou de grupo que caracteriza o setor de OOH.

5. Qual a classificação dos agentes de OOH enquanto agentes de tratamento de dados?

Como núcleo do OOH, **o veículo, num primeiro momento de estabelecimento de potencial de público, ocupa a posição de controlador**, determinando os dados tratados, suas

finalidades e seu fluxo, **sendo o fornecedor um operador**. A depender de ajustes contratuais e circunstâncias práticas avaliados no caso a caso, **o fornecedor pode realizar atividades de controladoria**, pondo-se como um co-controlador ou até mesmo como o controlador do tratamento de dados.

No momento do anúncio, dado que a publicidade é um mercado criativo baseado na inovação, **o anunciante e/ou a agência de publicidade podem assumir papel de controladores** quando exigem a associação de interações com celulares ou outros arranjos a seus anúncios. Nesta hipótese, quanto a este tratamento, os veículos podem ser operadores (caso operem estrutura por onde passa o fluxo de dados) ou até mesmo não ter qualquer relação com os dados, sendo apenas um suporte físico para exibição de endereços eletrônicos inteiramente geridos pelos anunciantes.

Assim sendo, **a avaliação da posição dos agentes na cadeia de tratamento estabelecida pela LGPD deve ser realizada caso a caso**, levando-se em conta avenças contratuais e a especificidade de projetos especiais de clientes, circunstâncias de fato e o contexto do tratamento de dados, com especial atenção ao momento de sua realização.

6. Que informação relativa a uso de dados deve ser oferecida ao público?

Como dados anonimizados não são dados pessoais estão fora do âmbito de aplicação da LGPD, não havendo, assim, dever específico de informação ao público a respeito do uso de dados na maior parte dos processos do OOH. No entanto, nas situações residuais em que há uso de dados pessoais, o dever de informação se aplica.

Na oferta de conexão wi-fi a transeuntes por meio de cadastro, os usuários devem ser informados sobre os dados, fluxos e finalidades do tratamento, além de indicações sobre maneiras de se exercer direitos de titular, sempre de modo claro e simples. Uma boa maneira de concentrar a informação é oferecê-la em política de privacidade mostrada ao usuário antes da autenticação ou cadastro na rede ofertada.

Nas hipóteses em que fornecedores de dados trabalharem com dados pessoais, seus titulares devem ser informados, idealmente em política de privacidade, a respeito dos seguintes aspectos: dados, fluxos e finalidades do tratamento, além de indicações sobre maneiras de se exercer direitos de titular, sempre de modo claro e simples. Aqui é importante que o titular seja informado a respeito

do uso de identificadores, inclusive aqueles de geolocalização, e sobre o processo de anonimização a ser realizado antes da disponibilização do conjunto de dados aos veículos.

Além disso, mesmo nas situações em que houver apenas o tratamento de dados não pessoais, é aconselhável informar os transeuntes a respeito de procedimentos realizados, como forma de cumprir o dever geral de informação ao consumidor, ainda que por equiparação. Neste sentido, por exemplo, sugere-se a informação, na forma de aviso afixado junto aos locais de anúncios, sobre mecanismos de vídeo que venham a ser utilizados para a mensuração de público.

7. Que direitos de titulares de dados podem ser exercidos no OOH?

Quanto aos dados anonimizados, não há possibilidade dos titulares exercerem direitos criados pela LGPD, principalmente porque o controlador não pode identificar os titulares dos dados que usa.

Porém, os titulares podem, sempre que tecnicamente possível, exercer todos os direitos relativamente ao tratamento de seus dados pessoais nos casos residuais do OOH – notadamente, na oferta de conexão wi-fi a transeuntes e no preparo, por fornecedores de dados, de bases de dados de geocalização com pessoas identificadas ou identificáveis.

No caso da conexão wi-fi, o usuário pode solicitar acesso a seus dados, a revogação do consentimento, a retificação, a eliminação, o bloqueio e a anonimização dos dados pessoais. No caso de bases de dados não anonimizadas, o titular pode exercer os mesmos direitos, com a diferença de que o exercício destes não afetará o veículo se os dados anonimizados já se encontrarem transferidos pelo fornecedor de dados.

8. É permitido realizar cruzamento de dados?

