Brasil

Cross-Jurisdiction
Privacy Project

1. A LEI

1.1. Visão geral e principais atos, regulamentos e diretivas

- **A Lei Geral de Proteção de Dados Pessoais** ("Lei nº 13.709 / 2018" ou "LGPD") entrou em vigor em 18 de setembro de 2020, como resultado da sanção do Projeto de Conversão ("PLV") n.º 34/2020 do Presidente da República. No entanto, as sanções administrativas estabelecidas pela LGPD só serão aplicáveis pela Autoridade Nacional de Proteção de Dados do Brasil ("ANPD"), que é responsável pela supervisão e edição das regras sobre o tratamento de dados pessoais, em 1º de agosto de 2021 (Lei nº 14.010/2020).

- Não obstante, embora a ANPD só tenha sido instituída recentemente e as sanções só tenham passado a valer em 1 de agosto de 2021, outros órgãos como o Ministério Público Federal do Distrito Federal e Territórios (MPDFT), os órgãos de defesa do consumidor (PROCON), o Ministério Público Federal e a Secretaria do Consumidor (SENACON) já estão aplicando os princípios de proteção de dados e privacidade no Brasil.

O objetivo da legislação é impulsionar o desenvolvimento econômico e tecnológico do Brasil, proporcionando maior segurança jurídica às operações que envolvem o tratamento de dados pessoais, harmonizando outras leis setoriais no Brasil que também tratam dos direitos de privacidade e proteção de dados. Enquanto a LGPD foi fortemente inspirada no Regulamento Geral de Proteção de Dados (a "GDPR"), a legislação brasileira apresenta diversas peculiaridades e reflete questões específicas relacionadas à cultura e à realidade do país.

Nesse sentido, a LGPD difere da GDPR em relação a outros tópicos relacionados à privacidade, como as diferentes bases legais para tratamento de dados[1], prazo para resposta às solicitações dos titulares de dados, segurança da informação, marketing direto, consulta prévia, práticas de retenção, entre outros. Assim, fica claro que o cumprimento da GDPR não é suficiente para garantir o cumprimento da LGPD e vice-versa.

Não obstante, dada a importância do Brasil como economia digital, a entrada em vigor da LGPD impactou empresas que desenvolvem atividades de marketing direto on-line, assim como o marketing off-line.

1.2. Diretrizes

Não se aplica.

[1] A LGPD prevê a possibilidade de tratamento de dados pessoais para fins de proteção ao crédito, fundamento jurídico que não está previsto no GDPR: *Art. 7 O tratamento de dados pessoais deve ser realizado apenas nas seguintes circunstâncias: (...) X - para a proteção de crédito, inclusive conforme previsto na legislação específica*.

1.3. Jurisprudência

A LGPD só entrou recentemente em vigor, razão pela qual existem pouquíssimas decisões a envolvendo seus dispositivos. Não obstante, existem vários casos fundamentais referentes à privacidade e proteção de dados no Brasil.

Um caso recente é a decisão do Supremo Tribunal Federal ("STF") sobre o Referendo na Medida Cautelar ("PM") na Ação Direta de Inconstitucionalidade nº 6.389 do Distrito Federal[2], que suspendeu a MP nº 954. A decisão tratou sobre o compartilhamento de dados pessoais de clientes de operadoras de telefonia com o Instituto Brasileiro de Geografia e Estatística ("IBGE") para uso em estatísticas oficiais. Por 10 votos a 1, o plenário do STF manteve a liminar concedida anteriormente pela Ministra Rosa Weber, que obrigava as empresas de telecomunicações a conceder ao IBGE acesso aos nomes, telefones e endereços de seus consumidores pessoa física e jurídica. O IBGE pretendia identificar se os consumidores faziam "entrevistas domiciliares" para as vagas de emprego (isto é, entrevistas realizadas à distância, não presenciais), de forma a medir o desemprego no País. Considerados dados pessoais pela Ministra Weber, tais informações, se divulgadas sem autorização prévia, poderiam causar "danos irreparáveis à privacidade e, portanto, aos direitos constitucionais de mais de cem milhões de usuários".

Outra decisão proferida pelo Tribunal de Justiça do Estado do Rio Grande do Norte determinou a reintegração de um motorista de uma plataforma de caronas que foi indevidamente excluído do aplicativo por decisão automatizada do software. Mesmo sendo o motorista bem avaliado pelos clientes, o software o removeu da plataforma sem lhe dar a oportunidade de se defender ou mesmo exercer seu direito de ter a decisão revista. Nesse sentido, o caso reflete as regras estabelecidas pela Lei nº 13.853/2019, que alterou a LGPD, no que diz respeito à possibilidade de revisão de decisão automatizada.

Além disso, outro caso tratou da condenação de uma incorporadora imobiliária que compartilhou os dados pessoais de um dos seus clientes sem o seu consentimento prévio e com finalidade diferente da inicialmente informada - que era a aquisição de um imóvel. Com isso, o juiz entendeu que a empresa violou não só a LGPD, mas também a Constituição Federal e os dispositivos do Código de Defesa do Consumidor, razão pela qual a organização foi considerada responsável por indenizar a parte autora.

[2] Brasil. Superior Tribunal Federal. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.389 Distrito Federal. Rel. Min. Rosa Weber. Data de julgamento: 24 abr. 2020. Voto Conjunto ADIs 6.389, 6.390, 6.393, 6.388 e 6.387 pelo Min. Gilmar Mendes. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf

2. ESCOPO DE APLICAÇÃO

2.1. A quem as leis/regulamentos se aplicam?

A LGPD aplica-se a qualquer agente (pessoa física, jurídica ou órgão público) que realize atividades de "tratamento de dados pessoais", termo definido na Lei como "qualquer operação realizada com dados pessoais", desde o simples acesso aos dados de funcionários, fornecedores e até os consumidores ao armazenamento, transferência, classificação, eliminação ou qualquer outra utilização de dados pessoais (artigos 3º e 5º, X, LGPD). Assim, a LGPD aplica-se a todas as empresas estrangeiras que ofereçam serviços ou produtos ao Brasil ou realizem qualquer atividade de tratamento no território brasileiro, independentemente de tais empresas terem sede ou centros de tratamento de dados no Brasil.

Naturalmente, a LGPD aplica-se a todos os atores envolvidos na publicidade digital (*publishers*, anunciantes, DSPs, SSPs etc.) sempre que tratarem dados pessoais de pessoas localizadas na jurisdição brasileira. Além disso, se uma empresa não estiver localizada no Brasil, mas intencionalmente objetivar a coleta de dados de titulares de dados localizados no Brasil, a LGPD aplica-se às atividades de tratamento de dados dessa empresa.

Por outro lado, a LGPD não se aplica quando o tratamento de dados é realizado exclusivamente para fins jornalísticos, artísticos e acadêmicos; fins de segurança pública, defesa nacional ou segurança do estado; ou investigando e processando crimes. A LGPD também prevê exceções quando o tratamento de dados tem origem fora do território brasileiro e não está sujeito a nenhum tratamento posterior no Brasil, de forma que os dados estejam apenas em trânsito pelo Brasil.

2.2. Que tipos de tratamento são abrangidos/excetuados pela LGPD?

O Art. 5, X da LGPD define tratamento como qualquer tipo de operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A LGPD aplica-se a qualquer atividade de tratamento, independentemente do meio, do país em que a sede do controlador está localizada ou do país em que os dados estão localizados, desde que:

- A atividade de tratamento seja realizada em território brasileiro;
- O objetivo da atividade de tratamento seja oferecer ou fornecer bens ou serviços a pessoas físicas localizadas no Brasil;
- Os dados pessoais tenham sido coletados em território brasileiro;
- Os dados pessoais coletados pertençam a um titular de dados que se encontre no território brasileiro no momento da coleta.

As seguintes atividades de tratamento de dados estão isentas do escopo de aplicação da LGPD:

- Tratamento efetuado por pessoa física, exclusivamente para fins privados e não econômicos;
- Tratamento para fins jornalísticos e artísticos;
- Tratamento para fins acadêmicos (mas com observância das regras estabelecidas nos artigos 7º e 11º da LGPD);
- Tratamento realizado com o objetivo exclusivo de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;
- As atividades de tratamento de dados pessoais originadas fora do Brasil, de países que oferecem um nível adequado de proteção de dados à LGPD, não estão sujeitas à LGPD, desde que esses dados pessoais não sejam compartilhados ou comunicados aos agentes de tratamento brasileiros.

2.3. Leis Especiais

Com relação à privacidade e proteção de dados no Brasil, as seguintes Leis também se aplicam:

Constituição Federal Brasileira de 1988	Estabelece o direito à privacidade como um direito fundamental e determina a proteção da intimidade, privacidade, honra, imagem e confidencialidade das informações e comunicações pessoais. Além disso, o Projeto de Emenda Constitucional nº 17/2019, atualmente pendente de votação no Plenário da Câmara dos Deputados, busca incluir a proteção de dados pessoais como direito fundamental e estabelece a competência privada da União para legislar em matéria de proteção de dados pessoais.
Código Civil (Lei nº 10.406/2002)	Afirma que a vida privada da pessoa física é inviolável, como um "direito de personalidade" inerente.
Lei da Internet (Lei nº 12.965/2014 e Decreto nº 8.771/2016)	Regulamenta o tratamento de dados pessoais coletados pela internet, especialmente por provedores de serviços de internet e conexão.
Código de Defesa do Consumidor (Lei nº 8.078/1990)	Regula a privacidade e a proteção de dados dos consumidores, garantindo que os consumidores tenham acesso total às suas informações (artigo 43).
Lei de Interceptações Telefônicas (Lei nº 9.296/1996)	Determina que as interceptações telefônicas e telemáticas só podem ocorrer quando autorizada por ordem judicial para fins \de investigação criminal.
Lei de Telecomunicações (Lei nº 9.472/1997)	Regulamenta os direitos dos consumidores à privacidade em relação aos serviços de telecomunicações.

2.4. Alcance Jurisdicional

A LGPD tem aplicação extraterritorial. Em outras palavras, a LGPD também se aplica a entidades não localizadas no Brasil, quando os dados pessoais forem coletados de pessoas físicas localizadas no Brasil ou quando a atividade de tratamento tiver por objetivo oferecer ou fornecer bens ou serviços a pessoas físicas localizadas em território brasileiro.

O titular de dados precisa estar fisicamente localizado dentro da jurisdição brasileira quando os dados são coletados e tratados? Isso ocorre em quais contextos (por exemplo, quando uma empresa está fora do território da União Europeia, no caso da GDPR)? Sim, o titular de dados precisa estar fisicamente localizado no Brasil no momento da coleta e tratamento dos dados, pois o escopo de aplicação da LGPD abrange dados "coletados em território nacional"[3].

Assim, a LGPD é aplicável independentemente do meio, do país em que se encontra a sede do controlador ou do país onde se encontram os dados, desde que se verifique uma das seguintes hipóteses: (i) a atividade de tratamento seja realizada em território brasileiro; (ii) a atividade de tratamento vise a oferta ou prestação de bens ou serviços, ou o tratamento de dados de pessoas físicas localizadas no Brasil; ou (iii) os dados pessoais tenham sido coletados no Brasil.

2.5. Cenários de aplicação da LGPD para Publicidade Digital

Situações hipotéticas para avaliar preocupações/alcance jurisdicional.

Cenário 1: um usuário residente no Brasil (determinado pelo endereço IP ou identificador geográfico) acessa um domínio brasileiro e recebe um anúncio de um anunciante brasileiro. O anunciante usa os dados do usuário para construir um perfil de usuário.
A LGPD é aplicável.

Cenário 2 (usuário fora do Brasil): um usuário conectado, conhecido pelo publisher como residente no Brasil, entra em um domínio brasileiro, mas o endereço IP ou identificador geográfico do usuário indica que ele está localizado fora do Brasil. Um anunciante brasileiro exibe um anúncio e usa os dados do usuário para construir um perfil de usuário.
A LGPD é aplicável desde que os dados pessoais estejam sendo tratados por uma empresa situada no Brasil (o anunciante). De acordo com art. 3º da LGPD, (I), a lei é aplicável quando a atividade de tratamento for exercida em território brasileiro.

- P1: A resposta muda se este for um usuário desconectado, sem nenhuma maneira de saber onde ele está localizado?
  Não, visto que os dados foram coletados e utilizados por uma empresa (anunciante) em território brasileiro.

[3] De acordo com o Artigo 3, parágrafo 1, da LGPD.

Cenário 3 (domínio do publisher fica fora do Brasil): um usuário localizado no Brasil (determinado pelo endereço IP ou identificador geográfico) visita um website hospedado fora do Brasil. Um anunciante brasileiro exibe um anúncio e usa os dados do usuário para construir um perfil de usuário.
A LGPD é aplicável, uma vez que os dados foram coletados no Brasil, o que desencadeia o escopo territorial da LGPD: quando os dados pessoais forem coletados em território brasileiro (de acordo com o Artigo 3, §1, dados pessoais de um titular de dados localizado no Brasil na hora da coleta é considerado como tendo sido coletados no Brasil).

- **P1:** A resposta muda se o website hospedar conteúdo direcionado a residentes brasileiros (por exemplo, um agregador de notícias com uma seção sobre atualidades no Brasil)?
  Não.

- **P2:** A resposta muda se o anunciante estiver localizado fora do Brasil?
  Não.

Cenário 4 (anunciante fora do Brasil): um usuário residente no Brasil (determinado pelo endereço IP ou identificador geográfico) vai para um domínio brasileiro e recebe um anúncio de um anunciante com sede fora do Brasil. O anunciante usa os dados do usuário para construir um perfil de usuário.
A LGPD é aplicável uma vez que os dados foram coletados no Brasil.

- **P1**: A resposta muda se o anunciante tiver uma afiliada/empresa do grupo com sede no Brasil?
  Não. A aplicação da LGPD é desencadeada pelo fato de os dados tratados terem sido coletados em território brasileiro.

