Selma Carloto
Autora

GUIA DE CONSENTIMENTO COMO HIPÓTESE LEGAL DE TRATAMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

REALIZAÇÃO

CENTRO DE PESQUISAS JUDICIAIS DA AMB

AMB Associação dos Magistrados Brasileiros

ANPT ASSOCIAÇÃO NACIONAL DOS PROCURADORES E DAS PROCURADORAS DO TRABALHO

INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

PPG DIREITO UFRGS UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

Luciane Cardoso Barzotto
Supervisora

LTr

Elaboração: Selma Carloto

Supervisão: Luciane Cardoso Barzotto

Revisão Sonia Bramante

Capa e Elementos Gráficos: Danilo Rebello

Diagramação: RLUX

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Carloto, Selma
Guia de consentimento como hipótese legal de tratamento da lei geral de proteção de dados (LGPD) [livro eletrônico] / Selma Carloto. – São Paulo : Ltr Editora, 2024.
PDF

Bibliografia.
ISBN 978-65-5883-318-5

1. Proteção de dados – Direito – Brasil
2. Proteção de dados – Legislação – Brasil
I. Título.

24-216223 CDU – 342.721(81)

Índice para catálogo sistemático:

1. Brasil : Proteção de dados pessoais : Direito 342.721(81)

Eliane de Freitas Leite – Bibliotecaria – CRB 8/8415

Dedicamos este trabalho às vítimas das devastadoras enchentes que assolaram o Rio Grande do Sul em 2024. Que este guia sirva como um testemunho de nossa solidariedade e um lembrete da importância de políticas eficazes e da união em momentos mais difíceis como este.

Este guia analisa detalhadamente as peculiaridades do consentimento enquanto hipótese legal para o tratamento de dados pessoais e sensíveis, destacando-se em um contexto de notáveis avanços tecnológicos. Elaborado pela Professora Selma Carloto durante seu pós-doutorado na Universidade Federal do Rio Grande do Sul (UFRGS), com a supervisão da Professora Luciane Cardoso Barzotto, o documento oferece uma exposição aprofundada e clara sobre o consentimento como base legal para o tratamento de dados pessoais, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD).

Integrando a experiência e pesquisa desenvolvidas na União Europeia, especialmente as diretrizes do Grupo de Trabalho do Art. 29 e do Comitê Europeu de Proteção de Dados, o guia simplifica o consentimento como hipótese legal de tratamento, caracterizado por ser uma manifestação livre, informada e inequívoca. Além da sólida base teórica, o texto ilustra com exemplos práticos como o consentimento deve ser corretamente obtido, documentado e aplicado, enfatizando sua importância fundamental na proteção dos direitos à privacidade em diversos contextos, em meios físicos e digitais.

Sumário

Objetivo do Guia

Este guia foca na análise detalhada do consentimento como uma manifestação **livre, informada e inequívoca**, explorando sua aplicação em diversos contextos. Com uma abordagem acadêmica rigorosa, este trabalho explora a intersecção entre a Lei Geral de Proteção de Dados (LGPD) do Brasil e as regulamentações e diretrizes da União Europeia. O objetivo é **esclarecer as complexidades e especificidades legais que definem este conceito,** demonstrando, por meio de exemplos práticos e boas práticas, além de guias e outras orientações da Autoridade Nacional de Proteção de Dados (ANPD) do Brasil e diretrizes e pareceres da União Europeia, como o consentimento é interpretado e implementado.

Conteúdo

Este guia aborda a complexidade do consentimento conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD) do Brasil, um tema essencial para operadores do direito e profissionais envolvidos na proteção de dados pessoais. O texto começa com uma definição precisa de consentimento, explora os direitos do titular relacionados a esse conceito e discute as finalidades específicas que justificam sua coleta e tratamento segundo a legislação.

Explora as nuances que tornam o consentimento livre, destacando a importância de uma escolha autônoma, desvinculada de qualquer forma de coação ou influência indevida. O texto avança ao detalhar o que constitui um consentimento informado, sublinhando a necessidade de clareza e acessibilidade das informações fornecidas aos titulares dos dados.

Prossegue com a discussão sobre o consentimento inequívoco, enfatizando como a manifestação de vontade deve ser inequívoca e clara. A granularidade é outro ponto tratado, explicando como o consentimento deve ser dado com detalhamento suficiente para cada uso específico dos dados.

