

GUIA DE PROTEÇÃO DE DADOS PESSOAIS

MARKETING

CC.04.003.2023

OUTUBRO, 2023

FICHA TÉCNICA

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: MARKETING VERSÃO 2.0 – OUTUBRO, 2023.

Diretoria de Controles Internos – DCI

Maria Alice da Justa Lemos
Diretora de Controles Internos

Analista responsável por este Guia:

Alessandra Rigueti Barcellos

Jordan Vinícius de Oliveira

Encarregado de Proteção de Dados Pessoais

Equipe Extracontratual:

Laila Sá Ferreira

Taís Povill Rocha

Alessandra Rigueti Barcellos

Nadja Nayra da Cruz Ferreira Ribeiro

Pesquisador responsável pela [versão 1.0](#) do Guia:

Jordan Vinícius de Oliveira

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

AVISO LEGAL

Este Guia foi atualizado pela Equipe do Encarregado de Proteção de Dados Pessoais da Fundação Getúlio Vargas – FGV a partir do documento original, publicado em outubro de 2020 pela Equipe do Centro de Ensino e Pesquisa em Inovação – CEPI, da FGV Direito SP. É possível que constem trechos da obra original neste Guia, uma vez que o intuito da modificação é manter as diretrizes atualizadas de acordo com os novos posicionamentos em matéria de proteção de dados pessoais no âmbito nacional e internacional.

Os créditos autorais deste Guia seguem ao autor original – Jordan Vinícius de Oliveira. Este autor também participou do processo de revisão e atualização desta versão, a qual, por sua vez, está credenciada, ainda, à autora Alessandra Rigueti Barcellos.

O presente documento possui intuito meramente informativo, não sendo utilizado para fins de exploração comercial e apresenta a devida referência na página 2. Do mesmo modo, este documento não deve ser considerado como aconselhamento jurídico e não substitui a avaliação de uma equipe profissional de proteção de dados para cada caso.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

SUMÁRIO

1. CONTEXTUALIZAÇÃO	5
2. DADOS PESSOAIS E ATIVIDADES DE <i>MARKETING</i>: ASPECTOS INICIAIS	6
3. LGPD E <i>MARKETING</i>: PRINCIPAIS BASES LEGAIS	11
3.1 A BASE LEGAL DO INTERESSE LEGÍTIMO	12
3.2 A BASE LEGAL DO CONSENTIMENTO.....	15
4. PROTEÇÃO DE DADOS PESSOAIS EM ATIVIDADES DE <i>MARKETING</i>.....	18
4.1 COLETA DE <i>LEADS</i>	19
4.2 LISTA DE CONTATOS PARA <i>MARKETING</i>: POSSO COMPRAR? PRECISO DE CONSENTIMENTO PARA AS QUE JÁ POSSUO?.....	20
4.3 USO DE FERRAMENTAS E NOVAS TECNOLOGIAS DE PUBLICIDADE.....	23
4.4 TRATAMENTOS AUTOMATIZADOS: QUANDO OS USOS DE <i>PROFILING</i> E <i>CHATBOTS</i> REQUEREM CUIDADOS ADICIONAIS?	27
4.5 TÉCNICAS DE <i>BUSINESS INTELLIGENCE</i> (BI) E LGPD	31
4.6 <i>TELEMARKETING</i>: ENTRE A LGPD E REGULACOES ESTATAIS AUTONOMAS	33
4.7 USO DE IMAGEM, ÁUDIO E VÍDEO: CAMPANHAS, DIVULGAÇÕES E REDES SOCIAIS	35
4.8 <i>MARKETING</i> E TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES	37
5. CONSIDERAÇÕES FINAIS	38
APÊNDICE 1: MODELO DE TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM E VÍDEO – ADAPTADO À LGPD E COM COMENTÁRIOS.....	41
APÊNDICE 2: DIRETRIZES PARA FORMULÁRIOS DE INSCRIÇÃO EM EVENTOS, CURSOS E SIMILARES	43
ANEXO ÚNICO – PERGUNTAS PARA A FERRAMENTA DE AVALIAÇÃO DO INTERESSE LEGÍTIMO (LIA).....	45

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

1. CONTEXTUALIZAÇÃO

O presente Guia foi desenvolvido no âmbito do projeto de adequação da Fundação Getúlio Vargas – FGV às leis setoriais de proteção de dados pessoais, especialmente a Lei Geral de Proteção de Dados ("LGPD"), aprovada em agosto de 2018.

A LGPD é aplicável a qualquer operação de tratamento de dados pessoais, seja ela realizada por pessoa natural, pessoa jurídica de direito privado ou pessoa jurídica de direito público. Na condição de Instituição Educacional, a FGV desenvolve, entre outras atividades, operações de caráter administrativo, acadêmico e educacional (como por exemplo, a necessidade de guarda permanente de históricos escolares, provas, realização de pesquisas, desenvolvimento de projetos etc.). Nesse sentido, a FGV deverá observar as obrigações normativas específicas das entidades públicas reguladoras, como, por exemplo, o Ministério da Educação ("MEC") e a Autoridade Nacional de Proteção de Dados ("ANPD").

Assim, a FGV desenvolveu, em maio de 2019, um projeto para cumprir com os objetivos de sua conformidade regulatória ante as leis de proteção de dados, denominado Projeto Presidência – Implantação do Programa de Conformidade: Leis de Proteção de Dados Pessoais ("**Projeto**"). Esta iniciativa, entre outras atividades, buscou parametrizar ações de conformidade da FGV ao novo contexto regulatório de proteção de dados, bem como, a partir das lições aprendidas, fornecer subsídios e materiais de apoio, especialmente ao setor educacional.

Após a conclusão do **Projeto** inicial, a FGV criou a Equipe do Encarregado de Proteção de Dados Pessoais, no âmbito de sua Diretoria de Controles Internos ("DCI"). Esta Equipe tem como finalidade principal manter o programa de adequação da FGV às normas de proteção de dados aplicáveis às suas atividades, bem como funcionar como interlocutora junto aos variados setores da instituição, à ANPD, aos titulares de dados pessoais e aos demais agentes de tratamento.

Este Guia se destina a orientar, de modo geral, práticas comunicacionais que tenham por escopo: a coleta ou qualquer forma de tratamento de dados para os fins de promoções e comunicações relacionadas a produtos, serviços, eventos, cursos, concursos, avaliações e exames de qualquer natureza, dentre outros.

Não obstante outros objetivos, este Guia busca, ainda:

(a) trazer reflexões sobre práticas de *marketing* a fim de que estejam em conformidade com os direitos à privacidade e à proteção dos dados pessoais;

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

- (b) apresentar parâmetros de conformidade em serviços ou produtos que tratem dados pessoais e lidem com dados de públicos-alvo de interesse (*suspects, prospects, leads e customers*¹); e
- (c) relacionar as leis de proteção de dados pessoais aos bons padrões de condutas para a gerência e o disparo de mensagens no setor de *marketing*.

Este Guia está distribuído em quatro eixos centrais: inicialmente serão abordados aspectos iniciais das atividades de *marketing* e a relação com dados pessoais ([Capítulo 2](#)). Após essa introdução, serão trabalhadas as principais bases legais aplicáveis às atividades de *marketing* ([Capítulo 3](#)) e, ainda, apresentadas atividades de *marketing* recorrentes especialmente ao contexto de Instituições de Ensino e sua relação com o direito à proteção de dados pessoais ([Capítulo 4](#)). Boa Leitura!

2. DADOS PESSOAIS E ATIVIDADES DE MARKETING: ASPECTOS INICIAIS

Definido pela Associação Americana de Marketing (“AMA”)² como uma atividade que reúne “instituições e processos para criar, comunicar, entregar e trocar ofertas as quais possuam valor para consumidores, clientes, parceiros e a sociedade em geral”, o *marketing* é primordial na comunicação de instituições para com a sociedade da informação. Neste capítulo serão abordados alguns aspectos introdutórios sobre o tratamento de dados pessoais nas atividades de *marketing*.

A relação entre *marketing* e dados pessoais se estreitou na medida em que novas tecnologias e dispositivos conectados à internet foram inseridos no cotidiano de consumidores e de organizações. Atualmente o dado pessoal é um importante elemento capaz de personalizar uma relação e

¹ Em estratégias de *marketing*, *suspect* é qualquer indivíduo em geral que tenha ou possa ter interesse por um determinado segmento ou nicho de produtos ou serviços e que, após uma análise mais apurada, pode vir a ser classificado como *prospect* de uma marca em específico. Equivalente à primeira de quatro etapas do afunilamento na relação com um potencial cliente. O *prospect* é o *suspect* que passou por um filtro básico de compatibilidade de interesses com a marca, produto ou serviço em específico e que, após uma análise mais apurada, pode vir a ser abordado como *lead*. Equivalente à segunda de quatro etapas do afunilamento na relação com um potencial cliente. O *lead* é o *prospect* analisado e recomendado a uma abordagem mais refinada para os fins de promoção de produtos, serviços ou marcas e com razoáveis chances de se tornar um consumidor final ou *customer*. Equivalente à terceira de quatro etapas do afunilamento na relação com um potencial cliente. São pessoas ou empresas que demonstram interesse no produto ofertado. O *customer*, é o *lead* convertido com sucesso em novo consumidor. Equivalente à quarta e última etapa do afunilamento na relação com um potencial cliente. Para os fins deste Guia, as definições de *suspects, prospect, lead e customer* foram feitas conforme: D’HAEN, Jeroen; POEL, Dirk Van den. Model-supported business-to-business prospect prediction based on an iterative customer acquisition framework. Universiteit Gent Working Paper 2013/863, 2013. Disponível em: <[link](#)>. Acesso em: 25 jan. 2020.

² AMA. *Definitions of Marketing* (tradução livre). American Marketing Association, 2017. Disponível em: <[link](#)> Acesso em: 27 jan. 2020.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

desenvolver vínculos mais precisos de consumo e de divulgação de uma marca, produtos e serviços.

Antes de mais nada, quando se define a aplicação da LGPD a partir da conceituação de dado pessoal, é imprescindível diferenciar informações de pessoas jurídicas e informações de pessoas naturais. Assim, dados estritamente relativos a pessoas jurídicas, como um registro contábil, estão fora do escopo da legislação, a não ser que englobem indicativos sobre pessoas naturais.

A fim de entender a aplicabilidade da LGPD sobre as atividades de *marketing*, a presente seção foi organizada para, primeiramente, responder a cinco questões introdutórias ao tema: **(i)** qual a diferença entre dado pessoal e dado pessoal sensível? **(ii)** O que é titular de dados? **(iii)** O que são os agentes de tratamento, controlador e operador? **(iv)** O que é uma operação de tratamento de dados? **(v)** Como determinar o que é ou não dado pessoal no contexto de relações corporativas (ou *business to business*, B2B³) versus relações consumeristas (ou *business to consumers*, B2C⁴)?

Sobre a primeira pergunta, como já abordado, em tempos de *internet*, dispositivos móveis e de comunicações cada vez mais personalizadas, as atividades de *marketing* dependem, em boa medida, da capacidade de obtenção e análise de dados pessoais. Mas, o que seriam dados pessoais na terminologia da lei?

A LGPD, ao definir o dado pessoal, o conceituou como aquele capaz de tornar uma pessoa identificada ou identificável. Apesar de um conceito aparentemente simples, é preciso cautela quando abordamos dados gerados no ambiente *online*. Dados de geolocalização, dados dos dispositivos de seus usuários, e “identificadores *online*” também são considerados dados pessoais, na medida em que são capazes de identificá-los, ainda que não revelem diretamente o seu nome.

Vale mencionar, que antes mesmo da LGPD ser sancionada, o Decreto 8.771/2016, em seu artigo 14, inciso I definiu dado pessoal como “dado relacionado à pessoa natural identificada ou identificável, **inclusive números identificativos, dados locais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa**” (grifado)⁵.

Em atividades de *marketing online*, por exemplo, é de fundamental importância entender o que é um dado capaz de tornar uma pessoa identificável/identificada e, ainda, o que é um dado agregado, que se limita a informações genéricas, muitas vezes quantitativas, incapazes de identificar uma pessoa. A fim de promover campanhas publicitárias, tem se tornado comum o uso de tecnologias de perfilamento e predição comportamental com objetivo de impactar um público de interesse, porém

³ *Business to business* (B2B): relação comercial desenvolvida entre duas entidades corporativas, como fornecedores.

⁴ *Business to consumers* (B2C): relação comercial desenvolvida entre uma entidade corporativa e seus clientes.

⁵ BRASIL. Decreto nº 8.771 de 11 de maio de 2016. Brasília, 2016. Disponível em: <[link](#)>. Acesso em 30 mai 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

não é uma regra que essas tecnologias se valham de dados pessoais identificados.



EXEMPLO

A VARIAÇÃO “IDENTIFICADA OU IDENTIFICÁVEL” POSSUI ESPECIAL RELEVÂNCIA PARA A CARACTERIZAÇÃO DE UM DADO COMO PESSOAL.

- Dizer que uma estudante de nome X faz graduação na Escola Y e possui um e-mail <x@provedor.com>, é lidar com dados pessoais identificados. Dizer, contudo, que a estudante da Escola Y, cujo número de matrícula começa com os caracteres 0123 tirou a nota A no processo seletivo para uma bolsa de estudos, é lidar com dados pessoais identificáveis. Aqui, as informações fornecidas sobre a estudante permitem o cruzamento com um banco de dados prévio que aponte para a identidade exata da discente.

Ok, mas e o dado pessoal sensível, qual é a diferença? O dado pessoal sensível é uma espécie do gênero dado pessoal, cujas preocupações do legislador foram maiores pelo possível risco de uso indevido por parte dos agentes de tratamento. Nos termos da lei, estão incluídos os dados relativos à origem étnica e religiosa, de filiação a organização política, religiosa ou filosófica, de aspectos ligados à saúde ou à vida sexual, e os que tratam da origem genética ou biométrica da pessoa natural identificada ou identificável.

EXEMPLO

DEFINIÇÃO DE DADO PESSOAL SENSÍVEL.



- No exemplo da nossa aluna da Escola Y, podem ser classificados como dados pessoais sensíveis, a sua digital do registro acadêmico (dados biométricos), a opção assinalada para a etnia na ficha de cadastro e matrícula (se branco, indígena, afrodescendente...) e sua participação junto a centros e diretórios estudantis (filiação a organização política, dada uma interpretação ampla).

A diferenciação do dado pessoal sensível na legislação ocorre porque esse tipo de dado possui maiores chances de ser manipulado de forma tendenciosa e discriminatória, causando danos a indivíduos ou a certos grupos de indivíduos. Portanto, a LGPD trouxe esse conceito e o conectou às exigências adicionais a fim de resguardar os direitos individuais e coletivos dos titulares.