3. PRINCIPAIS DEFINIÇÕES | CONCEITOS BÁSICOS

3.1. Coletar:

- Quando um publisher permite o *pixel* de uma adtech em sua página, quem será responsável por "coletar" dados pessoais e, consequentemente, incorrer em obrigações legais (por exemplo, obrigações de controlador/co-controlador nos termos do GDPR ou obrigações de "negócios" nos termos da CCPA): o publisher, a adtech ou ambos?

  Esta ainda é uma área "cinzenta" no Brasil, mas existem duas interpretações diferentes aplicadas pelo mercado, cada qual com seu próprio nível de risco:

  Interpretação A: Considerando uma interpretação literal das definições de controlador e de operador – e até mesmo pelo escopo de aplicação da LGPD – é possível argumentar que o publisher não está tratando nenhum dado pessoal (nesta atividade de tratamento em particular), com a implicação de que todas as obrigações legais serão aplicadas apenas à adtech, como a única controladora.

  Esse entendimento reside no fato de que, neste cenário, o fluxo de dados vai do titular de dados diretamente para o servidor da web da adtech – e o publisher não tem influência ou interferência no processo em si e não tem acesso aos dados coletados, afastando assim a definição de controlador ou operador.

  Interpretação B: Considerando uma interpretação holística e levando em consideração os fundamentos da LGPD, a **Interpretação A** acima pode ser questionada por que pode ser difícil para o titular de dados exercer seus direitos de proteção de dados.

  Nesse cenário, uma vez que o publisher permita a coleta de dados por meio de sua página da web, o gerenciamento da coleta de dados está em seu poder e, portanto, ele deve ser considerado um controlador de dados. A adtech também é controladora de dados, pois será responsável por tomar todas as decisões subsequentes sobre a atividade de tratamento. Muitos profissionais veem isso como a interpretação mais conservadora.

Lembre-se de que, neste cenário, o publisher é quem decide usar a tecnologia de anúncios em seu próprio website e essa decisão é suficiente para colocá-lo em uma posição de controlador de dados, mesmo que não se aplique ao tratamento subsequente pela adtech.

3.2. Tratamento de dados

Qualquer operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Tipo de Informação Coletada	Esta Categoria Independente Constitui Dado Pessoal? (Sim/Não)	Observações (se houver)
Endereço de IP	Sim	
IDs de Anúncios Móveis (IDFA, AAID)	Não	
Identificadores do consumidor como: • ID do dispositivo do usuário • ID persistente do publisher/ID de cookie de vários publishers • ID do domicílio	Não	O identificador em si, quando não contém nenhuma informação que possa identificar um indivíduo (por exemplo, o nome, um número de telefone ou um SSN), não é um dado pessoal.
Identificadores com *hash*, como: • E-mail com *hash* • Endereço IP com *hash*	Não	Os identificadores com *hash*, os quais são considerados informações pseudônimas, só serão considerados dados pessoais se o responsável pelo tratamento tiver as informações adicionais que permitem a identificação do titular de dados.
Agente de Usuário, como: • Sequência de caracteres que identifica o aplicativo • Sistema operacional • Informações do navegador, fornecedor e/ou versão do agente de usuário solicitante	Não	
Informações do Dispositivo, como: • Tipo, versão, configurações do sistema, etc.	Não	
Informações do Website, como: • Nome • URL, etc.	Sim	Essas informações serão consideradas dados pessoais se contiverem identificação pessoal, como nome e sobrenome, ou dados pessoais

		combinados (ou seja, nome e local de trabalho).
Informações de Anúncios, como: • Colocação • Título • ID do criativo, etc.	Não	
Carimbos	Não	
Métricas, como: • Contagens • Quantidade de tempo	Não	
Dados de Eventos, como: • URL completo, incluindo sequência de caracteres de consulta • URL de Referência	Não	Sequências de caracteres de consulta podem conter mecanismos de rastreamento, nomes de usuário, endereços de e-mail e outras informações sobre usuários. Nesses casos, as sequências de caracteres de consulta serão consideradas dados pessoais.
Geolocalização precisa (latitude, longitude)	Sim	Desde que tais dados identifiquem ou potencialmente identifiquem uma pessoa física.
Localização geográfica geral (cidade, estado, país)	Não	A menos que esses dados identifiquem ou potencialmente identifiquem uma pessoa física. Neste caso, eles serão considerados dados pessoais.

3.3. Dados pessoais

Informações relacionadas a uma pessoa física identificada ou identificável.

- **Identificadores digitais pseudônimos são, por si só, dados pessoais (por exemplo, IDFA, IDs de cookies, IDs próprios, endereços IP etc.)?**
  O identificador em si, quando não contém nenhuma informação que possa identificar um indivíduo (por exemplo, o nome, um número de telefone ou um SSN), não é um dado pessoal.

  No entanto, como a definição de dados pessoais em LGPD é contextual (veja o exemplo 1 abaixo para ilustrar este ponto), é importante analisar o contexto de onde esse identificador é comumente usado.

  Quando, de acordo com este contexto, for fácil vincular o identificador ao indivíduo, então o identificador deve ser considerado dado pessoal (ver exemplo 2 abaixo, para melhor esclarecer este ponto).

Nesse sentido, considerando que no setor de adtech é uma prática comum usar outras informações agregadas com identificadores persistentes com o objetivo de identificar um indivíduo, IDs de cookies, IDFA, IDs de proprietários, endereços IP etc., eles devem ser considerados dados pessoais.

Exemplo 1: O Apple Marketing ID (IDFA), inicialmente, não é um dado pessoal para terceiros (embora o seja pela perspectiva da Apple), uma vez que apenas a Apple pode relacionar o IDFA a um indivíduo. No entanto, esse identificador geralmente é compartilhado com um anunciante quando um usuário da Apple clica em um anúncio por meio de seu iPhone.

Após clicar neste anúncio, o anunciante poderia utilizar outros identificadores (ou coletar outras informações do titular de dados) que permitiriam a identificação desse usuário específico. Como esse anunciante possui informações que podem identificar o usuário, ele agora pode vincular o IDFA a um indivíduo identificado, o IDFA será, portanto, considerado dado pessoal.

Exemplo 2: O endereço IP sozinho e por si só não consegue identificar um indivíduo (embora isso possa mudar no futuro, dependendo da implementação do IPv6). Portanto, de uma perspectiva estrita, não se trata de dado pessoal. No entanto, no Brasil, todos os ISPs devem ser capazes de identificar o indivíduo por meio de um endereço IP (que poderia ser divulgado, por exemplo, em uma ordem judicial ou em um inquérito policial), o que significa que, no contexto brasileiro, um endereço IP pode ser facilmente vinculado a um indivíduo e, consequentemente, é considerado dado pessoal do ponto de vista da LGPD.

- **Se a resposta à pergunta acima for "não", se uma Empresa possui um identificador digital persistente no Banco de Dados 1 e tem esse mesmo identificador no Banco de Dados 2 com informações de identificação direta, isso faz com que as informações pseudonimizadas no Banco de Dados 1 sejam consideradas dados pessoais?**

  Da perspectiva da LGPD, o Banco de Dados 1 contém informações pseudonimizadas e o Banco de Dados 2 contém dados pessoais. No entanto, a LGPD não diferencia os dados pessoais dos dados pseudonimizados no que diz respeito às obrigações dos agentes de tratamento, o que significa que os dados pseudonimizados estão sujeitos às mesmas obrigações, princípios e requisitos relativos aos dados pessoais. Em outras palavras, os requisitos legais aplicados ao Banco de Dados 2 devem também ser aplicados ao Banco de Dados 1.

  É importante enfatizar que este não seria o caso se o Banco de Dados 1 e o Banco de Dados 2 pertencessem ou fossem controlados por duas empresas diferentes e essas empresas não compartilhassem informações de identificação direta.

- **A posse de um identificador pseudonimizado e outros dados de identificação indireta pela empresa (por exemplo, idade, sexo, localização geográfica precisa ou imprecisa, sequência de caracteres de agente de usuário, registros de data/hora de acesso) configuraria o conjunto de dados como "dados pessoais"?**
  Uma vez que os dados pseudonimizados (de acordo com a definição da LGPD) são dados pessoais, outros dados vinculados a esse identificador são considerados dados pessoais.

- **A empresa possui "dados pessoais" de um identificador pseudonimizado se ela puder contratar um provedor de serviços ou se envolver em uma transação com um terceiro em que o identificador *possa* corresponder à pessoa, mas a Empresa optar por *não* contratar tal serviço ou realizar tal transação? O simples fato deste serviço estar *potencialmente* disponível para corresponder à pessoa é suficiente para transformar esse identificador pseudonimizado em "dado pessoal"?**
  Não, neste caso, o identificador não será considerado um dado pessoal. O simples fato de haver um serviço disponível que possa identificar um indivíduo por meio de um identificador persistente (como o IDFA) não é o fator determinante para que esse identificador seja ou não considerado um dado pessoal; isso só aconteceria se a empresa decidisse utilizar este serviço e "transformasse" o dado em informação relacionada a um determinado indivíduo.

  Observe que a definição de dados pseudonimizados na LGPD considera que os identificadores e os dados pseudonimizados são sempre mantidos pelo mesmo controlador.

- **Qual é o nível de localização geográfica dos dados pessoais (preciso vs. aproximado)? É necessário estar associado a um identificador para ser considerado PI?**
  A localização geográfica em si e como dados isolados, não são dados pessoais. Mas, se associado a mais dados que possam identificar a pessoa a quem se refere à localização geográfica, devem ser considerados dados pessoais.

  Além disso, conforme indicado acima, o contexto de onde a localização geográfica está sendo usada deve ser avaliado para definir se esses dados são dados pessoais ou não.

- **O identificador de um domicílio é um dado pessoal? (exemplo: se uma empresa tiver um endereço IP residencial (ID em nível de domicílio) e vários IDs de dispositivos exclusivos (por exemplo, MAIDs para cada dispositivo móvel da casa) associados a esse endereço IP, isso afetaria a consideração do identificador doméstico como sendo dado pessoal?)**
  O próprio HHID não é considerado dado pessoal, uma vez que não permite a identificação de um indivíduo em si.

No contexto fornecido, as informações domiciliares devem ser consideradas dados pessoais, uma vez que o endereço IP é um dado pessoal pela perspectiva da LGPD (ver explicação no primeiro item do item 3.2. Acima), a agregação de ambos os identificadores transforma o HHID em dados pessoais.

- **Um identificador com *hash* é um dado pessoal? (Considere que existem serviços comercialmente disponíveis que pegam conjuntos de e-mails cifrados usando *hashes* padrão e retornam alguns (geralmente uma alta porcentagem) de e-mails decifrados. Isso afeta o fato deles serem considerados dados pessoais, se tudo que uma empresa precisa fazer é pagar pelo serviço comercial?)**
  O identificador com *hash* pode ser considerado o mesmo que um identificador persistente, já que geralmente é um *hash* único vinculado a um indivíduo. Considerando isso, uma vez que um identificador com *hash* não contém dados pessoais por si só, e não é possível identificar o indivíduo ligado a esse *hash*, ele não é considerado dado pessoal.

  Além disso, conforme exposto abaixo, dados anonimizados são definidos como "dados relativos a um titular de dados que não pode ser identificado", considerando os meios técnicos razoáveis disponíveis no momento do seu tratamento.

  Considerando que, no contexto fornecido, a tecnologia usada para *hash* destes e-mails não é "razoável" para evitar a identificação de um indivíduo, por isso devem ser considerados dados pessoais.

- **As informações probabilísticas são consideradas dados pessoais?**
  Não, as informações probabilísticas não devem ser consideradas como dados pessoais, a menos que não sejam anônimas e possam identificar o titular de dados ou sejam agregadas a outros dados que possam levar à identificação do titular de dados.

3.4. Dados Sensíveis

Dados pessoais relativos à 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.

3.5. Dados Pseudonimizados

Qualquer dado sujeito a um processo de pseudonimização. Pseudonimização é o processo pelo qual os dados perdem a possibilidade de associação direta ou indireta a um indivíduo, exceto pelo uso de informações adicionais mantidas separadamente pelo controlador em ambiente controlado e seguro.

- **Os dados pseudonimizados são considerados dados pessoais?**
  Dado pseudonimizado é o dado que perde a possibilidade de ser associado, direta ou indiretamente, a um indivíduo, exceto pelo uso de informação adicional mantida separadamente pelo controlador em um ambiente controlado e seguro. Portanto, os dados pseudonimizados deverão ser considerados dados pessoais, pois se referem a uma pessoa física identificável.

  Ou seja, de acordo com a definição da LGPD, o dado pseudonimizado só existe no ambiente de um mesmo controlador, pois, se os identificadores diretos forem mantidos por controladores diferentes (e não trocados entre eles), esses dados são considerados dados pseudonimizados.

  Por exemplo, o RH de um escritório de advocacia compartilha uma lista de nomes de funcionários e suas preferências de marca de smartphone com sua equipe de TI, mas, em vez de fornecer os próprios nomes, eles alteram essas informações para um *hash* exclusivo. A equipe de TI não tem meios de reverter os *hashes* exclusivos dos nomes (e, portanto, está tratando dados pseudonimizados). No entanto, como o RH tem a chave para vincular o *hash* ao nome do funcionário, do ponto de vista do controlador, ele é considerado um dado pessoal.

  No entanto, existem três cenários possíveis, ao avaliar se o dado pseudonimizado é ou não um dado pessoal, dependendo de quem é o agente de tratamento, da seguinte forma:

  1. Controlador de dados que possui as chaves para decifrar uma determinada quantidade de dados ou os valores corretos para desbloquear um registro: as informações serão consideradas dados pessoais, pois o controlador pode identificar a quem os dados se referem e, assim, identificar o titular de dados.
  2. O operador que trata dados em nome do controlador dos dados, mas não tem o acesso às chaves ou aos valores para decifrar ou remover o *hash* do registro: os registros não serão considerados dados pessoais, porque o operador é incapaz de associar, direta ou indiretamente, eles a uma pessoa física.
  3. Co-controlador que também determina as finalidades do tratamento, mas não possui as chaves para descriptografar uma determinada quantidade de dados ou os valores corretos para remover o *hash* de um registro: os registros não serão considerados dados pessoais, porque o controlador não pode associá-los a uma pessoa física determinada.