Além disso, o guia examina o desequilíbrio de poder em relações assimétricas, reconhecendo situações em que a posição vulnerável do titular dos dados pode afetar a liberdade de seu consentimento. Seguindo esta linha, aborda o consentimento para o tratamento de dados pessoais sensíveis e de crianças e adolescentes, categorias que exigem atenções especiais devido à sua sensibilidade e aos riscos envolvidos.

Ao oferecer uma visão compreensiva desses tópicos, o guia serve como um recurso para aprofundar o entendimento e a aplicação prática dos aspectos legais do consentimento sob a LGPD, proporcionando orientações fundamentais para garantir que os processos de coleta e tratamento de dados estejam em conformidade com os requisitos legais e éticos.

Introdução

A preeminência das normativas europeias em proteção de dados pessoais é amplamente reconhecida, refletindo a liderança e influência significativa que a União Europeia exerce neste domínio. Essa liderança europeia tem catalisado uma reavaliação e recalibração das políticas de proteção de dados ao redor do mundo, em um movimento rumo à harmonização legislativa. Lima e Peroli (2020) descrevem este fenômeno como a "europeização" da regulamentação de dados pessoais, evidenciando como as diretivas europeias transcendem suas fronteiras originais. Caldeira (2019) reitera a influência substancial dessas normativas no contexto internacional, sublinhando seu impacto na evolução das legislações de proteção de dados em outras jurisdições, incluindo o Brasil, que tem buscado alinhar suas práticas aos padrões europeus.

Com a ascensão da era digital, emergem desafios notáveis na proteção de dados pessoais, onde a Lei Geral de Proteção de Dados (LGPD) do Brasil e o Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia se apresentam como marcos regulatórios essenciais. Essas legislações enfatizam a necessidade de uma manifestação de consentimento que seja livre, informada e inequívoca. O saudoso professor Doneda (2011) observa que, na Sociedade da Informação, os dados pessoais tornam-se fundamentais, substituindo muitas vezes a necessidade da presença física e permitindo às pessoas maior autonomia e liberdade. No entanto, ele adverte sobre os riscos inerentes ao tratamento desses dados, que incluem a exposição a usos indevidos ou abusivos, representação incorreta dos titulares dos dados e a possibilidade de acesso por terceiros sem o consentimento adequado. Diante desses riscos, Doneda (2011) ressalta a importância de se estabelecer mecanismos que assegurem aos indivíduos o controle sobre seus próprios dados, que são uma extensão direta de suas personalidades e, por extensão, um aspecto crítico de sua privacidade e dignidade individual. Assim, a proteção de dados pessoais não apenas salvaguarda a privacidade, mas também se configura como um direito fundamental, essencial para a proteção da pessoa humana.

Barzotto, Miskulin e Breda (2020) enfatizam a relevância da subordinação em relações assimétricas, um fenômeno tradicionalmente associado ao contexto laboral, mas que no contexto de privacidade e proteção de dados se estende a diversas outras relações, incluindo as interações sob o domínio do poder público. Em um cenário digital em constante evolução, a dinâmica de subordinação exige uma abordagem adaptativa que promova a progressão para uma compensação que busque corrigir distorções e tornar os direitos mais efetivos.

Essa evolução é particularmente essencial no que tange à hipótese legal consentimento e sua correta aplicação para a salvaguarda dos direitos fundamentais de todas as partes envolvidas. Essa abordagem não apenas fortalece o caráter humanizador da legislação, mas também a destaca como um elemento defensivo chave contra os riscos e desafios exacerbados no ambiente digital atual.

Esta visão é corroborada pelas reflexões de De Lucca e Queiroz (2023), que, em um capítulo da obra "Inteligência Artificial e Novas Tecnologias nas Relações de Trabalho", exploram como as ondas da tecnologia da informação têm reconfigurado a estrutura da sociedade moderna. Eles observam que o impacto transformador da tecnologia é incontestável, destacando-se a popularização da internet que, ao ampliar exponencialmente o número de usuários conectados, aumentou também o volume de dados coletados e a criação de vastos repositórios de informações. Esta nova realidade digital não apenas reformula comportamentos individuais, mas também redefine os contornos de sistemas sociais e econômicos, particularmente no que tange à coleta, armazenamento e uso de dados pessoais (DE LUCCA; QUEIROZ, 2023).