Um aspecto importante à análise de boas práticas de *marketing* é que, muitas vezes, dados que não são considerados sensíveis pela LGPD, ainda assim, podem ensejar práticas discriminatórias ao titular de dados. Como exemplo, se um dado pessoal de endereço de um cliente, for utilizado para tratá-lo de forma prejudicial/discriminatória em relação a outro cliente que resida em outra área, isso pode se caracterizar como uma violação à LGPD.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Desse modo, é preciso estar atento e adotar as práticas necessárias para salvaguardar os direitos dos titulares e coibir qualquer tipo de ação discriminatória no tratamento de dados pessoais, sejam eles taxativamente sensíveis ou não⁶. A discriminação, contudo, não guarda relação de estratégias legítimas pautadas em públicos-alvo, onde o tratamento de dados de um titular se deu em consonância com a LGPD.

Passando ao próximo esclarecimento: quem, afinal, é o titular de dados na LGPD? Como visto, sendo o dado pessoal qualquer informação atinente a uma pessoa identificada ou identificável, o titular é justamente a pessoa natural à qual esse dado se refere.

Mas, e quem é responsável por tratar esses dados: quem são os chamados agentes de tratamento? Conforme estipula a legislação, os agentes de tratamento podem ser classificados por duas categorias: controlador e operador. O controlador, é aquele que possui o poder de decisão sobre as atividades, aquele que define as regras do jogo. Já o operador é aquele que executa o que foi definido pelo controlador, não detendo assim, poder de decisão sobre as atividades.

EXEMPLO

DIFERENÇA ENTRE CONTROLADOR E OPERADOR



- Suponha que a Escola Y crie uma estratégia de marketing para divulgar seus cursos em parceria com uma agência durante a realização de um evento de Economia. Todo o gerenciamento e a indicação de participantes ao evento, além das formas de divulgação foram indicados pela Escola Y. À agência, caberá apenas a realização do evento segundo as ordens recebidas já que, no contrato, ela não possui autonomia para decidir nada sobre dados pessoais. Assim, a Escola Y é a controladora dos dados pessoais, sendo a parceira a operadora.

Esta distinção é importante para garantir a responsabilização em casos de ilícitos civis, administrativos e penais, além do cumprimento de obrigações legais frente a autoridades governamentais. O controlador terá um grau de responsabilidades maior a depender do contexto.

Tudo bem, até agora. Porém, o que significa uma operação de tratamento de dados pessoais na LGPD? O tratamento é qualquer tipo de ação relacionada a um dado pessoal. Na definição da lei são empregados vinte verbos não exaustivos para ilustrar essa conduta, a exemplo de acessar, coletar,

⁶Sobre a taxatividade legal de dados sensíveis em regulamentos de proteção de dados de diferentes países, SOLOVE apresenta curiosa crítica sobre o fato de que a depender do país, alguns dados são considerados sensíveis, enquanto em outro não, como por exemplo (dentre muitos) o dado de geolocalização, que em determinados países pode ser considerado como dado sensível. Esta divergência apresenta grande dificuldade para instituições globais realizarem o correto tratamento dos dados pessoais e ainda, demonstra o quão frágil é a definição de um dado como sensível ou não, sem a avaliação do contexto (SOLOVE, Daniel J. Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data, p.12-13. In The George Washington University Law School. GWU Legal Studies Research Paper No. 2023-22, GWU Law School Public Law Research Paper No. 2023-22. Disponível em: < [link](#) > Acesso em 26 abr. 2023).

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

classificar, avaliar, reproduzir, transmitir, arquivar, eliminar ou avaliar, entre outros.

Portanto, todas as ações relativas a dados de pessoas naturais – desde acessar uma base de registro de alunos recém-matriculados, a editar uma planilha com informações sobre inscritos em um evento acadêmico na Escola Y – estão abrangidas pela LGPD. A condição, é claro, é a de que esses dados sejam identificados ou estejam suscetíveis a identificação.

As ações de *marketing*, contudo, nem sempre lidarão com dados pessoais. Isso, porque as estratégias comerciais de comunicação e veiculação de uma marca, produto ou serviço passam tanto pelas relações de tratamento de dados B2B (relações corporativas, como entre duas empresas) quanto B2C (relações consumeristas, como entre a Escola Y e um aluno). E, nesse caso, como distinguir o que é ou não dado pessoal?

Caso a relação e os sujeitos afetados estejam no âmbito B2B e os dados tratados forem apenas institucionais, de caráter corporativo, a LGPD não será aplicável. Mas, cuidado! Ainda que no âmbito de uma relação B2B de cunho corporativo, é possível que sejam tratados dados pessoais, como de alunos ou empregados. A regra, nesse ponto, é clara: se um dado pessoal identificado ou identificável for tratado para fins de *marketing*, a LGPD é aplicável.

Já no âmbito de relações B2C, a lei de dados com seus princípios e garantias deverá ser observada e todas as obrigações previstas na LGPD vincularão a operação de tratamento.



DICA E-MAIL INSTITUCIONAL

- A constatação do nome da instituição à qual o profissional está vinculado no lugar de seu nome pessoal como assinatura, acompanhada de um e-mail institucional, por exemplo (departamento@instituiçãoxy), são indícios de que o dado se relaciona a atividades não pessoais. Contudo, essas distinções precisarão de uma avaliação cuidadosa caso a caso.

Na prática, contudo, a distinção pode não ser tão fácil, já que na relação com microempresários, por exemplo, a figura do representante comercial e do titular se confundem por muitas das vezes.

Do mesmo modo, embora não inserida no contexto de relacionamentos corporativos de fornecimento B2B, o contato com jornalistas também está suscetível de confusão entre o canal de comunicação institucional e o da pessoa natural. Nesses casos, a não ser que os meios de contato (como e-mails, telefones e endereços) sejam estritamente corporativos ou institucionais, é melhor classificar os dados como pessoais, uma vez que há um claro intuito de abordagem individualizada e a pessoa natural está devidamente identificada ou identificável na relação.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Em ações que serão trabalhadas nas próximas seções deste Guia, como o envio de e-mail *marketing*, é possível obter indicativos acerca da natureza do dado, se pessoal ou institucional. Trabalhados esses conceitos basilares, é hora de avançar para a próxima seção, onde serão investigadas as bases legais que fundamentam a realização de operações de tratamento para fins de *marketing*.

3. LGPD E MARKETING: PRINCIPAIS BASES LEGAIS

De modo geral, qualquer operação envolvendo dados pessoais necessitará de uma base legal, ou seja, uma hipótese autorizativa prevista na LGPD que permite o tratamento de dados pessoais de acordo com o contexto específico. Das hipóteses autorizativas previstas na lei⁷, duas costumam ser mais utilizadas quando abordamos atividades de *marketing* (sem prejuízo da aplicação eventual de outra base legal). São elas: interesse legítimo e consentimento.

Conforme será abordado no próximo tópico, o interesse legítimo precisa ser evidenciado por critérios específicos, contidos no inciso IX do art. 7º e no art. 10 da LGPD. Boas práticas na cultura internacional de proteção de dados, como a utilização do formulário de legítimo interesse – LIA (*Legitimate Interest Assessment*) – assunto também abordado no próximo tópico – são exemplos de mecanismos para evidenciar o correto enquadramento das atividades de *marketing* nesta base legal.

Quanto à utilização da base legal do consentimento, apesar desta hipótese ser muito difundida para atividades de *marketing*, é preciso ter cautela quanto ao seu uso e especificidades, seja pelos modos de sua obtenção, seus limites ou sua revogação. Não demonstrar que o consentimento foi obtido de forma livre, informada e inequívoca pelo titular de dados, para um fim determinado, garantindo sua pronta revogação – pode trazer riscos para a organização.

Esclarecidos os pontos introdutórios, o objetivo seguinte será conceituar essas duas hipóteses.

⁷ Para **dados pessoais** (não sensíveis), as hipóteses estão dispostas no artigo 7º da LGPD e são: (1) o fornecimento de consentimento pelo titular dos dados; (2) o cumprimento de obrigação legal ou regulatória, como registros tributários e contábeis; (3) a execução de políticas públicas pelo poder público; (4) a promoção de estudos por órgão de pesquisa; (5) a execução de contratos, bem como o desenvolvimento de expedientes contratuais preliminares; (6) o exercício regular de direitos em litígios administrativos, judiciais ou arbitrais; (7) a proteção da vida ou incolumidade física; (8) a tutela da saúde por parte de profissionais, autoridades ou prestadoras de serviços da área; (9) o interesse legítimo do controlador ou de terceiro; (10) a proteção do crédito. Para **dados pessoais sensíveis**, as hipóteses estão dispostas no artigo 11 da LGPD são: (1) consentimento pelo titular ou responsável legal; (2) cumprimento de obrigação legal ou regulatória, (3) execução de políticas públicas previstas em leis ou regulamentos, pela administração pública; (4) realização de estudos por órgão de pesquisa; (5) exercício regular de direitos, inclusive em contratos e em processo judicial, administrativo e arbitral; (6) proteção da vida ou incolumidade física; (7) tutela da saúde, seja por profissionais da área, serviços de saúde ou autoridades sanitárias e (8) garantia da prevenção à fraude e à segurança do titular em identificações e autenticações de cadastro em sistemas eletrônicos.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

3.1 A BASE LEGAL DO INTERESSE LEGÍTIMO

Enquanto base legal, o interesse legítimo é especialmente importante para situações as quais envolvam práticas de *marketing*, tendo se provado uma boa alternativa para a mitigação de riscos.

Nas estratégias de *marketing* contemporâneas, conforme já mencionado, é vital o contato com os potenciais clientes, conhecidos como *prospects* e *leads* (a diferença entre ambos e as diretrizes básicas de abordagem serão trabalhadas no [item 4.1](#)). Para desenvolver essa relação, é comum o tratamento de dados pessoais – como e-mail, nome, rede social e preferências de consumo, entre outros. Em Instituições Educacionais, sobretudo do setor privado, essa situação não é diferente.



PONTO DE ATENÇÃO

DADOS SENSÍVEIS x INTERESSE LEGÍTIMO

- A base legal do interesse legítimo não poderá ser utilizada para tratar dados pessoais sensíveis (como preferências sexuais, políticas, religiosas ou dados de saúde ou biométricos) em situações de *marketing*.

Citando-se a experiência internacional sobre o tema, no âmbito da União Europeia, o GDPR – Regulamento Geral de Proteção de Dados Europeu, legislação que serviu de inspiração para leis de proteção de dados ao redor do mundo, inclusive a brasileira – reconheceu a possibilidade de uso do interesse legítimo em determinados casos de ações de *marketing*. No “considerando”⁸ de número 47, o GDPR prevê que “o processamento de dados pessoais para propósitos de *marketing* direto pode ser considerado como de interesse legítimo”⁹.

Vale mencionar também o caso do Reino Unido, onde mesmo em um contexto regulatório mais rígido no qual o consentimento pode ser apontado como via preferencial para o envio de mensagens diretas de *marketing*– graças ao *Privacy and Electronic Communications (EC Directive) Regulations 2003* (chamado de “PECR”) –, existe a brecha/exceção razoável chamada de *soft opt-in*¹⁰ (ou adesão

⁸ Também chamado de “recital”, se refere a uma ponderação textual do legislador feita antes da apresentação de uma norma.

⁹ EUROPEIA, U. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Jornal Oficial da União Europeia, [s.l.], n. (Atos legislativos), [s.d.]. Disponível em:<[link](#)>. Acesso em:15 mar 2023.

¹⁰ “Uso de e-mail eletrônico para propósitos de *marketing* direto

22. (1) Esta regulação se aplica à transmissão de comunicações não solicitadas pela via de e-mail eletrônico a assinantes individuais.

(2) Exceto nas circunstâncias descritas no parágrafo (3), uma pessoa não deve transmitir ou fomentar a transmissão de comunicações não solicitadas para propósitos de *marketing* direto pela via de e-mail eletrônico, a menos que o destinatário desta mensagem tenha previamente consentido ao seu emissor para o recebimento momentâneo de tais comunicações

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

flexível em uma tradução livre).

Como explica a Autoridade de Proteção de Dados Pessoais do Reino Unido (“ICO”), a adesão flexível reflete um conjunto de situações de e-mail *marketing* onde, algumas variáveis concomitantes estão presentes, como: (i) se os dados pessoais de contato do titular foram obtidos pelo agente de tratamento diretamente (e não por terceiros que o repassaram); (ii) tais dados foram obtidos no decurso de uma relação de negociação ou venda de produto ou serviço com o titular; (iii) a estratégia de *marketing* destina-se ao oferecimento de produtos e serviços similares aos desejados ou contratados anteriormente; e (iv) é facilitada a opção de saída ou de discordância (*opt-out*) tanto no momento de cadastro do dado quanto do recebimento futuro de ofertas daquele anunciante¹¹.

É importante destacar que legislações como a PECR são mais restritivas do que o cenário legal brasileiro atual, no qual não há ordem de importância para a escolha de uma base legal. Entender as nuances da adesão flexível, contudo, ajuda a decifrar como o interesse legítimo pode ser um importante aliado a estratégias de *marketing*, observados os limites da legislação brasileira.

A esse respeito e, no contexto do Brasil, que limites seriam esses? A LGPD, ao dispor sobre a aplicabilidade da base legal do legítimo interesse, trouxe importantes indicadores a serem observados: (i) o relacionamento prévio com o titular, observado o princípio da transparência; (ii) a expectativa razoável do titular em receber algum tipo de conteúdo; e (iii) a garantia de direitos e salvaguardas do titular impactado com a ação de *marketing*.

De forma resumida, é necessário que a finalidade da ação seja legítima e guarde pertinência com o que está dentro da expectativa do titular de dados, que já possua algum tipo de relação com a instituição, independentemente de ter se tornado efetivamente um cliente.

Assim, a LGPD associou a noção de interesse legítimo ao conceito-chave de “legítima expectativa”, sinalizando que a operação de tratamento de dados precisa fazer parte de um horizonte razoável e esperado pelo titular de dados pessoais. Ainda, a LGPD atrelou o interesse legítimo à proteção de

por este disparadas ou instigadas.

(3) Uma pessoa pode enviar ou instigar o envio de e-mail eletrônico para propósitos de marketing direto quando—
(a) a pessoa obteve os detalhes de contato do destinatário do e-mail eletrônico no curso de uma venda ou negociação de um produto ou serviço ao destinatário;
(b) o marketing direto guarde similitude aos produtos ou serviços daquela pessoa; e
(c) o destinatário teve meios simples para recusar (livre de custos, exceto em relação aos custos da transmissão da negativa) o uso de seus detalhes de contato para propósitos de marketing direto, tanto no momento inicial da coleta quanto em comunicações subsequentes.” (REINO UNIDO. *Privacy and Electronic Communications (EC Directive) Regulations 2003*. Statutory Instruments, 2003, no. 2426. Tradução livre para o português. Disponível em: <[link](#)>. Acesso em: 12 jul. 2023).