- **A lei sujeita os dados pseudonimizados a menos obrigações do que os dados pessoais "comuns"?**
  Não. Todas as obrigações e requisitos aplicados a dados pessoais "normais" também se aplicam a dados pseudonimizados. A pseudonimização de dados pessoais é considerada apenas um mecanismo técnico interno para melhorar a segurança e a proteção de dados pessoais.

3.6. Dados Anonimizados/Desidentificados

A LGPD define dados anônimos como "dados relativos a um titular de dados que não pode ser identificado, considerando o uso de meios técnicos razoáveis disponíveis no momento do tratamento". Uma vez que os dados anônimos não são considerados dados pessoais, os dados anonimizados não se enquadram no escopo da LGPD.

- **Há diferença entre dados anonimizados ou desidentificados?**
  A LGPD não possui uma definição específica para dados desidentificados, mas na prática, considerando a definição de dados anonimizados (citada acima), poderia ser considerada a mesma.

- **Quais categorias de dados comuns são passadas entre publishers, anunciantes e adtechs que se enquadram nesta categoria quando nenhum identificador persistente está presente (por exemplo, tipo de navegador, tipo de dispositivo, sistema operacional, nome do aplicativo, site do publisher)?**
  Essas informações por si só podem não ser consideradas dados pessoais, mas quando associadas a informações que possam levar à identificação do indivíduo, elas se enquadram na definição de dados pessoais. O tipo do navegador ligado a um endereço IP, por exemplo, é considerado dado pessoal.

3.7. Controlador dos Dados

Pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões sobre o tratamento de dados pessoais.

3.8. Controlador Conjunto/Co-Controlador

Não há definição ou regras específicas aplicáveis ao controlador conjunto ou co-controlador.

3.9. Operador dos Dados/Prestador de Serviços (ou seja, uma entidade qualificada como um operador ou prestador de serviços de acordo com a lei porque atende a certos requisitos e trata dados de acordo com uma finalidade legítima em nome de um controlador/empresa)

Pessoa física ou jurídica, de direito público ou privado, que trata dados pessoais em nome do controlador.

3.10. Terceiro (ou seja, um terceiro que recebe dados de uma empresa para fins não comerciais e não tem necessariamente requisitos específicos ao abrigo da

lei quanto a esses dados, como um terceiro ao abrigo da CCPA)

Não há definição ou regras específicas aplicáveis a terceiros.

3.11. Consentimento

Manifestação livre, informada e inequívoca pela qual o titular de dados concorda com o tratamento dos seus dados pessoais para um determinado fim.

3.12. Encarregado de Dados

”DPO” ou, em português, “Encarregado de Dados”: pessoa designada pelo controlador ou operador para atuar como canal de comunicação entre os titulares de dados e a Autoridade Nacional de Proteção de Dados (“ANPD”).

3.13. Informações a Nível de Domicílio

Não existe uma definição de informação a nível de domicílio na LGPD.

3.14. Transferência Internacional de Dados

Uma transferência de dados pessoais para um país estrangeiro ou para uma entidade internacional da qual o país (Brasil) seja membro.

3.15. Relatório do Impacto à Proteção de Dados Pessoais

Uma 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.

3.16. Criação de Perfil/ Perfilamento

A LGPD não define especificamente o perfilamento e não há precedentes a respeito dessa situação.

3.17. Decisões Automatizadas

Não existe uma definição específica sobre decisões automatizadas, no entanto, o Artigo 20 da LGPD afirma que o titular de dados tem o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

4. DIREITOS E RESPONSABILIDADES DO CONTROLADOR DOS DADOS

Antes de avaliar as principais características do controlador de dados, aqui estão algumas notas sobre as atividades de marketing e publicidade digital no Brasil.

4.1. Breves Notas sobre marketing e publicidade no Brasil

O marketing direto é definido como o conjunto de estratégias empregadas para atingir um público-alvo que já demonstrou algum tipo de interesse em um produto ou serviço e tem muito mais probabilidade de convertê-lo em uma compra, cobrindo qualquer material publicitário ou promocional, não apenas comercial. Este é o caso de anúncios realizados através de meios on-line e off-line, como mensagens, e-mail de marketing, telefonemas, SMS, aplicações de mensagens, mídias sociais e web banners. Alguns conteúdos online são apresentados sem tratamento de quaisquer dados pessoais, por exemplo, sempre que o mesmo conteúdo seja apresentado a todas as pessoas que visitam um website, sem visar um público/indivíduo específico; neste caso, a proteção de dados não se aplica.

Ao contrário da GDPR, a legislação brasileira é omissa quanto à legalidade do tratamento de dados para fins de marketing e publicidade. Portanto, é possível realizar marketing direto e/ou publicidade por consentimento ou por *legítimo interesse do controlador*.

Se uma empresa optar por utilizar consentimento para fins de marketing e publicidade, geralmente obterá o consentimento de um indivíduo antes de enviar textos de marketing, e-mails ou fazer chamadas telefônicas e, normalmente, também obterá consentimento para compartilhar detalhes do cliente com outra organização. O consentimento deve ser uma manifestação informada, inequívoca e concedida livremente pelo titular de dados, autorizando o tratamento de seus dados pessoais para fins de marketing e publicidade.

A forma mais clara de obter o consentimento para estes fins é convidar o cliente a *opt-in* voluntariamente à publicidade, confirmando que pretende receber comunicações de marketing através de canais específicos (correio, e-mail, chamada, SMS etc.). A adesão voluntária, quando disponível, é uma prática recomendada à todas as organizações, uma vez que fornece uma declaração clara e proeminente, além de uma política de privacidade geral, explicando que a ação positiva de "marcar a caixa do *opt-in*" indica consentimento para receber marketing comunicação dessa organização, por exemplo.

Observe que as comunicações essenciais ou legalmente obrigatórias para o fornecimento dos bens ou serviços em si são consideradas comunicações comerciais e podem ser enviadas independentemente de consentimento. É o caso de um e-mail enviado para recuperação de senha, de uma comunicação informando um erro ou detecção de fraude. Os provedores precisam ser o mais claro possível sobre quais informações são obrigatórias para o fornecimento do produto ou serviço e quais informações os

titulares de dados podem escolher receber.

Portanto, uma forma de realizar atividades de marketing direto é confiar no consentimento e em suas regras gerais, incluindo a transparência e os direitos do titular de dados de retirar o seu consentimento e de se opor ao tratamento de dados posterior a partir deste momento.

No entanto, alguns juristas adotam uma interpretação mais flexível da Lei sobre este ponto, com base em argumentos de que os requisitos de consentimento poderiam diminuir significativamente a capacidade das empresas de anunciar, comunicar ao público, lançar novos produtos no mercado e ainda com base no fato da publicidade ser uma ferramenta essencial de comunicação com os consumidores, além de ter o poder de aumentar a demanda, ampliar a concorrência e até mesmo fortalecer a inovação – desempenhando, assim, um papel fundamental no desenvolvimento econômico.

Portanto, também é possível que as empresas realizem atividades de marketing e publicidade no Brasil com base em legítimo interesse, ao invés de obter consentimento prévio e expresso. O aspecto mais importante deste cenário é respeitar o *opt-out*, que é o mecanismo pelo qual os titulares de dados manifestam as suas expectativas de forma clara contra a utilização de seus dados para esses fins. Em outras palavras, a LGPD permite embasamento jurídico de legítimo interesse para fins de marketing e publicidade, nomeadamente quando o tratamento de dados pessoais visa apoiar as atividades do responsável pelo tratamento ou atos em benefício dos titulares de dados.

Lembre-se de que o "legítimo interesse" não pode ser usado como base legal para o tratamento de dados pessoais confidenciais em vez de receber consentimento.

Apesar das semelhanças entre LGPD e GDPR, há mais flexibilidade na legislação brasileira quando se trata de atividades de marketing e publicidade. Por exemplo, não há equivalente na LGPD ao Artigo 21 (1) ou (2) da GDPR, que permite ao titular de dados se opor ao tratamento com base em legítimo interesse ou quando realizado para atividades de marketing. Também não há equivalente no Brasil à *ePrivacy Directive* europeia, que exige consentimento para cookies não essenciais.

No entanto, a GDPR é influente no cenário de privacidade brasileiro. As melhores práticas da Europa são frequentemente aplicadas para construir compreensão e argumentos para alguns dos tópicos abaixo.

Isto posto, explicaremos, a seguir: (i) a visão geral sobre as características do controlador de dados previstas na LGPD (item 4.2); (ii) algumas notas sobre prestação de contas (item 4.3); (iii) os requisitos do aviso de privacidade (item 4.4); (iv) a análise específica sobre o consentimento e suas exceções (item 4.5); (v) os fins apropriados (item 4.6); e (vi) as salvaguardas necessárias (item 4.7).

4.2. Visão geral

Responsabilidades do Controlador de Dados:

- Cumprir todos os direitos do titular de dados;
- Cumprir as obrigações de notificação de incidentes de segurança;
- Manter um registro das atividades de tratamento de dados;
- Implementar medidas técnicas e administrativas de segurança para proteger os dados pessoais de acessos não autorizados e situações ilícitas ou acidentais de destruição, perda, modificação, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito;
- Elaborar relatórios de impacto à proteção de dados quando solicitado pela ANPD, ou em situações em que a atividade de tratamento imponha elevados riscos aos princípios de proteção de dados estabelecidos na LGPD, conforme regulamentado pela ANPD;
- Nomear um DPO.

Outra responsabilidade do controlador é indicar a base jurídica que autoriza o tratamento de dados pessoais. Quando se trata de publicidade digital, normalmente, há duas bases aplicáveis: consentimento do titular de dados e legítimo interesse. Há uma opacidade na Lei sobre essas duas bases e isso será tratado no tópico 4.5.2.

Como os Controladores de Dados são definidos

Os controladores e operadores são definidos de acordo com a forma como estão envolvidos nas atividades de tratamento de dados pessoais. Os controladores são os agentes encarregados de tomar decisões sobre o tratamento de dados pessoais.

A posição do controlador e do operador deve ser definida para cada atividade de tratamento de dados, o que significa que uma única organização pode ter processos em que figura como controlador e outras, onde figura como operador.

Responsabilidades do Controlador de Dados

É importante notar que a responsabilidade estrita pode ser imposta ao controlador e ao operador em relação às atividades de tratamento de dados, especialmente quando os titulares de dados são consumidores. Em outros casos, há espaço para diferentes tipos de responsabilização. Por exemplo, se o operador vai contra as instruções do controlador, esse operador sozinho será responsável na maioria das circunstâncias.

Assim, os agentes de tratamento de dados pessoais devem garantir que o tratamento seja realizado de forma adequada, proporcional e limitada ao mínimo necessário para o cumprimento de uma finalidade específica. Além deste requisito, a LGPD também estabelece uma série de outras obrigações e responsabilidades associadas ao tratamento de dados pessoais.

Ainda de acordo com o texto aprovado, além de cumprir a Lei, cabe ao agente de tratamento de dados tomar medidas eficazes e efetivamente capazes de demonstrar o cumprimento das normas. Essa obrigação faz parte do princípio de responsabilização que deve ser cumprido pelo agente de tratamento.

Legalidade do Tratamento

A LGPD exige que os controladores ou operadores que executam uma atividade de tratamento seguindo as instruções do controlador tenham uma base legal apropriada para tratar dados pessoais comuns ou sensíveis. Conforme explicado a seguir, as bases jurídicas pelas quais os dados pessoais sensíveis podem ser tratados são mais rigorosas do que as estabelecidas para os dados pessoais comuns.

Isto posto, de acordo com a LGPD, o tratamento de dados pessoais comuns só pode ser realizado nas seguintes circunstâncias:

(i) Com o consentimento do titular de dados;

(ii) Para cumprimento de uma obrigação legal ou regulamentar por parte do controlador;

(iii) Pela administração pública, para o tratamento e utilização partilhada de dados necessários à execução de políticas públicas previstas em leis ou regulamentos, ou com base em contratos, acordos ou instrumentos semelhantes;

(iv) Para a realização de estudos por entidades de investigação, garantindo, sempre que possível, a anonimização dos dados pessoais;

(v) Quando necessário para a execução de um contrato ou procedimentos preliminares relacionados a um contrato do qual o titular de dados seja parte, a pedido do titular de dados;

(vi) Para o exercício regular de direitos em procedimentos judiciais, administrativos ou arbitrais;

(vii) Para a proteção da vida ou segurança física do titular de dados ou de terceiros;

(viii) Proteger a saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridades sanitárias;

(ix) Quando necessário para atender aos legítimos interesses do controlador ou de terceiros, exceto quando prevalecem os direitos e liberdades fundamentais do titular de dados que exigem a proteção dos dados pessoais.

(x) Para a proteção de crédito, inclusive conforme previsto em legislação específica.

Quando o consentimento for a base legal utilizada, o responsável pelo tratamento deve obter o consentimento livre, informado e inequívoco do titular de dados por escrito ou por qualquer outro meio que possa garantir o consentimento do titular de dados para ambos – tratamento e compartilhamento de dados pessoais com outras empresas. O titular de dados poderá retirar tal consentimento a qualquer momento.

Além disso, a autoridade nacional poderá solicitar ao responsável pelo tratamento um relatório de impacto à proteção de dados (“DPIA”) quando o tratamento se basear no seu legítimo interesse, respeitando o sigilo comercial e industrial.