Em complemento, De Lucca e Queiroz (2023) argumentam que as questões de privacidade e proteção de dados pessoais têm ganhado complexidade e relevância diante do aumento do uso de plataformas digitais. Essa transformação modificou a percepção tradicional de vigilância, agora focada nos dados pessoais que se tornaram ativos essenciais nas atividades econômicas e alimentam uma economia orientada por dados. A proteção de dados pessoais está evoluindo para desempenhar um papel significativamente positivo no potencial de comunicação e interação entre os indivíduos. Esta evolução reflete a mudança no ambiente de circulação de dados,

onde os interesses na proteção dos dados pessoais estão cada vez mais evidentes, culminando na caracterização dos dados pessoais como um direito fundamental, conforme estabelecido pela Emenda Constitucional n. 115/2022 (DE LUCCA; QUEIROZ, 2023).

Refletindo sobre as profundas transformações na gestão de dados pessoais e pessoais sensíveis que demandam proteção qualificada e os novos desafios destacados pelos autores mencionados anteriormente, percebe-se a necessidade de normas robustas e bem definidas para a proteção desses dados. A LGPD do Brasil atende a essas exigências, posicionando o consentimento do titular como um elemento central em sua estrutura regulatória. Importante ressaltar, no entanto, que o consentimento é apenas uma das hipóteses legais para o tratamento de dados, mas não a única, sendo necessário cumprir requisitos específicos para sua validade. A Seção 1 deste guia explora os aspectos essenciais do consentimento sob a ótica da LGPD, ancorado nos arts. 5º., 8º. e 18, para oferecer um entendimento aprofundado sobre como o consentimento deve ser obtido, tratado e gerenciado, garantindo assim a proteção dos direitos fundamentais de liberdade e de privacidade.

1. CONSENTIMENTO NA LGPD: FUNDAMENTOS PARA A PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018, estabelece diretrizes fundamentais para a proteção de dados pessoais no Brasil. Esta seção visa esclarecer os aspectos fundamentais do consentimento sob a ótica da LGPD, ancorando-se nos arts. 5º., 8º. e 18, para oferecer um entendimento aprofundado sobre como o consentimento deve ser obtido, tratado e gerenciado, assegurando a proteção dos direitos fundamentais de liberdade e de privacidade.

1.1. Definição de Consentimento

A LGPD define o consentimento, conforme estipulado em seu art. 5º., XII, como a "**manifestação livre, informada e inequívoca**" pela qual o titular dos dados concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018). Este conceito é fundamental para esta hipótese legal que legitima muitos tratamentos de dados pessoais, sublinhando a importância da autonomia do titular sobre suas informações pessoais.

Os três aspectos essenciais do consentimento, conforme delineados pela LGPD e que serão aprofundados em seções próprias, são:

Livre: o consentimento deve ser expresso voluntariamente pelo titular, sem qualquer tipo de coação ou influência indevida. A livre escolha garante que o titular tenha real autonomia na decisão, assegurando que o consentimento seja uma manifestação genuína de vontade.

Informada: o titular deve receber informações claras e completas sobre o tratamento a que seus dados serão submetidos antes de dar seu consentimento. Isso inclui compreender quem está coletando os dados, quais dados estão sendo coletados, por que estão sendo coletados e como serão utilizados.

Inequívoca: o consentimento exige uma declaração clara ou um ato positivo inequívoco que indique a aprovação do titular ao tratamento de seus dados. Ações afirmativas claras, como marcar uma caixa em uma interface digital ou escolher configurações específicas em aplicativos ou serviços *online*, são exemplos de como o consentimento inequívoco pode ser expresso.

O art. 8º. da LGPD detalha ainda mais os requisitos e procedimentos para a obtenção de consentimento:

> Art. 8º. da LGPD: O consentimento previsto no inciso I do art. 7º. desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei.
>
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º. desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração. (BRASIL, 2018)

O art. 8º. da LGPD estabelece diretrizes específicas para a obtenção do consentimento, detalhando os requisitos que devem ser cumpridos para que o consentimento seja considerado válido. Cada parágrafo deste artigo desempenha um papel fundamental na definição de como o consentimento deve ser coletado, tratado e, se necessário, revogado. Abaixo, exploramos cada um destes parágrafos de forma detalhada:

1.2. Destaque do Consentimento

O art. 8º., § 1º da LGPD, estipula que, quando o consentimento for fornecido por escrito, este deve ser destacado das demais cláusulas contratuais. Esta disposição

legal tem como objetivo assegurar que o titular dos dados compreenda claramente o consentimento que está sendo solicitado, evitando que tal autorização se dilua entre outras disposições contratuais. A clareza e o destaque são vitais para garantir que a decisão do titular dos dados seja verdadeiramente informada e voluntária.