¹¹ REINO UNIDO. Information Commissioner’s Office (“ICO”). *Como cumprimos as regras de envio de marketing por correio eletrônico?* (tradução livre). Disponível em <[link](#)>. Acesso em 22 mai 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

direitos e liberdades fundamentais do titular de dados, de modo que uma estratégia pautada nesta base legal não possa gerar sérias repercussões à esfera individual deste sujeito.

EXEMPLO

ENVIO DE E-MAIL PARA EX-ALUNOS SOB A BASE DE INTERESSE LEGÍTIMO



- Uma Instituição Educacional possui uma lista de interesse no curso de especialização “Fundamentos Matemáticos de Criptografia”. Os interessados em receber informações sobre a abertura de futuras turmas preenchem seu nome e e-mail. Meses após, recebem um e-mail da mesma instituição, oferecendo curso de mestrado nas áreas de Matemática e Ciências da Computação acompanhado por uma opção de não recebimento de novas mensagens. Neste caso, sob o ponto de vista da LGPD, o contato é legítimo, pois há relacionamento prévio iniciado pelo fornecimento do contato pelo titular; há expectativa legítima observado o curso oferecido em relação ao desejado pelo titular; e o recebimento de mensagem de oferta de um novo curso não é capaz de ferir direitos e garantias fundamentais do titular que, se incomodado, poderá se descadastrar para não mais receber este tipo de mensagem.

Para garantir a aplicabilidade da base de interesse legítimo às ações de *marketing*, cumpre dar ênfase ao último requisito, garantia de salvaguardas e direitos do titular, que deve ser ponderado de forma cuidadosa e documentada pelo agente de tratamento.

Nesse sentido, na LGPD, o próprio §3º do artigo 10 dispôs que a ANPD poderá determinar a exibição de relatório de impacto¹² à proteção de dados pessoais quando a operação de tratamento de dados pessoais tiver por fundamento o interesse legítimo. A realização do relatório de impacto, contudo, é medida aplicável apenas para quando detectados “altos riscos” à garantia dos princípios gerais de proteção de dados pessoais e às liberdades civis e direitos fundamentais dos titulares, conforme explicação da própria ANPD¹³. No entanto, como documentar as operações de interesse legítimo que não sejam de altos riscos e não requeiram a elaboração de um relatório de impacto?

Nesse sentido, uma importante ferramenta já solidificada na experiência de proteção de dados pessoais da União Europeia ganha destaque: o formulário de avaliação de legítimo interesse – LIA (*Legitimate Interest Assessment*). Por meio desta ferramenta é possível fundamentar a utilização do legítimo interesse por três etapas: (i) finalidade, (ii) necessidade e (iii) balanceamento.

Primeiramente, é necessário que cada agente de tratamento responda à seguinte pergunta: há uma

¹² Conforme definições da própria LGPD, o relatório de impacto é a “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”.

¹³ BRASIL. Autoridade Nacional de Proteção de Dados Pessoais. *Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais*, Relatório de Impacto à Proteção de Dados Pessoais (RIPD), atualizado em 06 abr. 2023. Disponível em: <[link](#)>. Acesso em: 13 jul. 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

finalidade específica e legítima para tratar os dados pessoais? Portanto, meras bases de dados mantidas “por conveniência” e sem qualquer finalidade específica de uso não se encaixam no critério explicitado. Se as operações de tratamento ocorrerem por mais de um agente de tratamento, será necessário avaliar individualmente a finalidade de uso do dado conforme a legitimidade.

Em seguida, vem o teste de necessidade: é possível elencar outras formas viáveis e razoáveis de tratar dados pessoais pelas quais se consiga atingir a finalidade pretendida? Se existe uma alternativa de tratamento menos invasiva ao titular de dados, ela certamente deverá ser adotada.

A última e decisiva etapa se dá pelo teste de balanceamento. Por acaso há ameaça concreta de que os interesses legítimos do agente de tratamento possam interferir negativamente em direitos e garantias individuais dos titulares de dados pessoais? Para esta última etapa, será necessário considerar três requisitos adicionais: (a) a natureza da relação de tratamento de dados desenvolvida; (b) as expectativas razoáveis do titular em relação à abordagem do agente de tratamento; e (c) os efetivos resultados e repercussões da operação de tratamento para os sujeitos envolvidos. Ao término deste Guia, há um anexo com perguntas elaboradas pela ICO, autoridade de proteção de dados do Reino Unido, que auxiliarão no desenvolvimento do LIA em cada uma de suas etapas. Vale a pena dar uma olhada (vide o [Anexo Único](#)).

Embora tenha origem na GDPR para o plano de fundo europeu, a ferramenta de avaliação do interesse legítimo não deve ser menosprezada para o contexto brasileiro. Como visto, a legislação brasileira também menciona diretamente a necessidade de avaliar os impactos aos direitos e garantias individuais dos titulares de dados, sendo o LIA um importante recurso para que os agentes de tratamento consigam documentar operações pautadas nesta base legal.

Feitas as observações sobre interesse legítimo, passa-se à análise da base legal de consentimento.

3.2 A BASE LEGAL DO CONSENTIMENTO

Previsto no inciso XII do artigo 5º da LGPD como manifestação livre, informada e inequívoca do titular para autorizar a realização de operações com seus dados pessoais, o consentimento é uma base legal que exige cautela e precisão em sua aplicação. Os requisitos legais do consentimento possuem um objetivo principal: de fundamentar o processo de tomada de decisão do titular¹⁴. Conforme se verá neste tópico, é preciso evidenciar a liberdade de escolha do titular, o acesso a informações necessárias e garantir que ele tenha entendido o escopo do tratamento de seus dados.

Para garantir a condição “livre” do consentimento é necessário assegurar que não ocorra vício de

¹⁴ BIONI, Bruno Ricardo e LUCIANO, Maria. O Consentimento como Processo: em Busca do Consentimento Válido, p. 243 – 257. In: DONEDA, Danilo et. al. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

vontade (como coação ou indução a erro, por exemplo) para que os titulares expressem a sua anuência de modo a ceder seus dados pessoais para os fins almejados.

Quanto à condição “informada”, a LGPD estipulou o conjunto de esclarecimentos prestados ao titular de dados antes e durante a manifestação do consentimento. É preciso certificar que informações essenciais sobre o tratamento de dados, seus modos, agentes envolvidos e eventuais riscos, não sejam omitidos. Ainda, o uso de linguagem muito técnico e pouco acessível, além do excesso de informações também podem inviabilizar a manifestação informada.

Já “inequívoca” é a manifestação, firme e clara, acerca da concordância positiva do titular para o tratamento de seus dados, inclusive cabendo ao controlador o ônus da prova da sua obtenção regular. É imprescindível garantir que o indivíduo concordou ativamente com as operações que serão realizadas com seus dados, o que poderá se dar por escrito, de forma falada ou gestual, desde que devidamente registrada para fins de comprovação.

DICA

CONSENTIMENTO E FINALIDADE ANDAM JUNTOS



- O consentimento deve sempre se referir a finalidades determinadas! As autorizações genéricas para o tratamento de dados pessoais serão nulas para fins de cumprimento da LGPD; e
- É necessário avaliar sempre qual o propósito do dado coletado: identifique a finalidade para qual este dado será usado, em seguida, caso a base legal utilizada seja a do consentimento, avalie se ele está em sintonia para a finalidade estipulada. Finalidades distintas implicam consentimentos distintos.

Existem, ainda, outros dois requisitos adicionais (respectivamente previstos ao art. 8º, §§ 4º e 5º da LGPD) que formam uma espécie de “quinteto” de requisitos elementares do consentimento: a obrigação de obtenção para finalidades determinadas (invalidando pedidos genéricos ou pouco explicados) e a capacidade de revogação a qualquer tempo (o que torna essa base legal impraticável caso o agente de tratamento não possa parar a operação de tratamento após iniciado).

É preciso muita atenção para as situações em que o consentimento pode ser invalidado. Este deixará de ser livre caso o titular não tenha a capacidade de, facilmente, discordar acerca de um tratamento de dados pessoais e não o autorizar. Ainda, deixará de ser informado caso não sejam apresentadas, ao titular, as informações essenciais sobre o tratamento de seus dados pessoais (a Instituição Educacional deve avaliar o que precisa ser informado e em quais níveis, seja por meio de um simples aviso ou elaboração de Termos Uso e Avisos/Políticas de Privacidade, por exemplo).

Deixará, ainda, de ser inequívoco caso presuma uma vontade não externada pelo titular. Por exemplo, no preenchimento de formulários *online* que se utilizem do consentimento, a

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

disponibilização de uma caixa de seleção pré-marcada para um determinado fim não assegura sua legítima manifestação positiva.

O consentimento não será específico caso mescle finalidades distintas como se apenas uma fossem. Autorizações genéricas para o uso dos dados do titular que confundam finalidades distintas em um mesmo escopo e sem separação (ex.: caixa de seleção que integra ao mesmo tempo a inscrição em um evento opcional e a assinatura de uma revista eletrônica da entidade organizadora) são, assim, problemáticas e podem invalidar essa base legal.

Por fim, o consentimento também encontrará problemas como base legal caso não seja revogável. Assim, se o titular manifestar o desejo de revogar o consentimento outrora concedido, é importante ter ciência de que os tratamentos realizados até aquele momento são válidos (salvo se houver requisição de eliminação, situação em que uma análise legal e técnica se faz necessária sobre a viabilidade de exclusão dos dados), porém não poderão mais ser renovados.

Em Instituições Educacionais essa característica é de especial importância, pois muitas atividades se pautam em obrigações legais ou regulatórias ou mesmo em execução de contratos ou instrumentos jurídicos (junto ao Ministério da Educação ou outras agências de fomento), de modo que é importante separar as situações de consentimento para ações de *marketing* de outras operações de tratamento, as quais provavelmente seguirão por outras bases legais.

Um exemplo de situação em que a base legal do consentimento pode ser utilizada para ações de *marketing*, são os formulários de inscrições em eventos, cursos ou situações similares. No [Apêndice 2](#) deste Guia constam as principais diretrizes para sua elaboração.



DEFINIÇÃO CONSENTIMENTO

- **Livre:** o consentimento não pode ser manifestado sob vício de vontade ou imposição por parte do agente de tratamento;
- **Informado:** o consentimento só existe se todas as informações necessárias foram fornecidas de forma acessível ao titular ou a seu responsável legal para que ele forme o seu juízo de anuência ou vantagem;
- **Inequívoco:** o consentimento exige uma ação por parte do agente de tratamento que não pode ser presumida;
- **Específico:** o consentimento deve ser voltado a finalidades determinadas, vedadas autorizações genéricas; e
- **Revogável:** o consentimento deve ser articulado de modo que possa ser revogado a qualquer tempo e de forma fácil pelo titular, se ele assim o desejar.

Conforme visto, obter o consentimento válido do usuário é uma tarefa que exige cautela e demandará dos responsáveis por campanhas de *marketing* o que eles mais possuem: criatividade! Em tempos

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

tecnológicos e conectados como os de hoje, a disposição de textos longos, com letras muito miúdas e sem proximidade com o público-alvo é descontextualizada.



DICA

ESTRATÉGIAS CRIATIVAS E TRANSPARENTES DE CONSENTIMENTO

- O consentimento, de acordo com a LGPD, não precisa ser necessariamente escrito e muito menos extenso. Avalie, dentro da sua identidade visual e das estratégias de *marketing*, se há possibilidades inovadoras de obtenção do consentimento que respeitem e registrem o desejo do usuário. O uso de áudio, vídeo, de *checkbox* curtos e objetivos ou guias de navegação interativos são bons exemplos a depender das circunstâncias concretas variadas.

Assim, a utilização base legal do consentimento exige cautela e, ao mesmo tempo, pode ser uma oportunidade para articular novas estratégias de negócios e atividades às possibilidades tecnológicas que a *internet* e as formas de interação virtual proporcionam. É importante, contudo, o engajamento dos setores jurídico, tecnológico e de *marketing* para que os requisitos ora apresentados sejam implementados e mantidos corretamente, especialmente em ambientes eletrônicos que requeiram a correta configuração de funcionalidades para que o titular possa entender e concordar com o tratamento de seus dados pessoais por esta base legal.

4. PROTEÇÃO DE DADOS PESSOAIS EM ATIVIDADES DE MARKETING

Estabelecidas as análises acerca das duas principais bases legais para o tratamento de dados pessoais em ações de *marketing*, nesta seção serão trabalhadas algumas das situações mais comuns envolvendo *marketing* em Instituições Educacionais.

Alguns dos assuntos tratados serão: abordagem de prospects e *leads*, listas de e-mail *marketing*¹⁵, uso de ferramentas e novas tecnologias de publicidade, como *profiling*¹⁶ ou *chatbot*¹⁷, uso de técnicas de *business intelligence*, contato por *telemarketing*, ações promocionais com imagem e vídeo e *marketing* para crianças e adolescentes.

¹⁵ Para práticas razoáveis de *e-mail marketing*, consulte o Código de Autorregulamentação elaborado com a participação de diversas instituições dos segmentos de Direito e Publicidade, disponível na página da Associação Brasileira de Marketing e Dados (“ABEMD”) sob o título “*E-mail marketing – Boas Maneiras*”.

¹⁶ Perfilamento ou perfilagem, ato de processar dados pessoais, de forma automatizada ou não, para avaliar padrões de comportamento relativos a um indivíduo em concreto.

¹⁷ Programas desenvolvidos com a função de atendimento direto ao público e cujas interações podem ser baseadas em respostas fixas automatizadas ou em aprendizado de máquina.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

4.1 COLETA DE LEADS

Na literatura de *marketing* e estratégias comerciais, existe uma diferença entre *suspect*, *prospect*, *lead* e *customer*. Destaca-se, desde já, que não há uma terminologia universal para essas definições, sendo que o seu significado varia muito conforme o jargão utilizado pelo profissional de *marketing*. Para os fins deste Guia, as definições adotadas foram as seguintes:

FIGURA 1 - DO SUSPECT AO CUSTOMER



Fonte: D'HAEN; POEL, 2013

Um *suspect* é qualquer tipo de potencial cliente. Em uma lógica de funil, o *suspect* está no topo. São usuários genéricos que representam uma base de todos os clientes possíveis de serem abordados por uma marca. Em uma Instituição de Ensino Superior, por exemplo, podem ser todos os indivíduos que desejam cursar uma graduação ou pós-graduação.