Conforme supramencionado, no entanto, os dados pessoais sensíveis só podem ser tratados com fundamento nas bases legais previstas no artigo 11º da LGPD, que excluem a proteção de crédito, a execução de um contrato (embora seja possível o tratamento de dados para o exercício de direitos que

decorrem de um contrato) e legítimo interesse, da seguinte forma:

> *I - Quando o titular de dados ou seu representante legal consentir de forma expressa e distinta, para os fins específicos.*
> *II -Sem consentimento do titular de dados, nas situações em que for imprescindível:*
> a) Conformidade do controlador com uma obrigação legal ou regulatória;
> b) Tratamento compartilhado de dados quando necessário pela administração pública para a execução de políticas públicas previstas em leis ou regulamentos;
> c) Estudos realizados por órgão de pesquisa, sempre que possível garantindo a anonimização dos dados pessoais sensíveis;
> d) O exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (a "Lei de Arbitragem Brasileira");
> e) Proteger a vida ou a segurança física do titular de dados ou de terceiros;
> f) Proteger a saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridades sanitárias (Lei nº 13.853/2019);
> g) Garantir a prevenção de fraudes e a segurança do titular de dados, nos processos de identificação e autenticação de registro em sistemas eletrônicos, respeitados os direitos referidos no art. 9º desta Lei e exceto quando prevaleçam os direitos e liberdades fundamentais do titular de dados que requeiram a proteção dos dados pessoais.

A partir daí, à semelhança da GDPR, antes da atividade de tratamento, deve existir uma base jurídica que a suporte.

4.3. Responsabilização e Prestação de Contas

4.3.1. Visão geral

A responsabilização e prestação de contas é um dos princípios fundadores da LGPD, definido no Artigo 6 - X como *"demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar o cumprimento das regras de proteção de dados pessoais, incluindo a eficácia de tais medidas"*.

As regras da LGPD em relação à responsabilização e prestação de contas são aquelas que estabelecem a responsabilidade dos agentes de tratamento, que abordaremos mais adiante.

4.3.2. Aplicação na Publicidade Digital

Não há requisitos de responsabilização e prestação de contas específicos para o setor de publicidade digital.

Para os setores de publicidade digital, as principais medidas de responsabilização e prestação de contas que podem ser usadas são:

- Quando aplicável, manter um registro (por exemplo, logs) do consentimento fornecido, incluindo

quando e como foi fornecido (por exemplo, tipo de linguagem usada, quando a isenção de responsabilidade de consentimento foi inserida etc.);
- Gerenciar *opt-outs* de maneira rápida, especialmente quando o tratamento se baseia em legítimo interesse;
- Prestar contas sobre todos os terceiros que tiveram acesso aos dados de todos os titulares de dados afetados pelas suas atividades;
- Elaboração de LIAs/DPIAs de suas atividades mais críticas (por exemplo, uso de cookies de terceiros; tecnologias de rastreamento entre dispositivos, agregação de dados adquiridos de agências de dados, etc.).

4.4. Avisos

4.4.1. Visão geral

A LGPD afirma que o titular de dados deve ser capaz de acessar informações claras, precisas e de fácil acesso sobre as atividades de tratamento de dados que estão sendo realizadas.

- **Quando o aviso deve ser fornecido? O que deve estar no anúncio no contexto da publicidade digital?**

  (Considere também, que tipo de aviso precisa ser fornecido quando os pixels são disparados em uma página da web?)

  Em geral, é melhor avisar o titular antes da coleta de dados pessoais ou o mais rápido possível. Por exemplo, ao usar cookies ou *pixel tags* que carregam antes da visualização da página inicial (tratamento de dados pessoais antes da possibilidade de exibir qualquer informação ao titular de dados), é recomendável apresentar o aviso assim que o website for carregado.

  No entanto, o mais importante é que as informações sobre as atividades de tratamento possam ser facilmente acessadas pelos titulares de dados, o que significa que os links para avisos de privacidade e documentos semelhantes devem ser fáceis de encontrar. No contexto da publicidade digital, geralmente é melhor fornecer informações sucintas no início e disponibilizar o link da política de privacidade para que os titulares de dados possam saber mais.

  É importante observar que a LGPD não prevê nenhuma forma específica de divulgação de avisos de privacidade ou *disclaimers* para cookies (ou qualquer outra tecnologia de rastreamento). Portanto, o exemplo acima está alinhado com a prática geral das empresas brasileiras.

  Geralmente, esses banners de cookies possuem um texto simples com a indicação de um link onde o titular de dados pode obter mais informações. Por exemplo: "*Este website usa cookies e outras tecnologias semelhantes para oferecer publicidade personalizada. Para obter mais informações, consulte nossa Política de Cookies (ou Política de Privacidade).*"

  Se o website não pretende coletar consentimento para o uso de pixel ou cookies nos navegadores dos titulares de dados, é importante que este banner de cookie não tenha um

botão que diga "Aceito" ou "Autorizo" ou qualquer outra coisa que possa ser interpretado como forma de obtenção de consentimento.

- **Existe um requisito de notificação específico para dados pessoais sensíveis?**
  Não, não há requisitos de notificação específicos para dados pessoais sensíveis.

- **Existem requisitos específicos para fornecer notificações relacionadas ao tratamento de dados pessoais de crianças?**
  Sim. Para o tratamento de dados pessoais de crianças (0 a 12 anos) e adolescentes (13 a 17 anos), o artigo 14 §6º da LGPD exige que os responsáveis pelo controle forneçam notificações de forma simples, clara e acessível para fornecer as informações necessárias aos pais ou representante legal, e a notificação deve ser adequada para a compreensão das crianças. O tratamento de dados deve ser realizado tendo em mente o melhor interesse das crianças e adolescentes. Tal notificação deve levar em consideração as capacidades físico-motoras, perceptivas, sensoriais, intelectuais e mentais do titular de dados, utilizando recursos audiovisuais quando for o caso.

  Além disso, no tratamento de dados pessoais das crianças, os responsáveis pelo tratamento devem disponibilizar informações sobre os tipos de dados recolhidos, a forma como são utilizados e os procedimentos para o exercício dos direitos dos titulares de dados. Uma referência à informação dita na política de privacidade basta.

- **Existem requisitos que obrigam os fornecedores a coletar dados pessoais diretamente ou aqueles que as recebem de terceiros para fornecer avisos adicionais? Quem é o responsável por esses avisos? Publishers? Os fornecedores?**
  A LGPD estabelece que "o titular de dados tem direito a acesso facilitado às informações relativas ao tratamento", mas não especifica quem é o responsável pelo fornecimento delas. Apesar disso, o entendimento atual é de que cabe ao controlador que está coletando os dados do titular de dados a responsabilidade pelo aviso. Esse entendimento é baseado nos seguintes pontos:
  - O princípio da transparência, base das obrigações de notificação na LGPD, exige que os titulares de dados sejam informados sobre a atividade de tratamento e os agentes de tratamento (artigo 6º, VI). Apenas os controladores de dados têm a possibilidade de divulgar quais agentes de tratamento estão envolvidos em uma atividade de tratamento;
  - O Controlador é responsável por tomar decisões sobre a atividade de tratamento, especialmente a forma e a finalidade. As informações que devem ser disponibilizadas no aviso (como finalidade do tratamento, identificação e contato do controlador, forma e duração do tratamento etc.) só podem ser conhecidas, de antemão, pelo controlador;
  - O artigo 18º, que define os direitos do titular de dados, prevê que todos os direitos devem ser obtidos do controlador, incluindo o direito de acesso aos dados e informações sobre agentes públicos e privados com quem o controlador tenha compartilhado dados;

Isso não significa que os controladores não possam confiar nos operadores para avisar ao titular de dados, mas apenas que a responsabilidade final (e oponível a terceiros) não pode ser delegada.

Nesse caso, o publisher será responsável por informar ao titular de dados que seus dados estão sendo coletados e compartilhados com SSPs, DSPs, anunciantes etc.

Não obstante, o artigo 8º §6º da LGPD determina que, havendo alteração na atividade de tratamento de dados, o responsável pelo tratamento deverá informar o titular de dados, destacando especificamente o conteúdo das alterações. Portanto, é razoável supor que o controlador sempre será responsável por fornecer os avisos.

4.4.2. Aplicação à Publicidade Digital

- **Os terceiros precisam ser identificados? Por exemplo, se um editor fornecer um aviso de privacidade que indica que ele poderá compartilhar dados pessoais com terceiros para fins publicitários, é necessário especificar quais terceiros? As atividades ou propósitos específicos de publicidade digital também precisam ser divulgadas (por exemplo, propósitos TCF)?**
  A LGPD atribui ao controlador e ao operador o dever de transparência para com os titulares de dados, o que significa que devem garantir aos titulares de dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e respectivos agentes de tratamento, sujeito a sigilo comercial e industrial (art. 6º, VI, LGPD).

  Na mesma linha, para efeitos de conformidade LGPD, bastaria que a empresa que trata os dados pessoais divulgue ao titular de dados o fato que compartilha dados com terceiros na política de privacidade/aviso, sem necessidade de indicar terceiros nominalmente, além de indicar os fins do compartilhamento.

  Em outras palavras, as empresas precisam divulgar em seus avisos de privacidade as categorias de terceiros com os quais compartilham dados, e não os nomes reais das empresas desses terceiros.

  Ressalta-se que é obrigatório que as empresas divulguem a finalidade do compartilhamento, conforme o disposto no art. 9º, V, da LGPD:

  "Artigo 9. O titular de dados tem direito ao acesso facilitado às informações sobre o tratamento dos seus dados, as quais deverão ser disponibilizadas de forma clara, adequada e ostensiva, respeitando, entre outras características previstas no regulamento para cumprimento do princípio de acesso gratuito:

  V-informações sobre o uso compartilhado de dados pelo controlador e a finalidade."

Dito isso, vamos ver um exemplo:

» Uma empresa de marketing coleta dados de titulares de dados localizados no Brasil com o objetivo de marketing/publicidade. Ao coletar o consentimento dos titulares de dados por meio de uma caixa de opção de adesão voluntária (*opt-in*), a empresa apresenta uma declaração clara e destacada, indicando que os dados fornecidos pelo usuário serão utilizados para fins de marketing/publicidade, deixando implícito que haverá compartilhamento de dados pessoais com terceiros.

No exemplo acima, é necessário que o aviso divulgue aos usuários que seus dados serão compartilhados com terceiros e que eles poderão saber mais sobre esse compartilhamento no aviso de privacidade.

Entretanto, idealmente, considerando que a base legal adotada no exemplo é o consentimento e que tal base legal refere-se a finalidades específicas (de acordo com o artigo 8, o parágrafo quatro, da LGPD), a empresa que tratará os dados deverá indicar todas as finalidades pretendidas, na medida do possível (isto é, uso dos dados para anúncios, cookies, trackers etc. essenciais ou personalizados). Isso significa que, se as "finalidades de marketing" incluírem outras finalidades, essas finalidades deverão ser especificadas e informadas ao titular de dados, o que não significa que o controlador terá que obter consentimento para cada uma das finalidades.

Em relação à necessidade de nomeação de todos os terceiros, não há obrigação legal expressa de o fazer, salvo a indicação de que os dados pessoais tratados serão compartilhados com terceiros.

Não obstante, se a empresa já possuir uma lista contendo todos os fornecedores ou empresas com quem os dados dos titulares de dados podem ser compartilhados, esta poderá ser disponibilizada no aviso de privacidade de forma a respeitar o princípio da transparência, embora não seja obrigatório.

Por outro lado, se o titular de dados exercer o seu direito de acesso aos seus dados pessoais, solicitando um relatório completo dos seus dados nos termos do artigo 19º, II, da LGPD, a empresa será legalmente obrigada a apresentar os nomes dos terceiros com quem compartilham os dados pessoais. Observe que pode haver espaço para não fornecer a lista completa de terceiros se isso for considerado um segredo comercial.

Por último, é importante destacar que muitos publishers no Brasil identificam os terceiros que colocaram cookies ou *pixels* em seus websites. Esta prática não inclui a identificação de terceiros envolvidos nas outras etapas da cadeia. Portanto, se um cookie foi colocado em um determinado site por um SSP que posteriormente compartilhará as informações do titular de dados com um DSP, o publisher é obrigado apenas a divulgar em relação ao SSP e não ao DSP.

Normalmente, os publishers fornecem uma lista geral de cookies/rastreadores colocados em seus

websites, indicando o nome do cookie, sua finalidade e seu “proprietário”, como no exemplo abaixo:

Os cookies que usamos em nosso website são:

Terceiro	Finalidade
Mídia Específica	Tecnologia utilizada para divulgar mensagens personalizadas e publicidades em vídeos, a partir de sua interação com nosso website.

- **De uma perspectiva da indústria, é comum distinguir o uso de dados para segmentação de anúncios vs. construção de perfil vs. medição de campanhas publicitárias. O requisito de notificação exige a divulgação separada dessas coisas? Ou basta dizer algo geral como “publicidade e fins relacionados”?**
  Não há exigência legal para mencionar especificamente esses conceitos, mas a LGPD afirma que o tratamento deve ser feito "para fins legítimos, específicos e explícitos dos quais o titular de dados é informado", o que significa que os fins precisam ser divulgados tão claramente quanto possível.

No entanto, a prática geral do mercado não é ser muito específica para fins publicitários, divulgando apenas que os dados coletados serão utilizados para “fins publicitários e afins”, prática que pode ser questionada pelas autoridades brasileiras. É importante ressaltar que não temos nenhum caso ou ação judicial recente contestando essa prática.

4.5. Consentimento e Exceções ao Consentimento

4.5.1. Visão geral

- **Para que tipos de dados pessoais ou finalidades de tratamento é necessário obter consentimento?**

A base jurídica do consentimento é aplicável a qualquer tipo de dados pessoais comuns ou dados pessoais sensíveis, desde que o consentimento seja dado por escrito ou por outro meio capaz de demonstrar a manifestação da vontade do titular de dados, se referindo a finalidades específicas. Assim, a LGPD proíbe o tratamento de dados pessoais se o consentimento for insuficiente e, também, considera nulo o consentimento que não se refira a finalidades específicas.