A cláusula de destaque não é apenas uma formalidade, mas uma exigência essencial para proteger os titulares de dados. Esse mecanismo assegura que o consentimento se destaque visualmente, facilitando a sua identificação rápida e eficaz pelo titular, que muitas vezes é confrontado com extensos termos e condições. Isso é essencial, especialmente considerando que o consentimento deve ser uma manifestação livre, informada e inequívoca da vontade do titular.

Para cumprir com essa exigência da LGPD, as empresas poderão:

a – Empregar formatos visuais distintos, como fontes em negrito, itálico ou cores diferenciadas para a cláusula de consentimento.

b – Separar fisicamente a cláusula de consentimento das demais cláusulas contratuais, garantindo que ela seja imediatamente visível ao revisar o documento.

Ao mesmo tempo é importante fornecer explicações simplificadas e diretas sobre as implicações do consentimento dentro da cláusula destacada, evitando o uso de vocabulário técnico ou jurídico excessivamente complicado. A linguagem precisa ser clara e simples para o entendimento de qualquer um.

A exigência de destaque do consentimento em contratos escritos é uma salvaguarda fundamental para a autonomia e a proteção dos direitos dos titulares de dados pessoais. Ao implementar práticas que enfatizem a transparência e a clareza, as organizações não só cumprem com a legislação, mas também fomentam um ambiente de confiança e respeito pela privacidade dos indivíduos.

1.3. Ônus da Prova

O § 2º do art. 8º. da LGPD atribui ao controlador uma responsabilidade essencial: demonstrar que o consentimento foi obtido em conformidade com a le-

gislação. Esta disposição sublinha a necessidade de transparência e diligência no processo de coleta de consentimento, garantindo que este seja realizado de maneira livre, informada e inequívoca. Para atender a essa exigência, é essencial que o controlador adote práticas rigorosas de documentação.

É fundamental implementar um sistema de gestão de consentimentos que registre criteriosamente o contexto de cada consentimento obtido, incluindo data, horário, método utilizado e a versão específica do texto aceito pelo titular. Esses registros devem ser mantidos em um formato que possa ser facilmente auditado, garantindo que todas as informações possam ser verificadas de forma eficiente e confiável, sempre que necessário.

Em conclusão, o ônus da prova, que recai sobre o controlador, é um elemento essencial da LGPD, destinado a proteger os direitos dos titulares dos dados e promover práticas responsáveis no tratamento de dados. Este requisito não apenas fortalece a confiança dos titulares nos processos de coleta de dados, mas também impulsiona a adoção de medidas de *compliance* mais rigorosas por parte das organizações.

1.4. Da Proibição do Consentimento Viciado

O art. 8º., § 3º, da LGPD estabelece a proibição explícita do tratamento de dados pessoais com base no consentimento obtido por meios ilícitos ou viciados. Esta norma sublinha a importância de um processo de coleta de consentimento que seja livre de coação, engano ou manipulação.

O consentimento viciado pode manifestar-se de diversas formas, incluindo a obtenção de consentimento sob falsas pretensões, o uso de linguagem complicada que confunda o titular, ou a imposição de condições que efetivamente forcem o titular a consentir. A responsabilidade recai sobre o controlador para provar que o consentimento foi obtido de forma legítima e em total conformidade com a lei. O não cumprimento dessa obrigação pode resultar em severas penalidades regulatórias, além de comprometer a confiança do titular dos dados e prejudicar a imagem da organização. É essencial que os controladores implementem práticas rigorosas de verificação e manutenção de registros, para garantir e demonstrar a integridade de todo o processo de consentimento.