Já o *prospect* é aquele indivíduo que se encontra entre possíveis contatos classificados sob um perfil desejado. Esse segundo estágio representa uma etapa de maior refinamento da base genérica de *suspects*, seguindo-se alguns critérios aleatórios ou estruturados. Para uma Instituição Educacional, eles representam uma lista de indivíduos que podem se interessar pelos seus cursos.

O *lead*, por sua vez, qualifica aquele sujeito com razoável probabilidade de contato e retorno por parte da instituição promotora da estratégia de divulgação¹⁸. Para uma Instituição Educacional, indivíduos que tenham prestado vestibular e ainda não tenham se matriculado, ou indivíduos que já tenham concluído cursos anteriores são *leads* qualificados. Por fim, o *customer* é a parte mais estreita do funil, o *lead* que foi convertido em consumidor/cliente/usuário com sucesso em uma campanha.

¹⁸ No mesmo sentido, ver Stevens, para quem um *lead* é um prospect que possui algum potencial de se tornar um consumidor (STEVENS, Ruth P. *Maximizing Lead Generation: the Complete Guide to B2B Marketers*, p. 02. Indianapolis: Pearson Education, jul. 2011).

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

A distinção entre essas quatro categorias demonstra qual é o estado de interação entre uma instituição e um titular de dados pessoais. Quanto mais genérica, caso de *suspects* e *prospects*, menor a probabilidade de que uma base legal de tratamento de dados pessoais possa ser justificada sem o consentimento. Quanto mais afunilada, casos de *leads* e *customers*, maiores as chances de um relacionamento fixado no interesse legítimo (desde que devidamente documentado e juridicamente embasado) e que a estratégia de *marketing* seja positiva.

Foram finalizadas as considerações sobre *marketing* e coleta de *leads*. Mas não deixe de olhar os demais tópicos desta seção, pois podem guardar relação a este tema. Por enquanto, ressaltam-se os seguintes pontos:



RESUMO

MARKETING E COLETA DE LEADS

- Em estratégias de *marketing*, a relação com potenciais clientes pode seguir três etapas: o *suspect* é aquele que possui interesse geral em certos tipos de produtos e/ou serviços, o *prospect* é aquele que possui potencial interesse em um tipo específico de produtos e/ou serviços e o *lead* é aquele que já manifestou interesse nos produtos e/ou serviços de uma instituição. O *customer*, representa a conversão do interessado em consumidor.
- Observadas as bases legais da LGPD, quanto mais geral for a relação com o titular de dados (*suspects* ou *prospects*), maior a probabilidade de aplicabilidade do consentimento. Por sua vez, quanto mais afunilada a relação (*leads* e *customers*), maior a probabilidade de que o interesse legítimo possa ser utilizado, desde que justificado e documentado.

4.2 LISTA DE CONTATOS PARA *MARKETING*: POSSO COMPRAR? PRECISO DE CONSENTIMENTO PARA AS QUE JÁ POSSUO?

Para lidar com listas de contato de *marketing* (como as que contêm telefone e *e-mail*), é fundamental observar como elas foram formadas e se houve algum fluxo de compartilhamento. Seja no corpo de um documento de texto, de uma mensagem de *e-mail* ou de planilhas eletrônicas, as listas com contatos costumam circular livremente entre departamentos e/ou unidades internas de entidades públicas e privadas que desejam divulgar suas atividades, serviços, produtos ou eventos. Além de preocupações com a circulação segura dessas informações, é importante tomar cuidado com o modo pelo qual foram constituídas diante do cenário da LGPD.

A primeira ressalva a ser feita com relação a *marketing* se dá para situações de compra, permuta ou outro tipo de negociação envolvendo listas de endereços eletrônicos. Caso a sua instituição ou setor possuam listas de contatos adquiridas de um terceiro, é necessário ter em mente que essa é uma

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

situação delicada e que requer alguns cuidados.

Nesse sentido, importante trazer o conceito de *marketing* indireto (*thirdy party*): quando um titular de dados autoriza uma instituição (A) para que outra instituição (B), ou outras instituições (C e D), entrem em contato por meio de estratégias de conversão, como o e-mail *marketing*. A prática de *marketing* indireto é válida desde que siga algumas diretrizes básicas de controle, transparência e qualidade.

Primeiramente, é necessário provar que a base legal aplicável foi respeitada em relação ao titular e à empresa que repassou os dados. É aconselhável assegurar que o titular tenha mecanismos para acompanhar como se deu o tratamento e o compartilhamento de seus dados e com quem.

Caso a base legal para o tratamento dos dados seja a do consentimento, é necessário observar o seu sentido: o consentimento para compartilhamento de dados da empresa A com a empresa B segue a ordem A para B e não de B para C. O consentimento é específico àquele propósito de compartilhamento e não deve ser interpretado de forma alargada ou indiscriminada. Portanto, ser contatado em uma ação de *marketing* por uma empresa B, a partir de uma estratégia legal e transparente organizada pela empresa A é distinto de ser contatado promocionalmente por uma empresa C, não conhecida e cujas expectativas razoáveis de contato não possam ser presumidas.

Cumpra observar que é possível a aplicação da base legal de execução de contrato ou mesmo de interesses legítimos (art. 7º, V e IX da LGPD) para casos em que o compartilhamento dos dados para fins de *marketing* esteja disposto em instrumento contratual ou devidamente orquestrado com transparência e expectativas razoáveis.

Nesses casos, além da disposição contratual específica sobre o compartilhamento de dados para fim legítimo a partir de base legal válida, é importante, em atenção ao princípio da transparência, deixar claro a existência do compartilhamento e nomear o agente de tratamento que receberá os dados (podendo constar em Termos/Avisos/Políticas de Privacidade).

Por fim, é importantíssimo ressaltar que o recurso do *marketing* indireto precisa levar em conta qual a posição contratual da Instituição Educacional: se controladora ou se operadora de dados e quais as prerrogativas lhe foram concedidas quanto ao tratamento. Caso a instituição seja operadora de dados (apenas realiza opções de tratamento sob as ordens de uma parceira controladora), o uso dos dados para os fins de *marketing* poderá se configurar infração contratual e desvio de finalidade da conduta se não autorizada de forma expressa em contrato pela controladora.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	



PONTO DE ATENÇÃO

MARKETING INDIRETO

- Avalie junto ao setor de proteção de dados qual a posição contratual da sua Instituição Educacional antes de usar dados compartilhados para fins de marketing indireto. Se a instituição for operadora de dados, a abordagem poderá implicar infração contratual por desvio de finalidade da operação.

Feita a ressalva para as listas compradas, passemos a análise de como lidar, sob a ótica da LGPD, com listas de *e-mail* pré-existentes e construídas internamente pelo setor.

Inicialmente, é preciso considerar que as listas de *e-mail marketing* construídas internamente precisam ser avaliadas quanto ao modo de sua elaboração. É pertinente avaliar se a lista possui um processo detalhado, registrado e justificado de compilação e se indivíduos ali incluídos já possuem expectativas legítimas/razoáveis ou relação prévia com a Instituição Educacional. Quanto mais aleatória for a lista, maior a probabilidade de inadequação à LGPD.

Manter um processo de controle de qualidade de construção dessas listas, separando o tipo de titular e sua categoria específica é o mais indicado. Quanto maior o detalhamento, mais fácil será justificar o tratamento de dados pessoais, inclusive para aplicar o interesse legítimo.

Seja qual for a circunstância utilizada para listas de *e-mail marketing*, ainda que obtidas sob o consentimento válido, ou devidamente registradas sob o interesse legítimo, sempre disponibilize um canal para descadastramento dessas mensagens promocionais. Isso não inclui, *e-mails* de contato regular e necessário para o desenvolvimento de uma relação contratual de compra de produtos ou prestação de serviços (como *e-mails* contendo informações sobre a alteração do horário de funcionamento da instituição ou de cobrança de taxas ou mensalidades, por exemplo).

Foram finalizadas as considerações sobre listas de contatos para *marketing*, mas não deixe de olhar os demais tópicos desta seção, pois podem guardar relação a este tema. Por enquanto, destacam-se os seguintes pontos:

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	



RESUMO

LISTAS DE MARKETING

- Evite a compra e/ou negociação de bases de endereços para *marketing*. Se estritamente necessário, certifique-se de que a operação possui base legal (como consentimento, interesses legítimos ou execução de contrato) e de que há transparência ao titular. Solicite, antes, um parecer da Equipe de Encarregado de Dados (*Data Protection Officer/ DPO*) ou equivalente para avaliar essa operação. Para bases internas de *e-mail marketing*, avalie se existe algum tipo de controle sobre como foram construídas e se existem expectativas razoáveis dos titulares para receber o contato.

4.3 USO DE FERRAMENTAS E NOVAS TECNOLOGIAS DE PUBLICIDADE

É inegável que, com o surgimento da internet, novas tecnologias e sua democratização, a forma de fazer publicidade foi ressignificada. Foi-se o tempo de anúncios genéricos veiculados em jornais, revistas e canais de TV para um grande público, cujas informações individualizadas não eram tão acessíveis. Atualmente, contudo, com a evolução dos dispositivos tecnológicos de comunicação, a publicidade ganhou mais ferramentas de segmentação de público e divulgação.

As tecnologias disponíveis hoje no mercado podem apresentar um grande benefício para uma Instituição Educacional no modo de fazer publicidade, porém é necessário cautela quanto aos seus usos. Conforme vem sendo pontuado neste Guia, qualquer tratamento de dado pessoal precisa estar em conformidade com a LGPD.

A seguir, sem pretensão de exaurimento, listamos algumas ferramentas disponíveis hoje, seus riscos e como utilizá-las dentro das expectativas dos titulares de dados e dos requisitos legais aplicáveis.

- **Cookies**

O debate sobre a privacidade *online*, a proteção dos dados pessoais e o impacto do rastreamento *online* nos direitos individuais tem crescido nos últimos anos e gerou uma preocupação social em torno do uso dos famosos *cookies*. Afinal, muitas vezes uma pessoa visita uma página na *internet* sem saber que suas ações podem ser “vigiadas” e registradas por terceiros.

O tema merece atenção, porém não se pode deixar de observar que os *cookies* são um expediente técnico necessário ao funcionamento da *internet* contemporânea. O uso abusivo dessa ferramenta deve ser coibido, porém, uma “condenação genérica” sobre esta tecnologia não parece razoável.

Mas, afinal, o que são *cookies*? De acordo com o Guia Orientativo Cookies e proteção de dados pessoais da ANPD, *cookies* podem ser definidos como “arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

algumas situações, visando ao atendimento de finalidades diversas.”¹⁹

Os *cookies* podem ser classificados sob diversas perspectivas distintas. Valendo-se do critério de finalidade, podemos classificá-los, de forma geral, e ainda referenciando o Guia da ANPD, como: **(i) cookies de funcionalidade** (que permitem funções básicas ao usuário, por exemplo, lembrar preferências do site ou aplicação, como nome de usuário, região ou idioma); **(ii) cookies analíticos** (que permitem coletar dados e informações sobre como os usuários utilizam o *site*, quais páginas visitam com mais frequência, ou ainda a ocorrência de erros do próprio *site* ou da aplicação) e; **(iii) cookies de publicidade** (que servem para traçar um perfil do usuário baseado em dados relativos à sua navegação, auxiliando a exibição e criação de anúncios personalizados)²⁰.

No contexto deste Guia, os *cookies* de publicidade possuem destaque, especialmente nos casos em que eles possam rastrear de forma identificada ou identificável o comportamento de um usuário, observada sua navegação na *internet*. Assim, por meio deles é possível mensurar e veicular publicidade no ambiente digital de modo personalizado, e assim mostrar anúncios *online* de produtos e serviços que podem ser do interesse do usuário que está navegando na página.

Ao analisar o uso de *cookies* sob a ótica da LGPD, alguns aspectos precisam ser observados. Primeiramente é preciso deixar claro para o titular que o *site* faz uso de *cookies*. Isso pode ser feito por meio de um pequeno aviso na página para que o titular manifeste sua ciência e, ainda, por meio de um Aviso/Política de *Cookies*, que haja de forma detalhada os usos e finalidades de cada *cookie*.

Na prática europeia é comum a utilização da ferramenta de *cookie banner*, onde o titular pode fazer a gerência dos *cookies* que deseja aceitar ou não, em cada *site*²¹ a partir do consentimento para *cookies* opcionais. No Brasil, contudo, não há entendimento taxativo sobre a obrigatoriedade do uso desta ferramenta ou mesmo da base legal do consentimento (não há vedação ao uso da base legal do interesse legítimo), ficando a sua adoção a critério das instituições responsáveis por páginas e serviços de *internet*, observados os limites da LGPD.

É preciso, ainda, frisar que os *cookies* podem ser gerenciados no próprio navegador do usuário, de modo que este tem a liberalidade de deletá-los caso assim prefira. Outra alternativa simples é a utilização do recurso “aba privativa” do navegador, o qual é possível desabilitar o novo depósito de

¹⁹ BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo Cookies e proteção de dados pessoais, p. 08. Versão 1.0. Outubro de 2022. Disponível em: <[link](#)> Acesso em 08 de ago. 2023.

²⁰ Autoridade Nacional de Proteção de Dados Pessoais, op. cit., nota 19, p. 11.

²¹ Para mais informações sobre o uso de Cookie Banner no contexto europeu acesse o Relatório do trabalho realizado pela Força-Tarefa Cookie Banner (livre tradução), elaborado pelo Comitê Europeu para a Proteção de Dados (*European Data Protection Board* - “EDPB”) disponível em: <[link](#)>.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

cookies na sessão, sem excluir os já ativos.

- **Pixels de rastreamento, web beacons e tecnologias similares**

Ferramentas de *marketing* digital como *pixels* e *web beacons*, são alguns exemplos de tecnologias que, assim como os *cookies*, são utilizadas para rastreamento comportamental de navegação na *web*. Contudo, diferentemente destes, podem não ser facilmente notadas pelo usuário, o que implica uma maior cautela à utilização destas ferramentas, segundo a ótica de proteção de dados.

Apesar de guardarem similaridades quanto ao objetivo de rastreamento comportamental, cada ferramenta possui sua forma de implementação específica e funcionalidade.

Um *pixel* de rastreamento pode ser definido, de modo simples, como um pequeno pedaço de código depositado em um site ou anúncio, no qual a instituição responsável definirá as metas de rastreamento, como por exemplo, compras, cliques ou visualizações de página²². Estes códigos não necessariamente estão identificados para o usuário, o que desperta atenção especial quanto ao uso. Em síntese, os dados coletados podem ser usados para criar anúncios direcionados para quem tem maior probabilidade de se interessar pelo produto/serviço, com base no comportamento rastreado.