Se o consentimento se referir a múltiplas finalidades, a empresa que trata os dados pessoais deverá indicá-las ao titular de dados, na medida do razoavelmente possível. No entanto, a LGPD não obriga a coletar um consentimento específico para cada uma das finalidades, mas sim um único consentimento, abrangendo todas as finalidades.

Além disso, observe que se o consentimento for dado por escrito, ele deve ser incluído em uma cláusula que se destaque das demais cláusulas contratuais e de forma que destaque todas as finalidades do tratamento.

Por outro lado, se houver alteração (i) da finalidade específica do tratamento; (ii) o tipo e a duração do tratamento, sendo observado o sigilo comercial e industrial; (iii) a identificação do controlador; ou (iv) as informações sobre a utilização compartilhada de dados pelo controlador e a finalidade, o controlador deverá informar o titular de dados, destacando especificamente o conteúdo das alterações, caso em que o titular de dados poderá retirar o citado consentimento se eles discordarem sobre a alteração (conforme art. 8º, parágrafo sexto, da LGPD).

Em suma, se houver qualquer alteração em qualquer das informações mencionadas em (i), (ii), (iii) e (iv), o controlador deve notificar o titular de dados e obter novo consentimento. Esta obrigação não se aplica, por exemplo, se o controlador alterar suas informações de contato.

Além disso, é importante notar que, em regra, o tratamento dos dados pessoais das crianças deve ser realizado com base no consentimento dos pais, especialmente para fins de marketing e publicidade. Por outro lado, quando o tratamento é necessário para contatar os pais ou responsável legal, realizado apenas uma vez e sem armazenamento, ou é para proteção da criança, desde que os dados pessoais não sejam cedidos a terceiros, em nenhuma circunstância. O consentimento dos pais ou representantes legais poderá ser dispensado no melhor interesse da criança, que prevalecerá nos referidos casos.

- **Como o consentimento é manifestado - consentimento expresso, consentimento implícito ou opt-out?**

O consentimento deve ser sempre obtido (i) por meio de demonstração da vontade do titular de dados; (ii) antes da atividade de tratamento; (iii) por livre escolha do titular de dados; (iv) após o titular de dados ter recebido informações claras sobre a atividade de tratamento; e (v) por meio de um ato proativo do usuário indicando sua aceitação, ou seja, marcando uma opção de adesão voluntária, com uma declaração clara e destacada, além de uma política geral de privacidade, explicando que a ação proativa de “marcar a caixa” indica consentimento para receber marketing ou publicidade da empresa.

Além disso, quando o consentimento for dado por escrito (por exemplo, em um contrato), ele deve ser incluído em uma cláusula que se destaque das demais cláusulas contratuais.

- **É necessário um aviso específico como parte do consentimento?**

Sim. No entanto, o aviso específico sobre o consentimento é implicitamente exigido pela LGPD, pois o consentimento deve ser informado, o que significa que o titular de dados deve estar ciente do que está consentindo.

- **A obrigação de consentimento exige granularidade (ou seja, consentimento para atividades de tratamento distintas) semelhante à GDPR? Ou a obrigação de consentimento é mais**

generalizada (por exemplo, exigir que os consumidores optem pela "publicidade comportamental online" de forma mais ampla, sem ter que consentir com cada atividade/parte de tratamento constituinte)? O consentimento é diferente para usos ou tipos distintos de dados (por exemplo, dados confidenciais, criação de perfil, tomada de decisão automatizada etc.).

Não. A LGPD não estabelece requisitos específicos em relação à granularidade de uma opção de adesão voluntária. No entanto, o consentimento deve estar relacionado a uma finalidade específica e a LGPD determina explicitamente que "as autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas". Dito isso, é altamente recomendável ser tão específico quanto a situação permitir. Além disso, existem três situações em que a LGPD estabelece que o consentimento deve referir-se a um propósito distinto de outros: quando o consentimento for dado para (i) tratamento de dados pessoais sensíveis, (ii) tratamento de dados de crianças e (iii) transferência internacional de dados (se o consentimento foi escolhido pelo controlador como o mecanismo de transferência). Essas situações podem ser comparadas, mas não são necessariamente equivalentes, ao conceito de granularidade.

É importante observar que esses conceitos ainda não foram aplicados pelas autoridades competentes, e a prática geral no mercado é não ser muito específico em relação a fins publicitários, divulgando apenas que o consentimento é para "fins publicitários". No entanto, uma vez que a LGPD prevê a exigência de finalidade específica para consentimento válido, essa prática (ser genérica quanto à finalidade), poderá ser questionada pelas autoridades.

Este entendimento se aplica à criação de perfil, tomada de decisão automatizada etc. A LGPD é ainda mais enfática ao dizer que deve haver apenas consentimento específico para dados sensíveis. Portanto, se uma atividade de tratamento envolver dados pessoais sensíveis, é obrigatório que seja obtido consentimento específico para este tipo de dado. Por exemplo:

( ) Autorizo que os meus dados pessoais (nome, e-mail, telefone e localização geográfica) sejam tratados para fins publicitários. Para obter mais informações, consulte nosso Aviso de Privacidade.
( ) Autorizo a utilização dos meus dados pessoais sensíveis (biometria facial) para tratamento publicitário. Para obter mais informações, consulte nosso Aviso de Privacidade.

- **Os dados pessoais podem ser tratados para finalidades secundárias (ou seja, finalidades diferentes para as quais foi coletado)?**

  Via de regra, o tratamento para fins não informados é vedado, conforme definição do princípio de "finalidade", do artigo 6º da LGPD.

  Além disso, o artigo 8º §6º da LGPD estabelece que, sempre que houver alteração na finalidade específica do tratamento, o controlador é obrigado a informar o titular de dados sobre essa alteração. Se a base jurídica do tratamento for o consentimento, o titular de dados tem o direito de revogá-lo.

No entanto, a LGPD estabelece duas situações em que o tratamento para fins secundários é permitido: o tratamento de dados pessoais acessíveis ao público (artigo 7º §3º) e o tratamento de dados manifestamente tornados públicos pelo titular de dados (artigo 7º §4º).

De acordo com o Artigo 7º §7º:
"*O tratamento posterior dos dados pessoais a que se referem os parágrafos terceiro e quarto deste artigo pode ser realizado para novos fins, desde que sejam observados os fins legítimos e específicos para o novo tratamento e a preservação dos direitos do titular de dados, bem como os fundamentos e princípios estabelecidos nesta Lei.*"

- **Existem regras que obrigam os destinatários/operadores *downstream* de dados pessoais de fornecer avisos adicionais?**
  Não, não há obrigação de fornecer avisos adicionais pelos destinatários/operadores.

- **Existem questões relativas ao momento do consentimento?**
  Não existe uma regra expressa sobre o momento do consentimento, a não ser que deve ocorrer antes do tratamento/coleta de dados.

- **Como o timing do consentimento afeta o disparo de pixels quando o usuário acessa uma página?**
  Considerando que os pixels estão geralmente associados a cookies, o ideal seria notificar o usuário sobre o uso de cookies da plataforma assim que acessar o website, e oferecer ao usuário a opção de desativá-los, o que, consequentemente, também desativaria os pixels, a priori. Além disso, embora a LGPD não exija expressamente que as empresas o façam, as empresas brasileiras têm elaborado políticas de cookies que informam ao titular de dados as práticas da empresa em relação à ferramenta.

- **Os requisitos previstos no Brasil em relação à notificação dos usuários e ao uso de pixels são equivalentes a como as empresas fazem isso para o GDPR hoje ou os requisitos são substancialmente mais/menos específicos?**
  No geral, são equivalentes. Tanto a GDPR quanto a LGPD não regulam especificamente o uso de cookies (o GDPR menciona "cookies" apenas uma vez, nos [4]Considerandos 30, e a LGPD não menciona "cookies" de forma alguma).

[4] Considerandos: dispositivos introdutórios previstos na legislação europeia GDPR que dispõem em linguagem acessível orientações para interpretação dos artigos de leis do GDPR.

No entanto, na União Europeia, a conformidade com cookies é gerenciada de acordo com a ePrivacy Directive (EPD) que, entre outras disposições, determina que o agente de tratamento deve, antes de usar cookies, obter o consentimento do usuário, documentar e armazenar os consentimentos recebidos facilita para os usuários retirarem o consentimento etc. A legislação brasileira é omissa sobre o assunto. No entanto, o novo regulamento de privacidade eletrônica, que atualmente está sendo discutido pela UE, irá se basear no EPD e expandir suas definições, portanto, espera-se que a conformidade com cookies na UE exija mais esforços das empresas locais, ao contrário do Brasil, onde o cumprimento da EPD deve ser suficiente até que a ANPD decida de outra forma.

- **Existem requisitos de consentimento distintos para dados pessoais sensíveis?**
  Para dados sensíveis, além de cumprir os critérios gerais (livre, informado e inequívoco), o consentimento também deve ser específico e destacado.

- **Existem requisitos de consentimento distintos para definir o perfil dos consumidores? Considere: se uma empresa obtém consentimento para usar dados pessoais para fins de "publicidade e marketing", é necessário um consentimento separado (ou mais específico?) para construir um perfil de publicidade para publicidade?**
  A LGPD não fornece regras específicas sobre perfilamento. Conforme mencionado nas respostas acima, a melhor prática é ser mais específico quanto à forma como os dados serão tratados (Artigo 9, II, prevê que a forma da atividade de tratamento deve ser divulgada ao titular de dados), inclusive, no momento, para obter consentimento. No entanto, a prática de mercado tem sido não entrar nessas especificidades, obtendo consentimento "para fins de marketing" sem informar detalhes sobre como isso será realizado no termo/aviso de consentimento.

- **Existem requisitos de consentimento distintos para a tomada de decisão automatizada?**
  Não, não há requisitos de consentimento distintos para a tomada de decisão automatizada na LGPD.

- **Existem restrições de idade relacionadas ao consentimento? Existem requisitos de consentimento distintos em relação ao tratamento de dados pessoais de crianças?**
  Sim. As crianças não podem dar consentimento por conta própria. Para tratar dados relativos a crianças, é necessário levar em consideração o melhor interesse da criança, o qual pode conflitar com o consentimento exigido dos pais. A ANPD vai esclarecer essa questão no futuro. De acordo com a legislação brasileira, indivíduos menores de 12 anos são considerados crianças.

- **O consentimento, embora manifestado, pode ser revogado?**
  Sim, o consentimento pode ser revogado a qualquer momento, mediante pedido expresso do titular de dados através de um processo simples e gratuito, permanecendo válido o tratamento realizado antes da revogação. A LGPD não impõe requisitos adicionais em relação a este direito.

4.5.2. Solicitação para Publicidade Digital

Não há requisitos de consentimento específicos para o ecossistema de publicidade digital.

4.6. Legítimo interesse

O legítimo interesse é a base legal mais flexível para o tratamento de dados pessoais e pode ser utilizada em uma ampla gama de circunstâncias, uma vez que não se limita a uma finalidade específica. O Artigo 7 (IX) da LGPD reconhece que os dados pessoais podem ser tratados:

> *"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"*

Apesar disso, o legítimo interesse não pode ser usado como base legal para o tratamento de dados pessoais sensíveis, ao contrário do consentimento. Isto porque, no tratamento de dados pessoais sensíveis, a LGPD exige a adoção de garantias adicionais às que serão implementadas para o tratamento de dados pessoais em geral.

Dito isso, em consonância com os princípios da LGPD, o artigo 10 da LGPD estabelece as seguintes limitações ao uso de legítimo interesse como base legal para o tratamento de dados pessoais:

> "O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> I - apoio e promoção de atividades do controlador;
>
> e II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
>
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
>
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
>
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de

dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial."

Apesar de sua amplitude conceitual, a LGPD fornece algumas orientações sobre o uso autorizado de legítimo interesse pelos controladores de dados quando os interesses da empresa em relação ao tratamento de dados se baseiam em situações concretas que apoiam as atividades do controlador ou atuam nos melhores interesses dos titulares de dados, desde que (i) os dados tratados sejam reduzidos ao mínimo, (ii) o titular de dados esteja ciente e totalmente informado do tratamento de dados e (iii) o controlador mantenha um registro das atividades de tratamento de dados que se baseiam no legítimo interesse, estabelecendo, para cada atividade de tratamento de dados, os interesses buscados, os impactos previstos e as medidas mitigadoras desses impactos, incluindo a segurança.

Diante disso, os responsáveis pelo tratamento podem basear-se no legítimo interesse para o tratamento de dados pessoais dos consumidores, a fim de promover seus produtos ou serviços, incluindo a prospecção de novos clientes. Dito isso, as empresas ainda devem se certificar de que os dados pessoais tratados sejam reduzidos ao mínimo, que o titular de dados tenha acesso às informações sobre o tratamento de dados (especialmente quando eles não fornecem seus dados diretamente, mas são afetados por publicidade comportamental de terceiros online, por exemplo), que os dados sejam utilizados apenas com o objetivo de apoiar e promover as atividades do controlador e que tais atividades de tratamento de dados sejam devidamente registradas.

4.7. Finalidades Legítimas

- **A lei ou orientação legal exige uma base legal específica para atividades específicas de publicidade digital?**
  Esclareça para cada atividade (sugira o uso de "fins" TCF/IAB CCPA) ("perfil" deve ser abordado aqui).
  Não, a LGPD não estabelece uma base jurídica específica para atividades de publicidade digital.

  A legislação brasileira é omissa em matéria de marketing/publicidade. Os controladores devem utilizar uma base legal válida ao tratar dados para atividades de publicidade digital. De qualquer maneira, devem ser observados os princípios da LGPD, especialmente a transparência e o direito do titular de dados de se opor ao tratamento dos dados quando se utiliza a base jurídica de legítimo interesse.