De grande utilidade para o aperfeiçoamento de métricas, o cruzamento de dados pode ser realizado livremente nos casos de dados anonimizados, de que são exemplos estatísticas ou bases de dados compostas por dados que não possibilitem, por meios razoáveis, a identificação de titulares pelo veículo e/ou pelo fornecedor de dados, a depender de quem for agente de tratamento em cada situação.

Por outro lado, quando se tratar de dados pessoais, como no caso de bases de dados ainda não anonimizadas por fornecedores de dados, o cruzamento só pode se realizar com a devida informação ao usuário e apoiado em base legal da LGPD, como o consentimento.

9. É permitido realizar compartilhamento de dados?

O compartilhamento de dados com terceiros pode ser realizado livremente no casos de dados anonimizados, de que são exemplos estatísticas ou bases de dados compostas por dados que não possibilitem, por meios razoáveis, a identificação de titulares por todos os agentes envolvidos na operação (isto é, o controlador/operador e o terceiro).

Por outro lado, quando se tratar de dados pessoais, como no caso de bases de dados ainda não anonimizadas por fornecedores de dados, o compartilhamento com terceiros só pode se realizar com a devida informação ao usuário e **obtenção de consentimento específico**.

10. É permitido realizar perfilamento do público?

O perfilamento de transeuntes, sempre de acordo com grandes grupos não discriminatórios, é permitido desde que a pessoa não esteja identificada. Desta forma, é possível a classificação do público a partir de padrões observados em vídeo ou códigos alfanuméricos – por exemplo, pode-se inferir que o titular de um código alfanumérico utiliza a via pública em dado horário assim como se podem classificar pessoas em vídeo por idade, sexo e velocidade, contanto que esse perfilamento se realize em relação a uma pessoa que não esteja identificada.

11. É necessário realizar o registro de uso de dados?

Não há necessidade de registrar o tratamento de dados que não sejam pessoais, como os dados anonimizados. No entanto, nos casos residuais em que houver tratamento de dados pessoais, como na oferta de internet wi-fi a transeuntes através de registro na rede, deve ser realizado o registro do tratamento, conforme regulamentação da ANPD. Microempresas, empresas de pequeno porte e startups já podem utilizar modelo simplificado de registro de tratamento de dados pessoais disponibilizado pela Autoridade.

12. É necessário elaborar relatório de impacto à proteção de dados?

Na maioria das vezes, não há necessidade de elaborar relatório de impacto à proteção de dados, já que os dados usados pelo setor de OOH são quase sempre anonimizados e/ou de escala reduzida (como os pontos de acesso de internet wi-fi oferecidos pelos veículos, que podem atender um público restrito).

Ainda assim, considerando que a ANPD pode solicitar a realização de relatórios de impacto a qualquer tempo, é aconselhável que agentes que desenvolvam atividades que podem ser entendidas como de alto risco pela Autoridade preparem relatórios descrevendo seu fluxo de dados e destacando as salvaguardas e medidas de mitigação de risco. Por alto risco, entendam-se atividades com dados de elevado número de titulares, envolvendo dados sensíveis ou dados de crianças e adolescentes, baseadas exclusivamente em decisão automatizada, implicando em vigilância de áreas de acesso público ou apoiadas de meios inovadores.

Logo, no setor de OOH, é **aconselhável que fornecedores de dados que lidem com grandes bases de dados, mesmo quando anonimizadas, ou realizem análise de mídias publicitárias externas por meio de vídeo elaborem relatório de impacto à proteção de dados**, enxergando a tarefa como uma oportunidade de organizar as medidas técnicas postas em prática para garantir o anonimato dos dados, garantidos eventuais segredos comerciais.

Participantes do Comitê: LGPD no OOH

Esta Cartilha foi desenvolvida em 2023 pela ABOOH, através de seus associados participantes do Comitê **LGPD no OOH**, liderado por Conrado Kallas, com apoio dos participantes: Marco Munõz (AdsMovil OOH), Juliana Marques e Thais Gonçalves (Clear Channel), Livia Pires, Lucio Schneider e Rodrigo Cadena (Eletromidia), Caio Ferraro e Felipe Forjaz (Helloo), Danit Kelner e Marcos Gimenes (JCDecaux), Denis Gaumondie (Quividi), e Yuri Berezovoy (RZK Digital).