Já o *web beacon*, pode ser definido como uma imagem gráfica clara (normalmente de um *pixel* de tamanho) que é entregue por meio de um navegador da *web* ou *e-mail* HTML, funcionando como uma *tag* que registra a visita de um usuário a uma determinada página ou a visualização de um *e-mail* específico²³. Em síntese, o *web beacon* pode ser usado para monitorar aberturas de *e-mail*, visualizações de página, cliques em *links* e outras métricas.

Apesar da possibilidade de o usuário desabilitar esse tipo de rastreamento em seu navegador e nas configurações de seu *e-mail*, é importante sempre que possível que a Instituição Educacional que se utilize dessa tecnologia, além de sinalizar sobre sua utilização, informe também como é possível desabilitar essa função.

O principal ponto de criticidade dessas tecnologias, no aspecto de proteção de dados, é a transparência quanto à sua utilização. Não deixar claro que alguma dessas ferramentas estão sendo utilizadas, a finalidade ou quais dados serão tratados, pode representar risco de violação à LGPD e à integridade do titular de dados, pois não se sabe até que ponto dados sensíveis, por exemplo, serão tratados sem o seu conhecimento ou, ainda, compartilhados com outras empresas. Por fim, outro ponto relevante é quanto à garantia do direito de oposição do titular ao tratamento de seus

²² ESTADOS UNIDOS DA AMÉRICA. *Federal Trade Commission* (“FTC”). *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*. 16 mar. 2023. Disponível em <[link](#)>. Acesso em 10 ago. 2023.

²³ *The International Association of Privacy Professionals* (“IAPP”). *Web Beacon*. Disponível em <[link](#)>. Acesso em 10 ago. 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

dados, caso este não concorde.

Desse modo, antes de utilizar esse tipo de ferramenta é importante realizar uma consulta ao Encarregado de Proteção de Dados, ou setor responsável correspondente na instituição, a fim de que sejam ponderados os riscos e benefícios da utilização da ferramenta.

- **Retargeting**

O *retargeting* pode ser definido, de modo simples, como um tipo de publicidade *online* em que os visitantes de um *site* são segmentados com anúncios relacionados a esse *site* enquanto navegam em outros lugares²⁴. Em outras palavras, estratégias de *marketing* que se utilizam de *retargeting* permitem mostrar um anúncio a um usuário que já manifestou interesse por aquele conteúdo ou conteúdo similar, como por exemplo, uma pessoa que seleciona um produto e o adiciona em uma “sacola online” e depois desiste de sua compra.

Na prática, quando se direciona um conteúdo para uma pessoa que já manifestou interesse, a chance de conversão é mais alta do que uma divulgação para um público frio, que nunca teve contato com aquele produto/serviço. Contudo, apesar de se demonstrar uma boa estratégia de *marketing*, em termos de privacidade e proteção de dados algumas ressalvas devem ser feitas.

Quanto mais personalizado um anúncio direcionado, certamente mais dados (identificados ou não) acerca da pessoa impactada foram processados. Porém, em que momento foram coletados? Por quem foi coletado? Houve algum tipo de compartilhamento? É possível se opor a esse tratamento? Essas são perguntas que, para garantir a conformidade com a LGPD precisam ser respondidas.

Desse modo, conforme já foi dito, é necessário que haja transparência para com o titular de dados, além de ser garantido o direito de oposição ao tipo de tratamento realizado. Dispor na política de privacidade sobre a possibilidade de utilização dessa prática, descrevê-la de modo detalhado com caráter informativo e indicar um canal de exercício de direitos podem ser mecanismos suficientes para demonstração de conformidade.

Quanto à base legal aplicável, no Brasil é possível fundamentar o uso do *retargeting* por meio do legítimo interesse (observados todos os requisitos necessários, conforme exposto no [tópico 3.1](#)), porém há países em que será necessária a obtenção do consentimento do titular.

Assim, observadas as peculiaridades dessa estratégia de *marketing*, é imprescindível a consulta ao Encarregado de Proteção de Dados, ou setor correspondente, ao decidir utilizá-la.

²⁴ *The International Association of Privacy Professionals* (“IAPP”). *Retargeting*. Disponível em <[link](#)>. Acesso em 10 ago. 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	



RESUMO

USO DE FERRAMENTAS E NOVAS TECNOLOGIAS DE PUBLICIDADE

- **Cookies, pixels e web beacons** são alguns exemplos de ferramentas tecnológicas utilizadas, de modo geral, para rastrear o comportamento de usuários na *internet* a fim de personalizar e direcionar a publicidade ao público de interesse. O uso dessas ferramentas visa otimizar o impacto da publicidade. Ao fazer sua utilização, é preciso sempre garantir a transparência e informação sobre as finalidades de seu uso e o direito dos titulares impactados.
- A ferramenta de **retargeting**, em especial, garante o impacto de pessoas que já manifestaram interesse pelo conteúdo a ser vinculado. O uso dessa ferramenta pode ser fundamentado pelo legítimo interesse.

4.4 TRATAMENTOS AUTOMATIZADOS: QUANDO OS USOS DE PROFILING E CHATBOTS REQUEREM CUIDADOS ADICIONAIS?

O tratamento automatizado de dados pessoais pode ser entendido como aquele em que informações pessoais são tratadas mediante ferramentas tecnológicas, sem que seja necessário supervisão humana imediata na operação. Esses tratamentos podem considerar situações nas quais dados relacionados a pessoas naturais (ex.: seus dados financeiros), dados observados de pessoas naturais (ex.: seus hábitos de compra) ou dados inferidos de comportamentos individuais (ex.: sua pontuação em *rankings* de crédito) são manipulados por um sistema de forma automática.

Na LGPD, esse tipo de tratamento ganhou uma atenção especial tendo-se em vista a possibilidade de interferência direta nas preferências individuais e coletivas. Por previsão expressa, qualquer tipo de tratamento de dados realizado de forma automatizada poderá implicar o exercício de dois direitos aos titulares afetados: o direito à explicação e o direito à revisão.

Sobre o direito à explicação ou à informação, a legislação estipulou que o controlador deverá estar preparado caso utilize tratamento automatizado de dados em algum de seus produtos ou serviços. Nessa hipótese, ele poderá ser intimado a fornecer informações claras e adequadas sobre os critérios e procedimentos que levaram seu sistema ou ferramenta a uma certa decisão.

Já com relação ao direito à revisão, a LGPD foi explícita ao estipular que o titular exposto a qualquer tipo de decisão automatizada pautada em seus dados e capaz de afetar os seus interesses (ex.: decisão enviesada e discriminatória) poderá solicitar a sua reavaliação. Dessa forma, decisões sobre concessão de crédito, perfil psicológico, de consumo ou de outros aspectos da personalidade poderão estar sujeitas a uma reavaliação justificada. A lei não assegura, contudo, que a nova decisão deva ser necessariamente diferente da anterior, mas que seja revista sob a ótica de sua razoabilidade. Aqui, mais uma vez, o princípio da transparência revela-se de essencial importância.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Logo, os direitos à explicação e à revisão devem ser considerados sempre que houver tratamento automatizado de dados pessoais sem supervisão humana. O limite para estes direitos está nos segredos comercial e industrial, ou seja, onde há um mecanismo de propriedade intelectual protegido por lei e que limite o princípio da transparência em relação ao nível das informações reveladas.

Nas Instituições Educacionais, essa circunstância de tratamentos automatizados deve ser avaliada com cuidado, especialmente para duas situações de *marketing*: a prática de *profiling* e o uso de *chatbots*. Primeiramente será analisado o *profiling*.

A evolução da *internet* e a explosão de acesso a dispositivos e programas formados por sensores portáteis em celulares, relógios e outros produtos inteligentes, aumentou consideravelmente a capacidade de medir padrões humanos comportamentais. Nesse ponto, a prática de *profiling*, perfilamento ou perfilagem revela-se como uma poderosa ferramenta apta não apenas a compreender padrões embutidos nos hábitos humanos, mas a extrair valor dos mesmos.

O *profiling* pode ser definido, em linhas gerais, como uma forma de tratamento de dados pessoais que consista na utilização desses dados para avaliar determinados aspetos pessoais comportamentais de um indivíduo, podendo ser relacionado, por exemplo, a sua situação econômica, preferências pessoais, interesses²⁵, dentre uma infinidade de outros aspectos.

Para atividades de *marketing*, o *profiling* pode se tornar perigoso às vistas da LGPD quando causar ou possuir potencial de se desdobrar em práticas discriminatórias. A lei possui como um de seus princípios o da não discriminação, estipulando que qualquer tipo de operação de tratamento de dados não pode ser implementado quando gerar repercussões abusivas a uma pessoa ou grupo de pessoas.

É importante salientar que o conceito utilizado pelo regulamento europeu, o GDPR, foi o de tratamento automatizado de dados, conforme seu Recital 71²⁶. Na LGPD, contudo, a conceituação de *profiling* ficou aberta inicialmente, podendo incorporar tanto tratamentos supervisionados por humanos quanto não supervisionados.

O ponto de repercussão imediata para a LGPD é o de que se a prática for automatizada, é possível que seja necessário observar os direitos de explicação e de revisão (art. 20 da LGPD). Assim, é importante que a instituição esteja preparada para lidar com pedidos de explicação e revisão dos

²⁵ The International Association of Privacy Professionals ("IAPP"). *Profiling*. Disponível em <[link](#)>. Acesso em 11 ago. 2023.

²⁶ EUROPEIA, U. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Jornal Oficial da União Europeia, [s.l.], n. (Atos legislativos), [s.d.]. Disponível em: <[link](#)>. Acesso em 06 set 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

critérios e resultados de ações de *profiling* quando este for automatizado.

No caso de tratamentos de dados pessoais de forma automatizada com o intuito de *profiling*, ressalta-se, ainda, que quanto mais intrusiva for a prática – adentrando em hábitos estritamente particulares e sensíveis, como os relativos à saúde, às finanças, preferências políticas, sexuais ou de crença –, maior o risco de danos aos indivíduos e violação à LGPD.

Assim, por exemplo, um algoritmo que analisa por si só os dados pessoais de clientes e os classifica em categorias de perfis (etários, culturais, geoespaciais, sexuais, religiosos, etc.) para oferecimento de produtos ou serviços personalizados é um claro exemplo de *profiling* automatizado. Em contrapartida, qualquer classificação ou indicação de preferências realizada de forma manual (como preenchimento de formulários) não vincula o direito de revisão.

Portanto, se a sua unidade ou setor desempenha o papel de instigar tomadas de decisão automatizadas com base em *profiling*, será necessário estar preparado para construir justificativas cristalinas e, eventualmente, apreciar solicitações de revisão para decisões tomadas unicamente por soluções pautadas em algum tipo de inteligência artificial. Por outro lado, se as práticas de *profiling* são supervisionadas por humanos, o direito a explicação e a revisão não serão problemas, embora os demais direitos e princípios persistam.

Trabalhado o caso do *profiling*, a situação seguinte a ser analisada com cuidado especial para o direito à revisão é a dos *chatbots*. Ferramentas interativas digitais, os “robôs” de interação, ou *chatbots*, facilitam a comunicação com consumidores e potenciais clientes em meios virtuais.

Há diversos tipos e critérios que podem ser utilizados para classificação de *chatbots*. Cada critério de classificação poderá ensejar pontos de atenção específicos quanto à aplicabilidade da LGPD. Aqui, sem a pretensão de exaurimento sobre todos os tipos de classificação, registra-se com especial atenção a classificação quanto ao algoritmo utilizado para desenvolver o *chatbot*. Essa classificação define os *chatbots* em simples (limitados), inteligentes e híbridos²⁷.

O *chatbot* simples é aquele que apenas se alimenta de dados predispostos em uma fonte fixa, como textos de perguntas e respostas (“FAQ”) de instituições. Esse tipo de “robô” apenas analisa as entradas de digitação, por meio de palavras-chave contidas nas bases de alimentação. Se o usuário não usar palavras-chave ao se comunicar, o *bot* não o compreenderá, e a partir disso, poderá oferecer o canal de comunicação apropriado da instituição. Nesse caso não há risco de o robô interpretar ou criar um processo decisório autônomo. Assim, é preciso somente observar os princípios

²⁷ Trofymenko, Olenda; Prokop Y. V., Loginova, N. and Zadereyko, Alexander. Taxonomy of Chatbots. International Scientific And Practical Conference - Intellectual Systems And Information Technologies. Set. 2021. Odesa, Ukraine. Disponível em <[link](#)>.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

e direitos prescritos pela lei.

O *chatbot* inteligente, por sua vez, é aquele que desenvolve diálogos mais substanciais com os usuários, analisando sentenças linguísticas e respondendo de acordo com uma base de treinamento utilizada para ensinar o modelo de aprendizado de máquina. Esses robôs exigem uma grande base de dados para aperfeiçoamento do sistema²⁸. É possível ainda, que por meio da interação com o usuário, ele faça recomendações concretas e baseadas em seu interesse.

Já o *chatbot* híbrido pode empregar uma mescla de recursos dos dois tipos anteriores com vistas a guiar, passo a passo, as etapas de utilização do serviço por parte do usuário, desde a navegação inicial até o momento pós-compra, por exemplo.

Nesses dois últimos casos, portanto, os *chatbots* inteligentes e, eventualmente, o tipo de *chatbot* híbrido requerem a observância das mesmas diretrizes estipuladas anteriormente para a prática de *profiling*. Como esses robôs poderão tomar algumas decisões “próprias” baseadas nos dados fornecidos pelos usuários durante a interação, será necessário estar preparado para lidar com eventuais requisições de revisão desse processo interativo automatizado.

Ainda, ao utilizar esses dois tipos de robôs, será preciso tomar cuidado com situações de enviesamento em suas decisões para respeitar o princípio da não discriminação da LGPD, bem como prover mecanismos de informação ao usuário quanto ao processo decisório. Frisa-se que a LGPD não proíbe o tratamento automatizado de dados pessoais, mas apenas estipula regras de prestação de contas e disponibilização de informações mais claras e acessíveis.

RESUMO

TRATAMENTOS AUTOMATIZADOS E DIREITO À REVISÃO: QUANDO OS USOS DE *PROFILING* E *CHATBOTS* REQUEREM CUIDADOS ADICIONAIS?