  O legítimo interesse, de acordo com a LGPD, deve observar todos os seguintes requisitos ao mesmo tempo:
  - A atividade de tratamento deve buscar o estímulo e a promoção das atividades do controlador.
  - A atividade deve proteger o exercício regular dos direitos do titular de dados OU fornecer um serviço que o beneficie.
  - As expectativas legítimas do titular de dados devem ser levadas em consideração, mas não constituem o fator decisivo para a utilização desta base legal.

Não obstante a obrigação geral de observar todos os princípios previstos na lei, a LGPD enfatiza a necessidade de respeitar os princípios de transparência e minimização de dados no tratamento de dados pessoais com base legítimo interesse.

- **Se sim, quais são as bases legais (por exemplo, consentimento, legítimo interesse)? Existem requisitos relacionados à base legal (é necessária uma base legal válida para tratar) / justiça (o escopo do tratamento é legítimo) / transparência (transparência sobre a atividade de tratamento para o consumidor e a base legal)?**
  Apesar da inexistência de base legal específica para as atividades de publicidade digital, normalmente a base legal aplicável é a de consentimento ou de legítimo interesse (desde que não sejam tratados dados sensíveis e atendidas as circunstâncias apresentadas no item 4.6 acima).

- **A lei discorre sobre o tratamento para finalidades secundárias/diferentes das quais o dado pessoal foi coletado?**
  Sim. A LGPD não permite o tratamento de dados para fins não informados ao titular de dados. Quaisquer finalidades secundárias, ou mudanças na finalidade primária, devem ser informadas ao titular de dados (mas não requer consentimento ou aprovação, exceto quando o consentimento for a base legal aplicável).

4.8. Salvaguardas

4.8.1. Visão geral

A LGPD determina a adoção de medidas técnicas e administrativas de segurança para proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilegais de destruição, perda, modificação, comunicação ou qualquer forma de tratamento impróprio ou ilegal.

Além disso, há um incentivo para os agentes de tratamento que implementam regras de boas práticas e governança que estabelecem condições de organização, um regime de tratamento de solicitações relativas às atividades de tratamento de dados incluindo reclamações e solicitações de titulares de dados, normas de segurança, normas técnicas, obrigações específicas para as diversas partes envolvidas no tratamento, atividades educativas, mecanismos internos de supervisão e mitigação de riscos, e outros aspetos relacionados com o tratamento de dados pessoais.

4.8.2. Aplicação à Publicidade Digital

Não há requisitos de proteção específicos relacionados ao setor de publicidade digital.

5. DIREITOS DO TITULAR DE DADOS e EXCEÇÕES

5.1. Visão geral

A LGPD garante ao titular de dados uma série de direitos que devem ser viabilizados pelos agentes de tratamento - controlador e operador. Além disso, os agentes de tratamento são responsáveis por manter os titulares de dados informados sobre seus direitos de forma clara, objetiva e acessível.

Assim, de acordo com a LGPD, o titular de dados pode exercer os seus direitos mediante pedido direto ao responsável pelo tratamento ou ao operador (artigo 18º, n.º 3 da LGPD), ou através do seu representante legalmente constituído. Salienta-se que o pedido do titular de dados, com fundamento no exercício dos direitos previstos na LGPD, deve ser efetuado gratuitamente e nos prazos previstos na LGPD, nos termos do Artigo 18, parágrafo quinto.

Relativamente aos prazos que devem ser observados, a LGPD apenas estabelece o prazo para responder a pedidos de confirmação ou acesso aos dados pessoais. Nestes casos, o agente de tratamento deve fornecer as informações solicitadas pelo titular de dados (i) imediatamente, de forma simplificada; ou (ii) no prazo de 15 (quinze) dias a partir da data da solicitação do titular de dados, por meio de declaração clara e completa que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, sujeito ao sigilo comercial e industrial.

Além disso, caso haja um pedido de correção, exclusão, anonimização ou bloqueio de dados, o controlador deve informar imediatamente os demais agentes de tratamento com os quais os dados foram compartilhados para que possam realizar o mesmo procedimento, exceto em casos em que isto se prove impossível ou envolva esforço desproporcional, nos termos do art. 18, parágrafo sexto, da LGPD.

Portanto, a LGPD estabelece que o titular de dados tem direito de, a qualquer momento e por meio de uma solicitação, obter o seguinte do controlador:

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos ou de dados tratados em desconformidade com a LGPD;
- Portabilidade dos dados para outros prestadores de serviços ou fornecedores de produtos, mediante solicitação expressa do titular de dados, conforme regulamentação da ANPD, observada a proteção de segredos comerciais e industriais no processo;

- Eliminação dos dados pessoais tratados com o consentimento dos titulares de dados, exceto nos casos previstos no artigo 16º da LGPD;
- Informações sobre as entidades públicas e privadas com as quais o controlador compartilhou dados;
- Informações sobre a possibilidade de não fornece consentimento e sobre as consequências dessa recusa;
- Revogação do consentimento, nos termos do disposto no nº 5 do artigo 8º da LGPD;
- Revisão das decisões com base no tratamento de dados pessoais realizado exclusivamente por meios automatizados.

Os direitos de confirmação da existência de tratamento e acesso aos dados podem ser tratados pelo controlador de imediato quando em formato simplificado ou até 15 dias quando em declaração clara e completa.

Para os demais direitos do titular, a ANPD regulamentará o prazo adequado que deve ser observado pelos controladores.

5.2. Acesso

A LGPD fornece o direito de acesso aos dados pessoais de todos os titulares de dados. É obrigação do responsável pelo tratamento fornecer esse acesso a qualquer momento, mediante solicitação feita pelo titular de dados (ou seu representante legal).

Existem dois tipos de pedidos de acesso definidos pela LGPD: em formato simplificado ou em declaração completa. Este último deve indicar a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento (sujeito ao sigilo comercial e industrial). Os pedidos de acesso em formato simplificado devem ser respondidos de imediato, enquanto os pedidos em formato completo devem ser prestados no prazo de 15 dias a contar da data do pedido do titular de dados.

5.3. Correção

A LGPD fornece aos titulares de dados o direito de corrigir quaisquer dados pessoais incompletos, imprecisos ou desatualizados. É obrigação do responsável pelo tratamento providenciar a retificação, a qualquer momento, mediante solicitação do titular de dados (ou de seu representante legal). Além disso, se o controlador tiver compartilhado os dados que receberam uma solicitação de correção (ou para exclusão, anonimização ou bloqueio), o controlador tem a obrigação de informar o agente (outro controlador ou operador) que recebeu os dados, de acordo com o artigo 19 §6º.

5.4. Exclusão

A LGPD concede o direito de exclusão de dados pessoais em duas circunstâncias: (i) quando os dados são desnecessários, excessivos ou tratados em não conformidade com a LGPD; e (ii) quando os dados são tratados com consentimento do titular de dados.

Quando os dados são desnecessários, excessivos ou tratados em não conformidade, o titular de dados pode solicitar exclusão, anonimização ou bloqueio, e o controlador deve avaliar se é o caso para atender à solicitação.

Quando o titular de dados solicita a exclusão de dados pessoais tratados com base no consentimento, há uma exceção: o responsável pelo tratamento pode recusar a exclusão dos dados se eles forem tratados para uma das finalidades estabelecidas no Artigo 16 da LGPD, conforme segue:

"Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados."

Além disso, se o controlador tiver compartilhado os dados que receberam uma solicitação de exclusão (ou para correção, anonimização ou bloqueio), ele tem a obrigação de informar ao agente que recebeu os dados, conforme o artigo 18 §6º.

"O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional."

5.5. Bloqueio

A LGPD concede o direito de restringir o tratamento quando estabelece o direito de solicitar o bloqueio de dados. Este direito está previsto no Artigo 18 - IV, com os mesmos requisitos e garantias que o direito de exclusão, ou seja (i) quando os dados forem desnecessários, excessivos ou tratados em desconformidade com a LGPD; e (ii) quando os dados são tratados com o consentimento do titular de dados.

5.6. Portabilidade de Dados

A LGPD concede aos titulares de dados o direito à portabilidade dos dados para outro fornecedor de serviços ou produtos, mediante pedido expresso. A única exceção ao direito à portabilidade é que ele não inclui dados que já foram anonimizados pelo controlador. A LGPD não estabelece outras orientações para o exercício deste direito. A ANPD regulamentará o direito à portabilidade de dados no futuro.

5.7. Direito de Oposição

Quando os dados são tratados com qualquer base legal diferente do consentimento, o titular de dados tem o direito de se opor ao tratamento se não houver conformidade com as disposições da LGPD. Quando o tratamento é baseado no consentimento, o direito de contestar é substituído pelo direito de revogar o consentimento, independentemente da não conformidade.

5.8. Direito de Revisão de Decisões Automatizadas

A LGPD fornece aos titulares de dados o direito de solicitar revisão das decisões tomadas exclusivamente com base no tratamento automatizado de dados pessoais que afetem seus interesses. A LGPD menciona explicitamente que isso inclui "decisões destinadas a definir seu perfil pessoal, profissional, de consumidor e de crédito, ou aspectos de sua personalidade".

Além disso, a LGPD impõe a seguinte responsabilidade ao controlador:

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Não existe prazo estabelecido pela LGPD para o exercício deste direito.

5.9. Respondendo a Solicitações de Direitos do Consumidor

Não há disposições específicas na LGPD (nem no Código de Defesa do Consumidor) que tratem de como responder às solicitações de direitos do consumidor.

5.10. Manutenção de Registros Relativos a Solicitações de Direitos

Não existem disposições específicas na LGPD no que diz respeito à manutenção de registros relativos a solicitações de titulares, embora, atendendo ao princípio da responsabilização, seja obrigação do agente de tratamento manter provas de que as suas obrigações são cumpridas.

5.11. O Atendimento aos Direitos dos Titulares é Obrigatório ou Facultativo?

Todos os direitos dos titulares de dados são exigidos pela LGPD, não meras sugestões.

5.12. Aplicação à Publicidade Digital e Extensão do Dever de Responder ao Titular de Dados

Conforme explicado no item 5.1 acima, tanto o controlador quanto o operador são obrigados pela LGPD a possibilitar aos titulares de dados o exercício de seus direitos. Nesse sentido, a LGPD prevê

que o titular de dados possa exercer os seus direitos previstos na LGPD mediante solicitação encaminhada ao agente do tratamento; ou seja, a LGPD considera que tanto o controlador quanto o operador são obrigados a responder à solicitação do titular de dados. No entanto, o controlador e o operador estão autorizados a estabelecer entre si por meio de um Termo de Tratamento de Dados ("DPA") de modo que, se um titular de dados apresentar um pedido ao operador relativo a um de seus direitos, o operador notificará imediatamente o controlador e, nesta circunstância, o operador redirecionará a solicitação do titular de dados para o controlador e ajudará o controlador no cumprimento de tal solicitação, adotando as medidas técnicas e organizacionais adequadas.

6. TERMOS DE TRATAMENTO DE DADOS ENTRE CONTROLADORES E OPERADORES

6.1. Visão geral

Não há regras específicas sobre contratos de controlador e operador na LGPD. O único requisito para os operadores é que eles sigam as instruções legais dos controladores. Os controladores são obrigados a verificar se suas instruções estão em conformidade com os regulamentos de proteção de dados.

6.2. Terceirização do Tratamento do Controlador de Dados

A LGPD não estabelece regras sobre terceirização de tratamento, como a exigência de termos escritos. No entanto, as melhores práticas no Brasil incluem ter um acordo por escrito fornecendo certas regras para a terceirização de tratamento, especialmente:

- **Finalidade:** Os termos de tratamento de dados muitas vezes contêm uma cláusula que proíbe o operador de usar os dados pessoais para fins diferentes daqueles estabelecidos pelo controlador e informados aos titulares de dados.
- **Transferência:** Os termos poderão proibir o operador de transferir os dados pessoais a terceiros (exceto em casos de cumprimento de obrigações legais) ou condicionar tais transferências a autorização prévia e por escrito do controlador.
- **Resposta às Solicitações do Titular de Dados:** As partes poderão concordar com as responsabilidades de receber, responder e cumprir as solicitações de direitos do titular de dados. De acordo com a LGPD, o Titular de Dados poderá apresentar um requisito a qualquer agente de tratamento, mas o controlador é o responsável final por cumpri-lo. É comum estabelecer em um Termo de Tratamento de Dados que o operador deve auxiliar o controlador a responder às solicitações de titulares, por exemplo, recebendo demandas, enviando uma confirmação de recebimento e encaminhando a demanda ao controlador.
- **Notificação de incidente:** Os Termos de Tratamento de Dados muitas vezes estabelecem a obrigação do operador de notificar o controlador no caso de quaisquer incidentes envolvendo os dados pessoais. As partes também poderão definir o conteúdo mínimo da notificação, seu cronograma, canal específico de comunicação (ex.: endereço de e-mail do DPO) e obrigação do operador de assistir o controlador com as notificações à ANPD (DPA Brasileira) e Titulares de Dados afetados.
- **Responsabilidade dos agentes:** As partes podem alocar suas responsabilidades em caso de danos causados pelo tratamento de dados - sejam os danos causados aos titulares de dados ou a um dos agentes de tratamento. Esta alocação contratual de responsabilidade é limitada pelas regras de responsabilidade da LGPD. Os contratos muitas vezes reforçam o direito de regresso da parte que paga as indenizações (caso essa parte não seja a única responsável pelos danos), definindo o Termo como um título de execução extrajudicial.
- **Auditorias:** Os Termos de Tratamento de Dados muitas vezes estabelecem o direito do controlador de realizar auditorias no operador, para garantir a conformidade com as normas de

proteção de dados e os detalhes relativos a tais auditorias (por exemplo, um tempo mínimo de aviso prévio ao operador, confidencialidade das auditorias etc.).