1.5. Finalidades Determinadas

O § 4º do art. 8º. da LGPD impõe uma condição clara e estrita para a validade do consentimento: ele deve ser concedido para finalidades determinadas. Isso significa que o consentimento não pode ser vago nem abrangente; deve haver uma delimitação precisa dos objetivos para os quais os dados pessoais serão utilizados. Esta exigência legal assegura que o titular dos dados está plenamente ciente e concorda especificamente com cada contexto de tratamento de seus dados, reforçando a noção de que o consentimento deve ser uma manifestação de vontade previamente informada e deliberada.

Ao invalidar autorizações genéricas, a LGPD promove uma maior responsabilidade e transparência por parte dos controladores de dados. Eles são obrigados a especificar claramente as finalidades do tratamento ao solicitar o consentimento, garantindo que os titulares possam fazer uma escolha sobre uma finalidade determinada e previamente informada sobre o uso de suas informações pessoais. Esta abordagem não só protege a privacidade e a autonomia dos indivíduos, mas também estabelece uma base de confiança mais sólida entre os titulares de dados pessoais e as entidades que os manuseiam, facilitando uma relação mais clara e justa.

A LGPD impõe requisitos estritos para a validade do consentimento, enfatizando especialmente a necessidade de este ser concedido para finalidades bem definidas. Isso visa garantir que os titulares dos dados estejam plenamente cientes das razões pelas quais seus dados estão sendo coletados e concordem com elas. A seguir, apresentarei um exemplo prático que destaca a importância de estabelecer e comunicar finalidades determinadas no processo de coleta de consentimento, conforme a LGPD. Este exemplo ajudará a ilustrar como os controladores de dados podem implementar esse requisito na prática, respeitando assim tanto a legislação quanto a autonomia dos indivíduos.

EXEMPLO 1: Rede de supermercados

Uma rede de supermercados implementa um aplicativo móvel visando aprimorar a experiência de compra dos seus clientes e no momento do registro no aplicativo

planeja coletar dados pessoais dos usuários para finalidades determinadas. Segundo o § 4º do art. 8º. da LGPD, é mandatório que a rede de supermercados especifique com clareza as finalidades para as quais o consentimento é solicitado.

Por exemplo, uma rede de supermercados poderia em seu site ou em um aplicativo elencar as seguintes finalidades para o uso dos dados com consentimento:

> A – Personalização de Ofertas: tratar os dados de compras anteriores para fornecer ofertas personalizadas futuras e que se alinhem com as preferências e padrões de consumo do titular.
>
> B – Comunicações de Marketing: utilizar canais de comunicação como e-mail ou notificações no aplicativo para informar os usuários sobre campanhas promocionais e eventos, sempre condicionado ao consentimento prévio do titular para tais comunicações.
>
> C – Análises de Mercado: tratar dados de compras para realizar análises detalhadas sobre as tendências de consumo, visando otimizar a gestão de estoque, assim como a diversidade de produtos oferecidos.

Para cada finalidade, é imperativo que sejam proporcionadas previamente explicações transparentes e claras e que o usuário tenha a opção de consentir de forma independente para cada finalidade determinada. Ademais, é fundamental que a rede de supermercados facilite o procedimento para que os usuários possam revogar seu consentimento em qualquer momento, seja por meio das configurações do aplicativo ou por meio de contato direto com a empresa.

1.6. Direito de Revogação

O direito de revogação do consentimento, estipulado no art. 8º., § 5º da Lei Geral de Proteção de Dados Pessoais (LGPD), é uma salvaguarda crítica que sublinha a autonomia do titular dos dados. Este dispositivo legal permite que o titular retire seu consentimento a qualquer momento, assegurando que o processo seja simples, gratuito e acessível. Essa facilidade de revogação garante que os titulares possam

reavaliar e alterar suas decisões em relação ao tratamento de seus dados pessoais conforme mudanças nas suas perspectivas ou nas práticas do controlador.

A implementação prática do direito de revogar o consentimento exige que os controladores disponibilizem mecanismos eficientes e claros. Sistemas *online*, por exemplo, devem oferecer opções facilmente acessíveis e compreensíveis para que os usuários possam retirar seu consentimento. Isso pode incluir configurações de privacidade intuitivas ou links diretos para a revogação. É fundamental que os controladores comuniquem transparentemente como os usuários podem proceder para revogar o consentimento, detalhando quaisquer consequências relacionadas a essa ação. Após a revogação, é imperativo cessar prontamente o tratamento dos dados e informar o titular sobre a conclusão do processo.