- O tratamento automatizado decorre do processamento de dados pessoais sem a imediata supervisão humana. Na LGPD, esse tratamento incorporará possíveis demandas pautadas no direito à explicação e no direito à revisão
- O *profiling* caracteriza-se pelo tratamento de dados pessoais, automatizado ou não, para avaliar padrões individuais de um sujeito. Se automatizado, poderá ensejar eventuais requisições de explicação e revisão das decisões.
- Os *chatbot* são ferramentas interativas que facilitam a comunicação com o usuário/cliente. Dentre muitos critérios de classificação, citou-se a classificação por tipo de algoritmo (dividindo-se em simples, inteligentes ou híbridos). Caso sejam inteligentes ou híbridos, a Instituição Educacional também precisará saber lidar com eventuais requisições de explicação e revisão das decisões.

²⁸ Trofymenko, Olenda; Prokop Y. V., Loginova, N. and Zadereyko, Alexander, op. cit., nota 27.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

4.5 TÉCNICAS DE *BUSINESS INTELLIGENCE* (“BI”) E LGPD

Como já abordado, ao utilizar novas tecnologias e usufruir do universo de dados gerados por meio de navegação *online*, o *marketing* se tornou uma atividade ainda mais estratégica nas Instituições Educacionais e empresas em geral. Por meio do processamento de um alto volume de dados, é possível traçar análises inteligentes sobre um público específico que se busca atingir.

Nesse contexto, é válido mencionar neste Guia a utilização de plataformas de *business intelligence*, que têm se demonstrado fundamental na geração de análises de dados do negócio para diversas empresas. Em síntese, pode-se dizer que essas plataformas possuem um conjunto de ferramentas de análise de negócios que permite mensurar dados e compartilhar informações.

Por intermédio de diversos formatos de painéis de informações (“*dashboards*”) os dados de negócios podem ser registrados em tempo real, demonstrando indicadores de desempenho a eles atrelados. Essas plataformas são importantes para gerar dados agregados do negócio, que muitas vezes não precisam estar relacionados a pessoas identificadas/identificáveis.

As grandes questões, sob a ótica da proteção de dados pessoais, estão centralizadas em quatro pontos: (i) observar uma base legal válida (caso os dados estejam em formato identificado/identificável) e os princípios (ii) da segurança, (iii) não discriminação e (iv) necessidade.

É importante frisar que dados agregados, ou seja, dados genéricos e/ou quantitativos em que não é possível identificar uma pessoa, não entram no escopo de aplicação da LGPD. Assim, as análises de *marketing* com dados agregados não merecem ressalvas quanto à proteção de dados pessoais (ressalta-se somente a sua importância sob a ótica do sigilo e confidencialidade do negócio).

Porém, quando dados pessoais como nome, endereço, número de matrícula e curso, por exemplo, se encontram disponíveis individualmente, é preciso observar uma base legal válida da LGPD, sendo que dificilmente o consentimento se aplicará nesse cenário, já que o conhecimento (dentro das regras legais) sobre uma base de titulares é uma prática legítima de negócios e instituições e nem sempre é possível e viável acionar os titulares para toda e qualquer operação de tratamento.

Ainda, a observância do princípio da segurança²⁹ também é imprescindível. Para garanti-la é possível restringir o acesso nestas plataformas por meio de diferentes modalidades.

A título exemplificativo, o recurso chamado de RLS (segurança em nível de linha) da ferramenta de

²⁹ O princípio da segurança está disposto no art. 6º, VII da LGPD como a “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão”.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Business Intelligence da *Microsoft*, permite que seja gerenciado o acesso a *workspaces* (áreas com diversos painéis – *dashboards* – compartilhados) e, também, aos *dashboards*, por meio da modalidade “gerenciar funções”. Através dessa função é possível selecionar exatamente o perfil de acesso a dados específicos em um *dashboard*³⁰. Essa segregação de perfis é útil para evitar que dados ou informações importantes da Instituição estejam acessíveis a terceiros cujas funções não estejam atreladas à necessidade de acesso a eles.

Sobre o potencial risco discriminatório que estas ferramentas podem gerar, é necessário evitar que sejam traçados perfis de público-alvo por meio de critérios de análise enviesados. É crucial sempre estabelecer uma linha clara de diferenciação entre a seleção de um público potencialmente interessado em um produto/serviço e a segregação de pessoas por questões relacionadas a vieses preconceituosos e discriminatórios.

Por fim, quando se faz uso destas ferramentas de inteligência de negócio, é preciso sempre refletir sobre quais dados são efetivamente necessários para gerar os indicadores desejados. O princípio da necessidade, nesta ótica, é importante, não somente para a preservação do titular de dados, mas, também, para a geração de indicadores mais exatos que apontem de modo claro e sem informações desnecessárias, as estatísticas que realmente importam para a instituição.

O que podemos concluir é que o uso dessas plataformas, quando exploradas as diversas funcionalidades de segurança, não necessariamente apresenta risco de violação da LGPD, ao contrário, se utilizadas corretamente, é possível garantir a segurança de dados necessária.

RESUMO

TÉCNICAS DE *BUSINESS INTELLIGENCE* (“BI”) E LGPD



- Ferramentas de inteligência de negócios permitem hoje analisar dados em alta escala, traçar padrões e mensurar indicadores e métricas dos dados analisados. Caso as informações estejam tão somente agregadas/sem possibilidade de identificação de uma pessoa, a LGPD não será aplicável. Ao usar essas ferramentas é preciso observar a existência de base legal válida e o respeito aos princípios da LGPD, em especial, da não-discriminação, da segurança e da necessidade. A busca pela não-discriminação é afetada se as características de uma pessoa forem usadas em seu desproveito ou em desproveito do grupo a que pertence. A segurança é especialmente importante no controle de acesso das informações e seu modo de compartilhamento. Por fim, a necessidade clama pela análise de pertinência e razoabilidade entre um dado e o fim desejado, evitando-se tratamentos excessivos ou desproporcionais.

³⁰ Informações quanto às funcionalidades da ferramenta de *Power BI* da *Microsoft* disponíveis em <[link](#)>

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

4.6 TELEMARKETING: ENTRE A LGPD E REGULAÇÕES ESTATAIS AUTÔNOMAS

Nem todas as abordagens de *marketing* serão, por certo, baseadas em estratégias computacionais. A busca por influência junto a consumidores e potenciais consumidores pode se dar de duas grandes maneiras: a instituição promotora da ação de *marketing* não sabe com quem está lidando em específico e apenas explora uma região (ou um indicador genérico de clientes) ou a instituição sabe exatamente com quem deseja falar para uma campanha.

No primeiro caso, existe forte probabilidade de que a promotora da estratégia tenha definido uma determinada região geográfica para o caso de *marketing* postal, ou de prefixo de DDD (Discagem Direta à Distância) para o caso de *telemarketing*. Aqui, não será necessário tratar dados pessoais de forma prévia, mas apenas definir um certo território de atuação. Portanto, neste caso, não há qualquer operação de tratamento de dados, ao menos em um estágio anterior ao do efetivo contato.

No segundo caso, porém, o cliente ou potencial cliente está claramente identificado como alvo da instituição promotora, a qual teve acesso a algum tipo de dado pessoal filtrado previamente. Aqui, será necessário observar algumas diretrizes de proteção de dados pessoais da LGPD.

Dentro de um senso de razoabilidade, abordagens por ligação podem gerar incômodos, especialmente a depender do horário do contato. Neste caso, o consentimento é preferencial em termos fáticos, pois o titular de dados pessoais está deliberadamente escolhendo uma forma imediata e possivelmente agendada de disponibilidade de seu tempo. Assim será possível garantir as preferências do cliente ou potencial cliente.

Em homenagem ao princípio da transparência, é necessário deixar claro os motivos da ligação, um canal de contato permanente e a identidade do emissor da mensagem. A finalidade do contato também deve ser sempre observada: se o propósito da ligação é o de desenvolver uma pesquisa de mercado sobre a marca ou um certo produto ou serviço, o responsável pela chamada deverá se limitar a este propósito e não estender o contato para ofertas adicionais. A prática, conhecida como *sugestionamento* ou *sugging*, é desaconselhada por violar o princípio da finalidade.

Além das disposições da LGPD, Instituições de Ensino que se utilizem de *telemarketing* precisam observar a existência de algumas regulações estatais específicas. Em âmbito nacional, vale lembrar que a Agência Nacional de Telecomunicações – ANATEL criou o serviço chamado de “não me perturbe”, onde uma lista de telefones cadastrados indica o desejo dos titulares das linhas a não serem contatados. A disposição, porém, não se aplica a Instituições de Ensino, mas apenas às empresas de telefonia.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

No plano regional de alguns Estados da Federação, porém, foram criadas listas gerais de bloqueio a toda e qualquer abordagem de *telemarketing*, o que inclui Instituições de Ensino. São Paulo e Minas Gerais, os dois estados mais populosos do país, possuem serviços específicos³¹ criados por suas Instituições de Proteção e Defesa do Consumidor (“PROCON”) para bloquear todo e qualquer tipo de chamada. Assim, será necessário que a instituição, unidade ou departamento efetue um levantamento acerca das áreas de contato e dos números cadastrados em listas regionais de “não me perturbe”.

Ressalta-se, em acréscimo, o Ato nº 10.413/2021 – “Procedimento Operacional para Utilização de Recursos de Numeração” da ANATEL, que estabeleceu o prefixo “0303” para serviços de *telemarketing* ativo³². Esta medida visa coibir a prática de ligações indesejadas aos consumidores, por meio da identificação do número telefônico de chamada iniciando-se por “0303”.

Por fim, vale pontuar, o Decreto nº 11.034/2022³³, que instituiu a obrigatoriedade do Serviço de Atendimento ao Cliente (“SAC”) para atendimento de demandas de clientes e prestação de informações sobre serviços contratados. Esse atendimento deverá estar disponível obrigatoriamente por contato telefônico, além de outros canais, segundo a regulamentação. Durante a chamada, o tempo de espera do cliente não poderá conter conteúdo publicitário, a menos que haja o consentimento prévio e específico, conforme determina o art. 4º, §5º do decreto.

Foram finalizadas as considerações sobre *telemarketing*, mas não deixe de olhar os demais tópicos desta seção, pois podem guardar relação a este tema. Por enquanto, dá-se ênfase ao seguinte:

³¹ Em São Paulo, o endereço é: <link>. Em Minas Gerais, consulte a seguinte página: <link>. Se a sua campanha de telemarketing possuir uma abrangência nacional, consulte se os Estados envolvidos possuem regulações específicas de listas para *telemarketing*.

³² BRASIL. Ministério das Comunicações. ANATEL. “0303 entra em vigor para chamadas de telemarketing”. Publicado em 10 mar 2022. Disponível em: <link> Acesso em 14 jun. 2023.

³³ BRASIL. Decreto nº 11.034, de 5 de abril de 2022. Diário Oficial da União, Brasília, publicado em 6 abr. 2022. Disponível em <link> Acesso em 14 jun. 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	



RESUMO

TELEMARKETING

- Para *telemarketing*, ou mesmo *marketing* postal, a preocupação sobre o uso de dados pessoais decorre da resposta à seguinte pergunta: você sabe quem é a pessoa que recebe o seu contato? Se sim, há certeza de tratamento de dados pessoais e a LGPD precisa ser seguida.
- De preferência, dê opção ao usuário para que ele escolha qual o canal de comunicação preferido (e-mail ou telefone) e respeite essa preferência.
- Observe, ainda, se o número contatado está cadastrado em listas estaduais de “não perturbe”. Em caso positivo, verifique se internamente existe o registro do consentimento daquele titular para que o contato por telefone para fins de *marketing* ocorra. Caso o usuário tenha consentido e, ao mesmo tempo, o seu telefone conste em uma lista de “não perturbe”, diz-se que o consentimento prevalecerá em concreto.
- Por fim, instituições que lidem com *telemarketing* ativo precisam avaliar se há conformidade dessas atividades ao Ato nº 10.413/2021 da ANATEL.

4.7 USO DE IMAGEM, ÁUDIO E VÍDEO: CAMPANHAS, DIVULGAÇÕES E REDES SOCIAIS

Em tempos de redes sociais e de disseminação de equipamentos de fotografia e videogravação, a utilização de imagens, áudios e vídeos para campanhas promocionais de *marketing* é um expediente a mais para divulgar marcas, produtos e serviços. As imagens, áudios e vídeos podem, a depender do contexto utilizado, identificar sujeitos e associá-los a determinados conceitos.

Dessa forma, ao tratar informações de imagem, áudio e vídeo para campanhas de *marketing*, é necessário certificar a não disseminação de que qualquer tipo de tratamento que possibilite a concreta discriminação de gênero, etnia, idade ou preferências políticas, sexuais ou religiosas.

Um primeiro ponto para se considerar com relação aos elementos audiovisuais está na análise acerca de sua natureza. A pergunta a ser feita aqui é a seguinte: é possível, a partir da captura de imagem e vídeo utilizada, identificar qualquer tipo de informação individualmente associada ou associável?

Se uma imagem revela a identidade de sujeitos, pequenos grupos de sujeitos ou qualquer outro tipo de informação que possa ser individualmente associável (ex.: um CPF ou número de matrícula), ela se baseia no tratamento de dados pessoais e deverá seguir as diretrizes abaixo expostas. Caso contrário, se o conteúdo audiovisual utilizado não permite essa identificação individual ou de pequenos grupos de sujeitos, mas é apenas genérico (ex.: uma imagem vertical de multidões ou de locais públicos sem identificação de indivíduos específicos), ele não possui dados pessoais e não

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

precisará seguir as diretrizes da LGPD.

É válido mencionar que o direito de imagem é um dos direitos da personalidade estabelecidos no Capítulo II do Código Civil de 2002, que em seu artigo 18, dispõe que a utilização do nome de uma pessoa para fins comerciais deverá ocorrer somente mediante autorização³⁴.

Assim, ainda antes da vigência da LGPD, o direito à imagem já era resguardado pelo ordenamento jurídico, cabendo ainda pontuar, no tocante à *marketing*, o enunciado da Súmula 403 do STJ³⁵, que estabeleceu que o direito à indenização pela publicação de imagem para fins comerciais sem a devida autorização independe da prova do prejuízo.

Desse modo, para fins de ações *marketing*, uma Instituição de Educacional deverá coletar, preferencialmente, a autorização expressa das pessoas cuja imagem estiver individualmente identificada e vinculada em uma campanha publicitária. Isto poderá ser enquadrado na base legal do consentimento, contida na LGPD, observadas as especificidades da lei, conforme abordado abaixo.



PONTO DE ATENÇÃO

USO DE IMAGENS E A FINALIDADE

- Se, por exemplo, uma campanha de divulgação institucional obtiver o consentimento destacado para uso de imagens de mulheres que integram uma Instituição Educacional com o propósito de homenagens do Dia Internacional da Mulher, as mesmas imagens não poderão ser utilizadas posteriormente fora de contexto, como para associá-las a uma visão político partidária. Qualquer uso descontextualizado implicará em violação à finalidade do consentimento obtido.