6.3. Direitos e Responsabilidades do Operador de Dados

Os operadores são aqueles que tratam os dados pessoais em nome do controlador. Os operadores de dados são responsáveis por seguir as instruções do controlador.

Além disso, os operadores também têm as seguintes responsabilidades:

- Manter um registro das atividades de tratamento de dados;
- Implementar medidas de segurança técnicas e administrativas para proteger os dados pessoais de acesso não autorizado e situações ilegais ou acidentais de destruição, perda, modificação, comunicação ou qualquer outra forma de tratamento inadequado ou ilegal.

Os operadores de dados também são responsáveis por quaisquer danos causados por suas atividades de tratamento de dados quando violarem a LGPD.

6.4. Solicitação para Publicidade Digital

Como a LGPD não estabelece regras específicas em relação ao Termo de Tratamento de Dados, os agentes do setor de publicidade digital têm ampla margem de liberdade contratual para negociar os termos de seu contrato, buscando um equilíbrio entre os interesses dos Anunciantes e dos agentes que normalmente atuam como operadores observando as regras de responsabilidade da LGPD.

7. TRANSFERÊNCIA DE DADOS E TERCEIRIZAÇÃO

7.1. Visão geral

Os titulares de dados têm o direito de acessar, de maneira fácil, as informações a respeito do uso compartilhado dos dados (o que inclui a transferência de dados) pelo controlador, bem como a finalidade do compartilhamento.

A LGPD impõe limitações à transferência de dados pessoais sensíveis. Os dados sensíveis relativos à saúde não podem ser compartilhados entre os controladores com a finalidade de obter benefícios econômicos (exceto nas hipóteses permitidas na LGPD). Além disso, a LGPD prevê que a ANPD poderá impor restrições ao uso compartilhado de quaisquer dados sensíveis entre os controladores, com o objetivo de obter benefícios econômicos.

Sempre que o controlador precisar compartilhar dados pessoais com outros controladores e não tenha informado previamente ao titular de dados que isso poderia acontecer, ele deverá obter o seu consentimento para esse fim específico, exceto quando dispensada a necessidade desse consentimento (ou seja, quando o responsável pelo tratamento precisar compartilhar os dados pessoais para cumprir uma obrigação legal prevista na legislação brasileira). No entanto, qualquer eventual dispensa da exigência de consentimento não isenta os agentes de tratamento das demais obrigações previstas pela LGPD.

7.2. Transferência Internacional de Dados

A LGPD permite a transferência internacional de dados pessoais para países que garantem nível de proteção de dados adequado à lei (conforme estabelecido pela ANPD), ou quando o controlador garante o cumprimento dos princípios e direitos do titular de dados e do regime de proteção de dados previsto na LGPD por meio dos mecanismos de transferência previstos na lei (ou seja, SCC, BCR ou selos, certificados e códigos de conduta). No entanto, a ANPD ainda não regulamentou boa parte destes mecanismos.

A transferência internacional de dados pessoais é permitida apenas nos seguintes casos (sem qualquer ordem de preferência):

- Para países ou organizações internacionais que fornecem um nível adequado de proteção de dados pessoais fornecido pela LGPD;
- Quando o responsável pelo tratamento fornecer e demonstrar garantias de cumprimento dos princípios e direitos do titular de dados e do regime de proteção de dados estabelecido na LGPD, na forma de:
  - cláusulas contratuais específicas para uma determinada transferência.
  - Cláusulas contratuais padrão.
  - Regras Corporativas Globais.

- Selos, certificados e códigos de conduta emitidos regularmente;
- Quando a transferência for necessária para a cooperação jurídica internacional entre inteligência governamental, investigações e órgãos policiais, de acordo com os instrumentos do direito internacional;
- Quando a transferência for necessária para a proteção da vida ou integridade física do titular de dados ou de terceiros;
- Quando a ANPD autorizar tal transferência;
- Quando a transferência resultar em um compromisso assumido no âmbito de um acordo de cooperação internacional;
- Quando a transferência for necessária para a aplicação de uma política pública ou atribuição legal da utilidade pública, mediante divulgação do disposto no inciso I do caput do artigo 23 da LGPD;
- Quando o titular de dados tenha dado consentimento específico e destacado para tal transferência, com informação prévia sobre o caráter internacional da operação, distinguindo-a claramente de quaisquer outras finalidades;
- Quando necessário para atender às hipóteses estabelecidas nos incisos II, V e VI do artigo 7º da LGPD.

Não há requisitos específicos para terceirização. Se envolver transferência internacional, deve-se seguir os requisitos supracitados.

7.3. Aplicação à Publicidade Digital

Não há restrições específicas quanto à transferência de dados para atividades de publicidade digital, uma vez que as únicas restrições impostas pela LGPD à transferência internacional de dados são as apontadas no item 7.2 acima. Assim, se o controlador se utilizar de um destes mecanismos, a transferência internacional será lícita. Obter consentimento específico e destacado do titular de dados, portanto, é apenas uma hipótese sob a qual a transferência internacional de dados será permitida (conforme artigo 33, VIII, da LGPD), mas não é, *per se*, um requisito para a operação em questão.

Em relação à transferência internacional de dados realizada sob consentimento, note que a LGPD não indica claramente a forma como deve ser obtida. Por exemplo, não está claro na legislação se o mesmo meio de obtenção de consentimento geral (ou seja, uma caixa de seleção vinculada à política de privacidade) pode ser usado para obter consentimento para transferências internacionais - desde que seja claro e distinto - ou se seria necessário obter consentimento por um meio diferente (ou seja, uma segunda caixa de seleção exclusivamente para esse fim) a fim de configurar uma aceitação específica. No entanto, é o que acontece quando o consentimento é necessário para a transferência internacional de dados, nos termos do artigo 33º da LGPD.

Por outro lado, se o consentimento foi a base legal original adotada pelo agente de tratamento para coletar os dados pessoais em primeiro lugar, e nesse momento o controlador não informou o titular de dados sobre a possibilidade de seus dados serem compartilhados para fora do Brasil, o controlador deverá notificar o titular de dados e obter novo consentimento. Note-se que a necessidade de obter

consentimento neste caso decorre do fato de que a finalidade original do tratamento foi alterada e, portanto, uma vez que o consentimento foi a base legal original adotada, a LGPD determina que o controlador precisa obter novo consentimento que englobe a nova finalidade (conforme art. 8º, § 6º, e art. 9º, I, da LGPD). Nesse sentido, o consentimento aqui não é um requisito para a transferência internacional em si, mas sim para a legalidade do consentimento fornecido pelo titular de dados.

Finalmente, é importante apontar que o consentimento é raramente usado como mecanismo de transferência internacional, justamente por ser pouco prática a sua implementação. Se o titular de dados retirar seu consentimento, as empresas precisam hospedar seus dados pessoais dentro do Brasil e deixar de compartilhá-los com terceiros fora do país.

8. AUDITORIA/RESPONSABILIDADE

8.1. Visão geral

Veja abaixo.

8.2. Aplicação à Publicidade Digital

- **Auditoria - Quais direitos de auditoria são ditados por lei? (Por exemplo, as empresas devem ter direitos de auditoria sobre seus fornecedores? A classificação desses fornecedores é importante?)**

  A LGPD não estabelece direitos de auditoria, exceto que as auditorias poderão ser realizadas pela ANPD.

- **Responsabilidade - as empresas/fornecedores devem manter certos registros para provar que atenderam a determinados requisitos? Quais são esses requisitos?**

  A lei exige o cumprimento do princípio da responsabilidade e prestação de contas, que exige a "demonstração, pelo agente de tratamento de dados, da adoção de medidas eficazes e capazes de comprovar o cumprimento das regras de proteção de dados pessoais, incluindo a eficácia de tais medidas."

  Destacadamente, os controladores e operadores são obrigados a manter registros das operações de tratamento de dados pessoais que realizam, "especialmente quando com base em legítimo interesse". O ônus da prova também recai sobre o controlador para demonstrar que o consentimento foi devidamente obtido em conformidade com as disposições da LGPD.

9. RETENÇÃO DE DADOS

9.1. Visão geral

A regra geral da LGPD para retenção de dados é que todos os dados devem ser excluídos quando o tratamento termina. De acordo com o Artigo 15, o término do tratamento deve ocorrer quando:

- A finalidade foi alcançada ou os dados não são mais necessários para atingir a finalidade;
- O período de tratamento termina;
- Existe comunicação do titular de dados, inclusive no exercício do direito de revogação do consentimento, levando em consideração o interesse público;
- A ANPD solicitar a exclusão por constatar que a LGPD foi violada.

A retenção de dados é autorizada, mesmo após o término do tratamento, nos seguintes casos (de acordo com o artigo 16):

- Cumprimento de uma obrigação legal ou regulatória por parte do controlador;
- Estudo por órgão de pesquisa (garantindo, sempre que possível, a anonimização dos dados pessoais);
- Transferência a terceiros, desde que sejam obedecidos os requisitos da LGPD para tratamento de dados;
- Uso exclusivo do controlador, sendo o acesso de terceiros proibido e desde que os dados estejam anonimizados.

9.2. Aplicação à Publicidade Digital

Não existem regras específicas de retenção de dados para o setor de publicidade digital.

10. AUTORIDADE DE PROTEÇÃO DE DADOS | AUTORIDADE REGULADORA

10.1. Visão geral

O órgão regulador responsável pela aplicação das regras de proteção de dados no Brasil é a ANPD - Autoridade Nacional de Proteção de Dados. Apesar dos vetos que sofreu o projeto original em 2018, que impactaram fortemente a criação da ANPD; em julho de 2019, com a sanção da Medida Provisória (MP) 869/2018 e sua consequente conversão em lei (Lei nº 13.853/2019), a criação da ANPD e do Conselho Nacional de Proteção e Privacidade de Dados foi finalmente promulgada. A ANPD foi criada como entidade integrante da administração pública federal, pertencente à Presidência da República, nos termos do artigo 55-A da LGPD.

Além disso, a referida Lei atribuiu uma natureza jurídica transitória à ANPD, podendo, no prazo de 2 (dois) anos, ser transformada pelo Poder Executivo em entidade da Administração Pública Federal Indireta, sujeita a regime autárquico especial e pertencente à Presidência da República, conforme art. 55-A, §1º, da LGPD.

A referida possibilidade de mudança na natureza da ANPD é benéfica às empresas que transferem dados à União Europeia, uma vez que o GDPR exige a independência das autoridades de supervisão em relação ao seu governo como um dos requisitos para considerar um país como tendo um nível de proteção adequado. Ser percebido como um país com um nível de proteção adequado na lista da Comissão Europeia facilita a interação no cenário de transferência internacional de dados com a UE, sem quaisquer eventuais procedimentos burocráticos envolvidos em outra base jurídica fornecida pelo GDPR.

Além disso, o Governo Federal publicou, em 27 de agosto, o Decreto nº 10.474/2020, definindo a estrutura da ANPD como órgão da Presidência da República.

10.2. Regulador Principal para Proteção de Dados

A Autoridade Nacional De Proteção de Dados (“ANPD”) é o principal órgão regulador. A ANPD é um órgão da administração pública federal, parte da Presidência da República, e é composta por:

- Conselho Diretor, como órgão máximo de direção;
- Conselho Nacional de Proteção e Privacidade de Dados Pessoais;
- Gabinete de Assuntos Internos;
- Ouvidoria;
- Órgão Consultivo Jurídico;
- Outras unidades administrativas e especializadas necessárias para a aplicação da LGPD.

O Conselho Diretor da ANPD é composto por cinco conselheiros, incluindo o diretor presidente, todos indicados pelo Presidente da República, de acordo com os requisitos: brasileiros, de reputação ilibada, alto nível de escolaridade, e uma grande reputação na área de especialização do cargo para o qual foram indicados.

10.3. Principais Poderes, Deveres e Responsabilidades

A ANPD é responsável pela aplicação da LGPD e tem os seguintes poderes disponíveis para garantir a proteção dos dados das pessoas físicas:

- Supervisionar a proteção dos dados pessoais, inclusive por meio da realização de inspeções, ou da determinação de sua ocorrência;
- Ponderar sobre como os segredos comerciais devem ser protegidos no contexto do tratamento de dados pessoais e transparência;
- Desenvolver diretrizes para proteção de dados pessoais e uma política nacional de privacidade;
- Receber e tratar reclamações de titulares de dados contra os controladores (depois de submetidas ao controlador e não solucionadas de acordo com a LGPD);
- Decidir como os agentes de tratamento de dados devem ser transparentes em relação às atividades de tratamento de dados pessoais;
- Solicitar às entidades públicas que desenvolvem atividades de tratamento de dados pessoais informações sobre o âmbito e natureza dos dados e demais pormenores do tratamento, podendo ser emitidos pareceres técnicos para garantir o cumprimento da LGPD;
- Alterar os regulamentos e procedimentos de privacidade e proteção de dados pessoais, incluindo relatórios de impacto à proteção de dados (“DPIAs”);
- Ouvir os agentes de tratamento de dados e a sociedade em assuntos de interesse relevante;
- Gerir seus fundos e publicar um relatório detalhado sobre suas despesas;
- Realizar convênios com agentes de tratamento de dados para eliminar irregularidades, incertezas jurídicas ou situações contenciosas em processos administrativos;
- Promulgar regras, diretrizes e procedimentos simplificados, inclusive em relação a prazos, para pequenas e microempresas, startups e negócios inovadores, a fim de ajudá-los a cumprir a LGPD;
- Assegurar que as atividades de tratamento de dados pessoais de pessoas idosas sejam realizadas de forma simples, clara, acessível e adequada à sua compreensão;
- Decidir sobre a interpretação da LGPD na esfera administrativa nos casos em que a lei é omissa
- Implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de

reclamações sobre atividades de tratamento de dados pessoais que não estejam em conformidade com a LGPD;

- Fiscalizar e sancionar casos de atividades de tratamento de dados em desacordo com a LGPD, por meio de processos administrativos que garantam o direito ao contraditório, a ampla defesa e o direito de recurso;
- Denunciar às autoridades competentes as infrações penais de que tenham conhecimento;
- Reportar à corregedoria qualquer não conformidade com a LGPD por parte de órgãos e entidades da administração pública federal;
- Disseminar conhecimento ao povo brasileiro sobre as normas legais e políticas em torno da proteção de dados pessoais e suas medidas de segurança;
- Estimular a adoção de normas de serviços e produtos que facilitem o controle e a proteção de dados pessoais por parte de seus titulares, considerando as especificidades das atividades e o porte dos controladores;
- Elaborar estudos sobre práticas nacionais e internacionais de proteção e privacidade de dados pessoais;
- Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de caráter internacional ou transnacional;
- Elaborar relatórios de gerenciamento sobre as atividades anuais.