O art. 18, inciso IX da LGPD é fundamental ao reforçar o direito de revogação do consentimento, estabelecendo que essa revogação deve ser facilitada e evidenciando a obrigação do controlador de respeitar a decisão do titular sem impor quaisquer penalidades. Esse inciso destaca o compromisso da legislação com a proteção dos direitos dos titulares de dados, enfatizando a importância de adaptabilidade em um ambiente digital em constante evolução, onde as condições de tratamento de dados frequentemente mudam. Além disso, é essencial lembrar que, apesar de frequentemente associada ao ambiente digital, a LGPD também se aplica a contextos que envolvem o tratamento de dados em meios físicos.

A relevância do direito de revogação se torna ainda mais significativa em um contexto em que as políticas de privacidade das empresas e as tecnologias utilizadas podem evoluir de forma acelerada. Permitir que os titulares de dados retirem seu consentimento lhes oferece a capacidade de responder a essas mudanças, seja por novos riscos emergentes associados a novas tecnologias ou por uma mudança na perspectiva pessoal sobre sua privacidade e segurança. Dessa forma, o direito de revogação atua como um elemento fundamental para manter o equilíbrio dinâmico entre os interesses dos controladores e os direitos dos titulares, reforçando a importância da confiança e da autonomia na gestão de dados pessoais na era digital.

1.7. Alteração das Condições Informadas

Finalmente, o art. 8º., § 6º determina que qualquer alteração nas condições informadas ao titular sobre o tratamento de seus dados deve ser claramente comunicada. Isso permite que o titular avalie as mudanças de tratamento e, caso discorde, possa revogar seu consentimento. Esta disposição garante transparência e mantém o titular informado e envolvido no processo de tratamento de seus dados.

Conclusão da seção

Esta seção proporcionou uma análise detalhada do art. 8º. da LGPD, que é fundamental para a compreensão e implementação prática dos requisitos legais relacionados ao consentimento na proteção de dados pessoais. O art. 8º. detalha o processo de obtenção de consentimento, sublinhando a importância de um consentimento que seja claramente documentado, seja por escrito ou por outro meio que demonstre inequivocamente a manifestação de vontade livre do titular dos dados.

Ele reitera a responsabilidade do controlador de provar que o consentimento foi obtido em conformidade com a lei, destacando o ônus da prova como um elemento essencial para a prática de governança de dados. O artigo também proíbe expressamente o tratamento de dados baseado em consentimento obtido por meio ilícito, reforçando a necessidade de integridade e legitimidade no processo de coleta de consentimento. Além disso, enfatiza o direito do titular de revogar o consentimento a qualquer momento e sem quaisquer penalidades, consolidando o compromisso da LGPD com a proteção dos direitos dos titulares.

Essas disposições garantem que os titulares dos dados estejam plenamente informados e possam exercer seu direito à autodeterminação informativa, enquanto impõem aos controladores um rigoroso padrão de transparência e responsabilidade no tratamento de dados pessoais e pessoais sensíveis.

2. DIREITOS DO TITULAR RELACIONADOS AO CONSENTIMENTO

Em um mundo cada vez mais digitalizado, a interação entre privacidade e tecnologia desafia constantemente os limites da legislação e da ética. A necessidade de proteger informações pessoais enquanto se permite a inovação e a utilidade dos dados é um equilíbrio delicado. A LGPD busca estabelecer esse equilíbrio, conferindo direitos aos indivíduos para controlar como seus dados pessoais são coletados, usados e compartilhados. Entre esses direitos, os relacionados ao consentimento são particularmente essenciais neste guia e fundamentam a autonomia do titular em relação aos seus dados.

> Art. 18 O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
>
> I – confirmação da existência de tratamento;
>
> II – acesso aos dados;
>
> III – correção de dados incompletos, inexatos ou desatualizados;
>
> IV – Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
>
> **VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;**
>
> VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
>
> **VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;**
>
> **IX – revogação do consentimento, nos termos do § 5º do art. 8º. desta Lei. (BRASIL, 2018)**

Esta seção focará especificamente nos incisos VI, VIII e IX do art. 18 da LGPD, explorando como esses direitos permitem que os titulares de dados gerenciem

proativamente seu consentimento e participem ativamente nas decisões sobre o uso de suas informações pessoais. Essa análise detalhada visa proporcionar um entendimento claro de como a legislação empodera os indivíduos, permitindo-lhes exercer seus direitos de maneira eficaz e informada, o que é fundamental para a manutenção de sua dignidade e liberdade na sociedade digital.