Como mencionado, a utilização de imagens ou vídeos de sujeitos ou grupos de sujeitos individualmente identificados ou identificáveis para os fins de *marketing* deverá seguir, conforme aplicação da LGPD, a base legal do consentimento. Ao divulgar campanhas institucionais que empregam de imagens de estudantes ou de colaboradores, uma instituição de ensino deverá obter o consentimento livre, informado, inequívoco, para uma finalidade específica e possibilitada a revogação dos participantes. Para tanto, o consentimento deverá informar o intuito da campanha e o escopo de sua divulgação (*banners*, *websites*, redes sociais, cartazes e outros).

Uma vez obtido o consentimento individual, caso a instituição promotora da estratégia de *marketing* queira utilizar a imagem ou o vídeo em um novo contexto que seja distinto do anterior, o consentimento deverá ser novamente obtido.

³⁴ BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

³⁵ BRASIL. Superior Tribunal de Justiça. Súmula 403, Segunda Seção, julgado em 28/10/2009, DJe 24/11/2009.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Mas qual a melhor forma de se registrar o consentimento? A manifestação do titular poderá ocorrer pela assinatura de termos de autorização de uso e imagem devidamente contextualizados para a LGPD (no [Apêndice 1](#) há um modelo de termo de uso de imagem e voz, adaptável) ou, ainda, por outra forma válida, como vídeos ou autorizações destacadas em formulários eletrônicos.

Vale lembrar, ainda, que o usuário poderá requisitar, a depender das circunstâncias e do tipo de Termo de Cessão de Uso de Imagem celebrado, a remoção do conteúdo veiculado. Portanto, empregue esforços razoáveis no sentido de disponibilizar um canal de contato para que a pessoa veiculada em uma campanha de *marketing* com sua foto e vídeo possa exercer seus direitos previstos na LGPD.

Um último ponto a se tratar aqui, e que não perdeu a validade a partir da LGPD, é o de situações de gravações de conteúdos autorais, como os decorrentes de aulas e eventos com exposição acadêmica. Caso o conteúdo venha a ser veiculado em canais institucionais e/ou redes sociais, ou transcrito e readaptado, a circunstância concreta poderá demandar a assinatura de um Termo de Cessão Onerosa (ou Não Onerosa) de Direitos Autorais Patrimoniais para a veiculação da exposição. Este termo pode ser incorporado ao Termo de Cessão de Uso de Imagem.



RESUMO

MARKETING E O USO DE IMAGEM E VÍDEO

- Para ações de *marketing* com o uso de imagem e vídeo, a preocupação sobre o uso de dados pessoais decorre da resposta à seguinte pergunta: é possível identificar um indivíduo ou grupos de indivíduos a partir dos elementos que compõem o recurso audiovisual? Se sim, há o tratamento de dados pessoais e aplicabilidade da LGPD. Nesses casos, a base legal será o consentimento, que poderá ser dado mediante assinatura de Termo de Autorização ([Apêndice 1](#)).
- Por fim, conteúdos autorais divulgados em eventos acadêmicos podem exigir a cessão onerosa ou não de direitos autorais e patrimoniais. As disponibilizações desses conteúdos em redes sociais devem ser informadas ao titular.

4.8 MARKETING E TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES

O último caso específico para tratar neste Guia é o de tratamento de dados pessoais de crianças e adolescentes para fins de *marketing*. Se a sua instituição fizer o tratamento de dados de menores de 16 anos (ou seja, aqueles que possuem até 15 anos, 11 meses e 29 dias), é recomendada a leitura completa do [Guia de Proteção de Dados Pessoais: Crianças e Adolescentes](#).

Cabe, contudo, pontuar neste guia, que houve recente enunciado proferido pela ANPD acerca da

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

interpretação do artigo 14 da LGPD³⁶. O referido enunciado dispõe que o tratamento de dados pessoais de crianças e adolescentes poderá ocorrer com base nas hipóteses legais previstas no art. 7º ou no art. 11 da LGPD, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da LGPD.

Desse modo, tendo em vista a recente interpretação, é importante que as ações de *marketing* que envolvam menores de 18 (dezoito) anos sejam objeto de consulta ao Encarregado de Proteção de Dados da Instituição Educacional (ou setor/responsável correspondente), a fim de ser observada a base legal mais adequada ao tratamento de dados.

Foram finalizadas as considerações sobre *marketing* e crianças e adolescentes. Este último tópico foi relativamente mais curto devido à existência de um guia sobre o assunto.

5. CONSIDERAÇÕES FINAIS

O presente Guia retratou situações de uso de dados pessoais para fins de *marketing*, com foco em práticas mais recorrentes em Instituições Educacionais. De modo geral, viu-se que o tratamento de dados pessoais – seja por qualquer modo, desde o simples acesso até a edição complexa de dados – em atividades promocionais e de divulgação de marcas, serviços e produtos precisa seguir critérios transparentes, registrados e fundamentados.

Observou-se que a LGPD não veio para inviabilizar as estratégias de *marketing* em tempos de *internet* e redes sociais, mas sim, para estabelecer a forma de utilização dos dados e garantir o direito de seus titulares. Ainda, a observância da qualidade dos dados nas ações de comunicação – que tenham, por exemplo, passado pelo filtro da necessidade e finalidade – trará mais vantagens para o negócio. Ao contrário, o excesso de dados sem propósito, poderá prejudicar a efetividade e o retorno das ações publicitárias promovidas.

Assim, algumas conclusões podem ser retiradas de cada um dos tópicos trabalhados neste Guia. Primeiramente foram destacadas as conclusões sobre as duas principais bases legais ou hipóteses de sustentação para estratégias de *marketing* na LGPD: o interesse legítimo e o consentimento.

A respeito do interesse legítimo, demonstrou-se que essa base legal, sempre que utilizada por uma instituição, deverá seguir um processo documentado de fundamentação. Os requisitos para o interesse legítimo em *marketing* seguem alguns pressupostos: (i) relacionamento prévio entre o titular e a instituição, (ii) legítimas expectativas sobre o conteúdo da comunicação/ação pretendida e

³⁶ BRASIL. Autoridade Nacional de Proteção de Dados. Enunciado CD/ANPD Nº 1, de 22 de maio de 2023. Disponível em: <[link](#)> Acesso em: 29 de mai. de 2023.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

interesses do titular e (iii) respeito a direitos e liberdades fundamentais desse indivíduo.

Sobre o consentimento, trabalhou-se que ele precisa ser livre, informado, inequívoco e possuir uma finalidade determinada, podendo ser revogável pelo titular. Desse modo, é importante que profissionais de comunicação, de direito e de tecnologia empenhem esforços para criar estratégias legalmente adaptadas e criativas para obtê-lo.

Saindo das bases legais e entrando em casos concretos mais regulares para ações de *marketing*, destacou-se situações de relacionamento com *leads*, listas de *e-mail*, uso de ferramentas e novas tecnologias de publicidade, *telemarketing*, *profiling*, *chatbot*, técnicas de *business intelligence* e uso de imagem e vídeo, além de *insights* sobre crianças e adolescentes.

No relacionamento com *leads*, explicou-se que segue uma lógica de funil, em que uma pessoa sem identidade com uma marca específica (*suspect*) é classificada como de potencial interesse (*prospect*) e abordada de maneira direta e planejada (*lead*) com vistas a se tornar um cliente (*customer*). Assim, quanto mais próxima dos dois últimos, maior a probabilidade de que a sua instituição possua um relacionamento mais fundamentado com o titular de dados e, com isso, utilizar a base legal do interesse legítimo.

No relacionamento com clientes e potenciais clientes por listas de contatos, demonstrou-se a ressalva de que o uso de tais listas para *marketing* deve, em caso de compra ou permuta, seguir um processo rigoroso de garantia da origem lícita e de aplicação de uma base legal válida. Em caso de listas criadas pela própria instituição, uma avaliação acerca do controle de qualidade sobre a origem dos endereços e a validação de base legal precisa ser efetuada. Esse processo levará a uma melhora qualitativa de contato com os usuários.

Quanto à utilização de ferramentas de inteligência de negócios, foi ressaltado sobre a necessidade de sempre observar o princípio da necessidade, da segurança e da não-discriminação, além da observância de uma base legal válida (especialmente o interesse legítimo). Assim, estas ferramentas devem ser usadas com parcimônia, sendo preferível o seu uso a partir de dados agregados (quando não é possível identificar os titulares dos dados).

Sobre o *telemarketing* (e também o *marketing* postal), explicou-se que um primeiro ponto de avaliação se dá pela resposta à pergunta: você sabe para quem está ligando ou enviando correspondência? Na hipótese positiva, há uma relação imediata e anterior de tratamento de dados pessoais, de modo que será necessário seguir uma base legal para o tratamento, bem como respeitar as preferências do usuário quanto à autorização e meio de contato, com especial atenção às listas de “não perturbe” e às normas ANATEL, quando aplicáveis.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

No tópico abordando ferramentas e novas tecnologias em ações de *marketing* foi apontado, de modo didático e não exaustivo, alguns exemplos de ferramentas tecnológicas que são utilizadas para rastrear o comportamento de usuários na *internet*, a fim de personalizar e direcionar o conteúdo ao público de interesse. A principal ressalva quanto ao uso dessas tecnologias é garantir a transparência sobre o seu uso e suas finalidades, bem como assegurar o direito dos titulares.

Com relação à prática de criação de perfis ou *profiling*, defendeu-se basicamente o seguinte critério: caso exista tratamento automatizado (ex.: com emprego de algoritmos ou inteligência artificial) para avaliar padrões de comportamento individuais relacionados a um sujeito em concreto, será necessário estar preparado para lidar com pedidos de explicação e revisão das decisões tomadas.

Já quanto ao uso de *chatbots*, baseando-se na classificação por tipo de algoritmo (divididos em simples, inteligentes e híbridos), demonstrou-se que não há grandes riscos com o uso de *chatbots* simples (aqueles que apenas reproduzem informações de uma base fixa, como um Perguntas & Respostas ou FAQ). Contudo, os *chatbots* inteligentes (capazes de analisar padrões de conversação e tomar decisões automatizadas baseadas no tipo de interação) e híbridos (que podem englobar características dos dois dos tipos anteriores) necessitam, de igual modo ao uso do *profiling*, que se esteja preparado para prover os direitos de explicação e de revisão de suas decisões.

Em relação ao uso de imagem e vídeo de pessoas naturais, desenvolveu-se a diferenciação entre imagens e vídeos de *marketing* que retratem pessoas a partir de grandes grupos não identificáveis *versus* pequenos grupos ou sujeitos identificáveis. No caso de identificação concreta de um sujeito ou de possibilidade de identificação, realçou-se que será preciso sua autorização para a participação na campanha, além de respeitar a finalidade para a qual a mesma foi desenvolvida. Ainda, a depender do uso a ser feito da imagem e vídeo, sobretudo em contextos acadêmicos, é necessário um Termo de Cessão de Direitos Autorais.

Sobre dados de crianças e adolescentes, referenciou-se o Guia de Proteção de Dados de Crianças e Adolescentes. Conforme entendimento da ANPD, as bases legais dos artigos 7º e 11 da LGPD poderão ser utilizadas, desde que haja justificativa fundamentada no melhor interesse da criança.

Por fim, espera-se que os conceitos apresentados neste Guia possam contribuir para o aperfeiçoamento das ações de marketing nas Instituições Educacionais. As instituições que utilizarem a LGPD em favor de seus modelos organizacionais, conseguirão atingir verdadeira vantagem competitiva e, ainda, criar relacionamentos qualitativamente mais significativos com seus clientes e com autoridades reguladoras.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

APÊNDICE 1: MODELO DE TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM E VÍDEO – ADAPTADO À LGPD E COM COMENTÁRIOS



TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM E VOZ E CESSÃO DE DIREITOS AUTORAIS PATRIMONIAIS

(I) TITULAR: *[identificação da pessoa natural a qual cederá seus dados para a campanha]*
_____, inscrito no CPF ou RNE/RNM sob o número _____.

(II) AGENTE(S) DE TRATAMENTO: *[instituição responsável por determinar todas as diretrizes de uso dos dados de imagem e voz, via de regra será a sua organização. Se houver mais de um agente de tratamento, e.g.: um controlador e um operador ou dois controladores, é necessário incluir todos aqui, devidamente qualificados como controladores ou operadores]*

[Inserir nome da SUA ORGANIZAÇÃO, unidade (se aplicável), endereço, nome do responsável e e-mail para contato].

(III) DADOS PESSOAIS OBJETO DE TRATAMENTO: *[quais dados serão necessários para a campanha]*

O titular autoriza o(s) Agente(s) de Tratamento identificado(s) na cláusula anterior ao tratamento (coleta, armazenamento, edição e divulgação) dos dados pessoais abaixo listados (**adaptar conforme caso a caso**):

() **Nome**; () **Qualificação ou vínculo com a SUA ORGANIZAÇÃO**; () **Imagem** (foto ou vídeo); () **Voz**; () **Outro(s)** (especificar): _____.

(IV) FINALIDADE(S) DO TRATAMENTO DE DADOS: *[objetivo para o qual os dados pessoais serão usados]:*

(a) Nome ou breve descrição da campanha promocional: _____
(“Iniciativa”);

(b) Os dados pessoais listados acima (cláusula “III”) serão utilizados pela **SUA ORGANIZAÇÃO**, sem qualquer contraprestação financeira ao titular, para fins de promoção da Iniciativa, a qual poderá ser veiculada em todo o território nacional e no exterior, nos seguintes meios (**adaptar conforme caso a caso**):

() Facebook; () Instagram; () LinkedIn; () YouTube; () *websites* da sua Instituição; () *outdoors*, *busdoors*, folders ou folhetos impressos em qualquer meio em geral;

() outros meios (especificar) : _____

(c) Prazo ou previsão de duração da campanha: *[especificar em meses, se não houver prazo certo como para eventos online que permanecerão no YouTube, por exemplo, assinalar “Prazo indeterminado, por se tratar de conteúdo veiculado na web”].*

(V) COMPARTILHAMENTO: *[envio e recebimento de dados por parte de qualquer um dos agentes de*

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

tratamento tendo em vista uma finalidade – se aplicável]

Se necessário, o Controlador fica autorizado a compartilhar os dados pessoais do Titular junto a agências, produtoras e/ou profissionais de produção de foto e vídeo sob o propósito estrito de atender à finalidade descrita no item IV e observados os princípios e direitos firmados pela Lei nº 13.709 [identificar quais entidades casuisticamente, identificar se haverá compartilhamento do conteúdo final com o público, como redes sociais ou outdoors por exemplo];

(VI) SEGURANÇA E DIREITOS DO TITULAR: *[expedientes de proteção e conservação dos dados pessoais a serem seguidos pelos agentes de tratamento, bem como atenção a direitos do titular]*

Durante o processo de elaboração da campanha promocional, o Controlador se compromete a proteger os dados contra qualquer perda ou processamento ilegal tomando as medidas legais e técnicas cabíveis para tanto, bem como a tratar os dados em atenção à finalidade deste Termo.