10.4. Aplicação à Publicidade Digital

A ANPD ainda não forneceu nenhuma orientação ou pronunciamento sobre a indústria de publicidade digital.

O calendário regulamentar da Agência para 2021/2022 não prevê regulamentação específica para este setor.

11. SANÇÕES

11.1. Visão geral

A LGPD prevê um sistema escalonado de penalidades, começando com um aviso e terminando com uma multa. Nesse sentido, o descumprimento da LGPD pelos agentes de tratamento de dados pode resultar em diversas penalidades, conforme artigo 52 da LGPD, entre elas: advertências; publicização da violação; bloqueio ou exclusão dos dados pessoais aos quais se refere a violação; multas diárias, ou multas simples de até 2% (dois por cento) sobre as vendas do grupo empresarial no Brasil - limitadas a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; suspensão parcial do funcionamento da base de dados por seis meses; suspensão do exercício da atividade de tratamento de dados pessoais por até seis meses; e proibição parcial ou total do exercício das atividades de tratamento de dados.

11.2. Responsabilidade

Independentemente do setor ou do tipo de tratamento realizado, a LGPD estabelece que os agentes de tratamento (controlador e operador) são obrigados a reparar os danos causados em decorrência do exercício da sua atividade de tratamento de dados pessoais, que violação a LGPD.

A alocação da responsabilidade entre os agentes de tratamento é estabelecida no artigo 42, da seguinte forma:

> *"§ 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.*
> *[...]*
> *§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso."*

As exceções à responsabilização estão no Artigo 43:

> *"Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:*
> *I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;*
> *II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou*
> *III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."*

- **Escopo de responsabilidade de publishers e anunciantes em relação a atividades de tratamento de adtechs.**

O controlador ou o operador que, como resultado do exercício da sua atividade de tratamento de dados pessoais, causar danos materiais, morais, individuais ou coletivos a outrem, em violação da legislação de proteção de dados pessoais, está obrigado a repará-lo, nos termos ao Artigo 42 da LGPD.

Para esse fim, os operadores serão solidariamente responsáveis pelos danos causados pelas atividades de tratamento, caso não sigam as instruções legais do controlador. O mesmo se aplica aos controladores que estiveram diretamente envolvidos no tratamento que resultou em danos ao titular de dados. Esta regra não se aplicará nos casos previstos no artigo 43 da LGPD acima apresentados.

Além disso, deve ser destacado que quem paga uma indenização por danos ao titular de dados tem o direito de exigir uma indenização das outras partes responsáveis na medida da sua participação no evento prejudicial.

Por exemplo: uma atividade de tratamento de dados realizada por uma determinada empresa deu origem a danos materiais ao titular de dados, cujos dados pessoais foram vazados. O controlador, no referido caso, realizou o pagamento da indenização ao titular de dados. Porém, o operador foi, de fato, aquele que deu origem ao dano. Nessa hipótese, o controlador tem o direito de exigir uma indenização do operador.

Além disso, o controlador e/ou o operador estarão sujeitos às sanções previstas na LGPD, caso o tratamento de dados pessoais não esteja em conformidade com a LGPD ou se o agente de tratamento envolvido - o controlador ou o operador - não fornecer a segurança que o titular de dados pode esperar, tendo, levando em consideração circunstâncias relevantes do tratamento (artigo 44º da LGPD), que pode incluir (a) a forma como o tratamento foi realizado; (b) o resultado e os riscos que se pode esperar dele; e (c) as técnicas de tratamento de dados pessoais disponíveis no momento em que foram realizados.

- **Escopo de responsabilidade de adtechs em relação a atividades de coleta de publishers e anunciantes.**

  Mesmos que acima.

- **Escopo de responsabilidade de adtechs em relação a outras adtechs envolvidas no processo.**

  Mesmos que acima.

11.3. Aplicação e Prática de Mercado

- **Como as alegações são realizadas de acordo com a lei?**
  As alegações referentes às violações da LGPD podem ser formuladas pela ANPD ou por qualquer titular de dados. Assim, embora a ANPD seja a autoridade competente para aplicar as sanções, o judiciário e outras entidades também podem aplicar sanções relativas a danos ou ao descumprimento da LGPD.

- **Quem os aplica?**
  A principal competência para aplicar as sanções da LGPD é da ANPD. Portanto, outras entidades (como procuradores-gerais, órgãos de defesa do consumidor etc.) poderiam usar a LGPD como fundamento para promover ações civis públicas e investigações. Há um precedente relacionado a esse tipo de ação específica para atividades de publicidade: https://www.zdnet.com/article/sao-paulo-subway-facial-recognition-system-slammed-over-user-data-security-and-privacy/

- **Qual é a prática destes órgãos (trabalhar discretamente com empresas para consertar; divulgar publicamente grandes investigações? Varia caso a caso?)**
  Ainda é difícil definir como a ANPD se comportará em relação às sanções administrativas, uma vez que as sanções ainda não são aplicáveis.

- **Que orientação foi dada até o momento sobre como lidar com particularidades do ecossistema de anúncios? Os reguladores foram informados sobre como o ecossistema opera? Os regimes de conformidade foram discutidos com eles? O feedback deles foi solicitado?**
  Não temos até o momento uma orientação oficial sobre como lidar com particularidades do ecossistema de anúncios. Não temos conhecimento de nenhum feedback solicitado pela ANPD para esse setor e o currículo de seus diretores indica que nenhum deles tem experiência no ecossistema de anúncios.

11.4. Sanções

Existe uma ampla gama de sanções que podem ser aplicadas quando uma organização viola a LGPD:

- Aviso, com indicação do prazo para adoção de medidas corretivas;
- Multa simples de até 2% (dois por cento) do faturamento de pessoa jurídica privada, grupo ou conglomerado no Brasil, pelo exercício anterior, excluindo impostos, até o valor total máximo de R$ 50.000.000,00 (cinquenta milhões de reais) por violação;
- Multa diária, observado o total máximo referido no item II;
- Divulgação da violação imediatamente após a sua ocorrência, uma vez que esta tenha sido devidamente apurada e confirmada;

- Bloqueio dos dados pessoais aos quais se refere a infração até a sua regularização.
- Eliminação dos dados pessoais aos quais se refere a infração;
- Suspensão parcial do funcionamento do banco de dados relacionado à violação por um período máximo de 6 (seis) meses, prorrogáveis por igual período, até à normalização da atividade de tratamento pelo controlador;
- Suspensão da atividade de tratamento de dados pessoais relacionada à infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
- Proibição parcial ou total das atividades relacionadas ao tratamento de dados.

Essas sanções entraram em vigor em 1º de agosto de 2021.

11.5. Direito de Petição

Os titulares de dados podem peticionar contra agentes de tratamento por conta da LGPD, por meio de ações em tribunais cíveis ou em processos administrativos perante a ANPD. Isso é estabelecido nos artigos 18 e 22, respectivamente:

> *"Art. 18 §1° O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional."*

> *"Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva."*

11.6. Problemas de Responsabilidade relativos à Publicidade Digital

Os problemas de responsabilidade que podem preocupar especialmente os agentes de publicidade digital são aqueles relacionados à responsabilidade do controlador pelas ações do operador (exceto quando o operador sozinho viola a lei e/ou as instruções do controlador).

É obrigação do controlador definir a base legal e a finalidade da atividade de tratamento. Portanto, questões relacionadas ao consentimento e legítimo interesse (por exemplo, ao usar cookies) precisam ser avaliadas cuidadosamente pelo controlador antes de compartilhar dados pessoais com um operador.

11.7. Aplicação à Publicidade Digital

Não existem regras específicas de responsabilidade ou sanção para o setor de publicidade digital. Os agentes deste setor estão sujeitos às regras gerais descritas acima e devem estar atentos a problemas específicos envolvidos em suas atividades, a fim de evitar sanções.

12. NOTIFICAÇÃO | CERTIFICAÇÃO | REGISTRO

12.1. Requisitos e Breve Descrição

A notificação ou registro de bancos de dados na ANPD não é exigida pela LGPD. Apenas a notificação de violação de dados é obrigatória.

13. ENCARREGADO DE DADOS

13.1. Visão geral

O Encarregado de Dados ("DPO") é a pessoa nomeada pelo controlador e operador para atuar como um canal de comunicação entre o controlador, o titular dos dados e a ANPD. Assim, a LGPD estabelece a obrigação do controlador para nomear um DPO, mas ainda não há quaisquer exceções a esta obrigação ou mesmo critérios específicos em relação às suas condições de elegibilidade e responsabilidade.

13.2. *DPO* - Nomeação Compulsória (Sim/Não)

Um DPO deve ser nomeado pelos controladores.

A ANPD pode dispensar os controladores de nomear um DPO de acordo com a natureza e o porte do agente ou o volume das operações de tratamento de dados. De acordo com o cronograma regulatório recentemente publicado pela ANPD, as regras complementares e isenções relativas aos DPOs serão abordadas pela Autoridade, por meio de Resolução, no primeiro semestre de 2022.

13.3. Requisitos

A identidade e os dados de contato do DPO devem ser divulgados de forma pública, clara e objetiva, preferencialmente no website dos controladores.

As atividades do DPO consistem no seguinte:

- Aceitar reclamações e comunicações dos titulares de dados, prestar esclarecimentos e tomar medidas;
- Receber comunicações da autoridade supervisora e tomar medidas;
- Orientar os colaboradores do agente sobre as práticas a serem adotadas em relação à proteção de dados pessoais;
- Desempenhar as demais atribuições estabelecidas pelo controlador ou em normas complementares.

A ANPD poderá estabelecer regras complementares sobre a definição e atribuições do DPO.

Apesar de não haver exigência de localização específica na LGPD, é recomendável que o DPO esteja localizado no Brasil; se, por outro lado, o DPO indicado não estiver no Brasil, é importante que ele possa se comunicar com a ANPD e com os titulares de dados em português, e esteja disponível para estar no Brasil quando necessário.

13.4. Aplicação à Publicidade Digital

Não existem regras específicas sobre o DPO para organizações de publicidade digital. Até nova comunicação da ANPD, todas as organizações de publicidade digital devem seguir as normas gerais e designar um DPO.

14. AUTORREGULAÇÃO

14.1. Visão geral

Não há iniciativas de autorregulação em vigor no Brasil com relação à proteção de dados no ecossistema online. No entanto, é possível adotar estes mecanismos, uma vez que a LGPD incentiva modelos de governança autorreguladora.

- **Há algum esquema de autorregulação do setor em vigor na jurisdição?**
  Ainda não, mas a LGPD permite a implementação de modelos de autorregulação e códigos de conduta para organizações, setores econômicos etc.

- **Há algum programa baseado em sinal usado no território para auxiliar na conformidade da publicidade digital?**
  Não. No entanto, seria possível aplicar tais programas baseados em sinais, uma vez que a LGPD incentiva a adoção de melhores práticas e regras de conformidade por associações autorreguladoras, especialmente para abordar:
- Condições de organização;
- Um regime de operação;
- Procedimentos, incluindo reclamações e petições de titulares de dados;
- Normas de segurança;
- Normas técnicas;
- Obrigações específicas para as várias partes envolvidas no tratamento;
- Atividades educativas;
- Mecanismos internos de supervisão e mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Portanto, um programa semelhante, por exemplo, as *Políticas da Estrutura de Transparência e Consentimento da Europa* do IAB poderia ser aplicável no Brasil. (Observe que a aplicabilidade se refere às características autorreguladoras e baseadas em sinal da Estrutura, **e não ao seu conteúdo**, uma vez que a LGPD difere da Diretiva Europeia de Privacidade Eletrônica).

14.2. Aplicação à Publicidade Digital

Embora não existam precedentes de esquemas de autorregulação e programas baseados em sinais para proteção de dados no Brasil, o setor de publicidade digital parece ser um bom campo de aplicação para essas iniciativas, uma vez que o setor precisa adaptar práticas e tecnologias para cumprir a LGPD.

15. PROJETOS DE LEI DE PRIVACIDADE PENDENTES

15.1. Visão geral

Atualmente no Congresso brasileiro existem poucos projetos de lei de privacidade pendentes, entre os quais o único que merece destaque é o Anteprojeto de Lei que visa regulamentar o tratamento de dados pessoais no contexto de investigações criminais. A Minuta Preliminar da chamada "LGPD Penal" foi apresentada pela Comissão Técnica, criada pelo Congresso em 5 de novembro de 2020, e pretende regulamentar o tratamento de dados pessoais nas áreas de segurança pública, investigações criminais e o processo penal. O projeto de lei é muito inspirado na Diretiva 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Há grandes chances de o projeto ser sancionado.

Além disso, vale citar o Projeto de Emenda Constitucional nº 17/2019, em tramitação na Câmara dos Deputados, que busca incluir a proteção de dados pessoais entre os direitos e garantias fundamentais previstos na Constituição Federal e estabelecer a competência privada da União para legislar sobre a proteção e o tratamento dos dados pessoais.

15.2. Aplicação à Publicidade Digital

Não há projetos de lei relativos a privacidade e o setor de publicidade digital.