O titular tem o direito de solicitar ao Controlador o exercício de qualquer dos direitos assegurados na Lei 13.709/2018, sendo a consequência da discordância com este Termo a não vinculação de sua imagem e voz na campanha pretendida. O canal exclusivo para exercício dos direitos do titular em relação ao Controlador é (informar o canal de proteção de dados da sua organização).

(VII) DIREITOS AUTORAIS PATRIMONIAIS: *[informação sobre a cessão gratuita, não onerosa de direitos autorais patrimoniais para exploração e divulgação de conteúdos autorais – se aplicável para exposições autorais, como palestras ou apresentações de trabalho]*

Nos termos da Lei 9.610/1998 e dos tratados internacionais relativos a direitos autorais, **cedo em caráter gratuito permanente** e com a finalidade de divulgação de conteúdos acadêmicos e institucionais os meus **direitos autorais patrimoniais** referentes à exposição oral no evento/peça relacionado, autorizando que SUA ORGANIZAÇÃO reproduza, no todo ou em parte, publicações relativas ao evento, o que inclui a comunicação, edição, reedição, adaptação e distribuição do conteúdo produzido em seus canais e em redes sociais ou por qualquer outro meio disponível.

(VIII) DA AUTORIZAÇÃO: *[declaração de anuência livre, informada e inequívoca com este termo]*

Por estar ciente dos termos acima, manifesto minha autorização para que o Controlador proceda ao processamento de meus dados descritos na cláusula III em atenção às finalidades descritas na cláusula IV e às demais circunstâncias descritas neste Termo. Eu declaro entender que, apesar do Controlador empregar todos os meios para usar meus Dados de acordo com práticas de boa-fé, ele não pode garantir ou ser responsabilizado por usos indevidos de terceiros do material após a sua divulgação.

_____, _____ de _____ de _____ (local, dia, mês e ano).

(Titular de Dados Pessoais ou seu Responsável Legal)

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

APÊNDICE 2: DIRETRIZES PARA FORMULÁRIOS DE INSCRIÇÃO EM EVENTOS, CURSOS E SIMILARES

A realização de eventos, cursos e similares costuma seguir diferentes modelos de acordo com as unidades e instituições parceiras, além de possivelmente variar conforme os sistemas de inscrição utilizados (Ex.: Google Formulários, formulários próprios e outros).

Por esse motivo, em vez de trazer um modelo de formulário de inscrição, o presente apêndice apresenta uma lista de checagem (*checklist*) de 6 (seis) elementos obrigatórios e 4 (quatro) elementos adicionais, os quais indicam conformidade do formulário utilizado em relação às diretrizes da Lei Geral de Proteção de Dados (LGPD):

Certifique-se de listar quais os dados efetivamente serão utilizados;

[Comentário: evite termos genéricos como “o titular autoriza o uso de seus dados”. Prefira nomeá-los, nem que por grupos e, se possível ao caso concreto, dê a opção de escolha ao titular acerca de quais dados deseja compartilhar para fins de evento. O titular pode, por exemplo, desejar ser contatado por e-mail pessoal, mas não desejar ser contatado por telefone. Assim, o ideal é, se possível ao caso, que ele tenha a opção de escolher quais dados autoriza o uso, como e-mails, telefones e redes sociais. Converse com a sua Equipe de tecnologia da informação para ver o que pode ou não ser implementado, pois alguns sistemas possuem especificidades que demandarão ajustes jurídicos na redação de avisos de privacidade]

Evite vincular obrigatoriamente finalidades distintas em uma mesma manifestação de consentimento, se esta for a base legal aplicável;

[Comentário: primeiramente, identifique quais as finalidades você deseja atingir a partir de um evento, curso ou similares. Separe-as e ofereça a opção de concordância a cada uma. Note, por exemplo, que a inscrição em um evento, o recebimento de e-mail marketing e de newsletter são três opções distintas, sendo que estas duas últimas não devem estar acopladas à primeira, sob violação da base legal do consentimento livre, informado e inequívoco];

Evite utilizar *checkboxes* pré-selecionadas, se o consentimento for a base legal aplicável;

[Comentário: o consentimento deve ser inequívoco. A seleção prévia de qualquer checkbox induz um comportamento de consentimento do usuário que não é aceito pela LGPD];

Evite utilizar textos muito longos no corpo da inscrição, especialmente para obter o consentimento;

[Comentário: no contexto da LGPD não é aconselhável apresentar textos longos de anuência, pois fogem ao que se espera do consentimento informado. Portanto, excesso de informação ou o uso de termos vagos fogem ao que se espera do provimento de informações claras e diretas ao usuário. O equilíbrio é importante];

Disponibilize, no sistema de inscrição, um *link* para que o usuário consulte a política/aviso de privacidade e proteção de dados pessoais da sua organização;

[Comentário: se possível, insira um link com o acesso do usuário à política/aviso de privacidade adotado pela sua organização. Esta política provavelmente estará disponível em um portal fixo de proteção de dados da sua organização];

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Disponibilize, no sistema de inscrição, uma opção concreta ou uma instrução para que o usuário se descadastre (opt-out);

[Comentário: ainda que o usuário tenha consentido de forma livre, informada e inequívoca, ele tem o direito de revogar o seu consentimento. Esteja pronto para gerenciar as opções de saída de acordo com o que o Titular indicar. Se a base legal for a do interesse legítimo, tenha em mente de que o direito de oposição também é aplicável];

Se for o caso e a depender do tipo de evento disponibilize, no sistema de inscrição, uma caixa de seleção na qual o usuário declare ter mais de 16 (dezesesseis) anos completos ou, a depender do caso, 18 (dezoito) anos completos;

[Comentário: se necessário incluir menores de 16 anos em determinados eventos, será necessário consultar a Equipe do Encarregado de Proteção de Dados ou área correspondente Leia o Guia de Proteção de Dados Pessoais de Crianças e Adolescentes. Desse modo, se o público infantojuvenil não faz parte da sua estratégia de marketing, pode ser preferível solicitar a confirmação do usuário de que ele possui mais de 16 anos completos];

Se for o caso, disponibilize, no sistema de inscrição, uma descrição ou um link de descrição dos parceiros com quem os dados serão compartilhados para o seu tratamento;

[Comentário: devido à transparência, é importante informar os agentes de tratamento com os quais o compartilhamento é possível. Caso os dados do usuário venham a ser compartilhados com uma outra instituição, pública ou privada, deixe essa informação clara desde o momento inicial sempre que possível];

Se for o caso, certifique-se de que a página de inscrição está em conformidade com os padrões de segurança da informação para receber dados financeiros, como de cartão de crédito;

[Comentário: em situações de produtos ou serviços pagos pelos quais o usuário insira informações como cartões de crédito ou débito diretamente no site da atividade, certifique-se de que os padrões de criptografia, como, por exemplo, certificados digitais e chaves criptográficas AES 256 ou outras mais recentes, se disponíveis, tenham sido implementados em homenagem ao princípio da Segurança];

Se for utilizar incentivos para que o usuário se inscreva em uma base de dados de e-mail ou telefone (como códigos promocionais, clube de descontos ou associações VIP, entre outros), deixe claro qual a finalidade da ação promocional, como os dados serão utilizados e uma opção de opt- out;

[Comentário: no mesmo sentido da finalidade, evite utilizar textos vagos como “preencha este formulário e ganhe um desconto de 10%”. Deixe claro as finalidades do cadastro e disponibilize meios para que o usuário escolha quanto a e-mail marketing, newsletter, SMS entre outras formas de abordagem. Sempre deixe uma alternativa para o usuário se descadastrar do serviço];

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

ANEXO ÚNICO – PERGUNTAS PARA A FERRAMENTA DE AVALIAÇÃO DO INTERESSE LEGÍTIMO (LIA)

Fonte: ICO. Sample LIA Template (Tradução e adaptação livre³⁷ para a LGPD por Jordan Vinícius de Oliveira). Information Commissioner's Office, versão 1.0 recuperada em 09 de outubro de 2020. [Disponível aqui](#). Acesso em: 09 out. 2020.

MODELO PARA AVALIAÇÃO DE LEGÍTIMO INTERESSE – LIA

O presente modelo de Avaliação de Legítimo Interesse (LIA) foi desenhado para ajudá-lo a decidir se o legítimo interesse é a base legal aplicável para a sua atividade de processamento. Ele deve ser utilizado em conjunto com o Guia de Legítimo Interesse [da ICO].

PARTE 1 – TESTE DE FINALIDADE

Você precisa avaliar se há legítimo interesse em relação à atividade de tratamento.

- Por que você deseja tratar o dado?
- Quais benefícios você espera da atividade de tratamento?
- Algum terceiro se beneficiará do tratamento?
- Existe algum benefício público decorrente do tratamento?
- Quão importantes são os benefícios que você identificou?
- Qual seria o impacto se você não pudesse seguir com o tratamento?
- Você está em conformidade em relação a regras de proteção de dados aplicadas à sua atividade de tratamento (e.g.: requerimentos sobre atividades de criação de perfis ou legislações de privacidade na internet)?
- Você está em conformidade em relação a outras leis relevantes?
- Você está conforme com as diretrizes do segmento de mercado do qual faz parte ou com seus códigos de conduta/autorregulamentação aplicáveis?
- Existe algum tipo de problema ético com a atividade de tratamento?

Respostas:

PARTE 2 – TESTE DE NECESSIDADE

Você precisa avaliar se a atividade de tratamento é necessária ao propósito que você identificou.

- A atividade de tratamento o auxiliará a atingir a finalidade pretendida?
- A atividade de tratamento é proporcional a esta finalidade?
- Você pode atingir a mesma finalidade sem o tratamento de dados pessoais?

³⁷ Atenção: à época desta adaptação (09/10/2020) todos os conteúdos veiculados na página da Information Commissioner's Office estavam disponíveis sob a licença livre Open Government Licence (OGL) e permitiam acesso, cópia e adaptações sob as condições de créditos autorais devidamente referenciados. A FGV não se responsabiliza por adaptações feitas sobre este documento que disturbem o seu sentido original. Este modelo carece de adaptações casuísticas para o tipo de atividade da SUA ORGANIZAÇÃO e do setor no qual ela se insere, bem como das orientações que serão feitas pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

- Você pode atingir a mesma finalidade tratando um volume maior de dados ou tratando dados em uma forma menos óbvia ou menos intrusiva?

Respostas:

PARTE 3 – TESTE DE BALANCEAMENTO/PROPORCIONALIDADE

Você precisa considerar o impacto nos interesses, direitos e liberdades dos indivíduos e avaliar se este impacto é capaz de suplantar o seu legítimo interesse.

Primeiro, use o guia [checklist para DPIA](#) [da ICO, DPIA é o acrônimo em inglês para Data Protection Impact Assessment, documento similar, guardadas as devidas proporções, ao Relatório de Impacto à Proteção de Dados Pessoais da LGPD]. No contexto da LGPD, se você se encaixar nos gatilhos daquela checklist, você precisa redigir um relatório de impacto e avaliar riscos de forma detalhada.

3.1 – Natureza do dado pessoal

- Há uso de alguma categoria especial de dados ou de dados relativos a histórico criminal?
- Há uso de dados que as pessoas provavelmente julgaram como particularmente “privados”?
- Você está tratando dados de crianças ou dados relativos a indivíduos vulneráveis?
- Os dados são referentes a pessoas em aspectos concernentes a sua vida pessoal ou a capacidades profissionais?

Respostas:

3.2. Expectativas Razoáveis

- Você possui um relacionamento existente com o indivíduo?
- Qual é a natureza do relacionamento e como você usou estes dados no passado?
- Você coletou dados diretamente do indivíduo? O que você disse a este indivíduo na ocasião?
- Se você obteve dados de terceiros, o que eles disseram aos indivíduos sobre o reuso das informações por terceiros para outros propósitos e, por acaso, isso cobre a sua atividade atual?
- Há quanto tempo você coletou os dados? Existem mudanças na tecnologia ou no contexto de coleta desde aquela época que possam afetar as expectativas dos titulares?
- A sua finalidade pretendida e o seu método são compreensíveis de uma forma geral?
- Você vislumbra fazer algo novo ou inovador com os dados?
- Você possui qualquer evidência sobre as expectativas do titular – e.g.: a partir de pesquisas de mercado, grupos focais ou outras formas de consulta?
- Há quaisquer outros fatores nas circunstâncias particulares que signifiquem que os titulares deveriam ou não deveriam esperar a atividade de tratamento?

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

Respostas:	
3.3. Impacto provável	
<ul style="list-style-type: none"> • Quais são os possíveis impactos à atividade de tratamento nas pessoas? • Os indivíduos perderão qualquer controle sobre o uso de seus dados pessoais? • Qual é a probabilidade e severidade de qualquer impacto potencial? • Alguns indivíduos provavelmente irão se opor ao tratamento ou achá-lo invasivo? • Você se sentiria confortável ao explicar o tratamento aos indivíduos? • Você pode adotar quaisquer salvaguardas para minimizar o impacto do tratamento? 	
Respostas:	
Você pode ofertar aos indivíduos um <i>opt-out</i> (descadastramento)?	SIM / NÃO

Decisão:

Aqui você usará as suas respostas às Partes 1, 2 e 3 para decidir se você poderá aplicar a base do legítimo interesse.

Você pode se apoiar no legítimo interesse para este tratamento?	SIM / NÃO
Você possui quaisquer comentários para justificar a sua resposta? (opcional)	
LIA elaborado por	
Data	

Mantenha o registro deste LIA e revise-o sempre que necessário. Elabore um DPIA se necessário. Inclua detalhes de seus propósitos e bases legais para tratamento em seus documentos de privacidade, incluindo uma entrada para o seu legítimo interesse.

GUIA DE PROTEÇÃO DE DADOS PESSOAIS: CC.04.003.2023	DATA DA APROVAÇÃO: 04/10/2023	APROVADOR: JORDAN VINÍCIUS DE OLIVEIRA
CATEGORIA DO ASSUNTO: CONTROLE E CONFORMIDADE	ASSUNTO: PROTEÇÃO DE DADOS PESSOAIS	