2.1. Direito de Não Fornecer Consentimento e Consequências da Negativa (art. 18, inciso VIII da LGPD)

O art. 18, inciso VIII da LGPD garante ao titular dos dados pessoais o direito de ser informado sobre a possibilidade de não fornecer consentimento, bem como sobre as consequências de sua negativa. Este direito é essencial para assegurar que o consentimento seja uma manifestação de vontade genuinamente livre, permitindo uma decisão verdadeiramente informada.

Por exemplo, no contexto de uma matrícula *online* em uma universidade pública, os novos estudantes são requisitados a fornecer dados pessoais. Se a universidade condiciona a continuação do processo de matrícula ao consentimento para finalidades genericamente descritas, como para "fins educacionais e outros correlatos", e não oferece alternativas viáveis para os estudantes que optem por não fornecer consentimento, tal prática viola a LGPD. O consentimento, neste caso, não seria considerado livre, pois estaria atrelado à realização de uma matrícula, um serviço essencial que não deveria depender da concessão de consentimento para finalidades adicionais.

É essencial que o titular seja claramente informado de que a negativa em fornecer consentimento não impede o acesso a serviços básicos e necessários. A universidade deveria, portanto, proporcionar uma opção clara que permitisse ao estudante prosseguir com sua matrícula sem conceder consentimento para o uso de seus dados além do estritamente necessário. Além disso, conforme afirma a ANPD (2023) no exemplo, a hipótese legal de tratamento não seria consentimento, já que o tratamento de dados pessoais é obrigatório sem a possibilidade de uma efetiva escolha do titular.

Adicionalmente, o art. 18, inciso VIII da LGPD assegura que o titular dos dados tem o direito de ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências dessa negativa. Neste cenário, a universidade não cumpriria com a exigência de proporcionar alternativas que permitissem ao estudante completar sua matrícula sem conceder consentimento para usos adicionais de seus dados, que ultrapassem o necessário para a realização da matrícula e para ter acesso a serviços essenciais. A falta de alternativas coerentes colocaria os estudantes em uma posição de vulnerabilidade, onde não poderiam exercer livremente sua escolha, contrariando a LGPD.

> Universidade pública solicita de novos estudantes o fornecimento de dados pessoais necessários para fins de cadastro e matrícula. O procedimento é realizado *online* e, para prosseguir para as etapas seguintes, com a escolha de disciplinas e horários, o estudante deve "aceitar" as condições estipuladas para o tratamento de seus dados. Essas condições são descritas de forma genérica, com a indicação de que os dados poderão ser utilizados para "fins educacionais e outros correlatos". Uma mensagem indica que, caso não fornecido o consentimento, a matrícula não será concluída e o estudante não terá acesso ao curso e a serviços como os de assistência estudantil e empréstimo de livros na biblioteca. (...) No exemplo citado, o consentimento eventualmente obtido será nulo, pois: (i) os estudantes não possuem condições efetivas de aceitar ou recusar o tratamento de seus dados pessoais, haja vista o caráter compulsório do tratamento realizado pela universidade; e (ii) a autorização é fornecida para uma finalidade genérica. Com o objetivo de adequar as suas práticas ao disposto na LGPD, a universidade deve fornecer informações claras e precisas sobre a finalidade específica do tratamento, identificando outra base legal mais apropriada para a hipótese, que não o consentimento. Ainda, em atenção ao princípio da necessidade, não devem ser solicitados mais dados do que o necessário para atingir as finalidades informadas ao titular. (ANPD, 2021, p. 13).

Conforme apontado pela ANPD, no exemplo citado, a universidade deve revisar suas práticas para alinhar-se com a legislação, especificando claramente as finalidades para as quais os dados são coletados e tratados, e explorando bases legais mais adequadas que não dependam exclusivamente do consentimento dos titulares dos

dados. Esta abordagem não só garantiria a conformidade com a LGPD, mas também reforçaria o respeito pelo princípio da necessidade, limitando a coleta de dados ao estritamente necessário para atingir os objetivos claramente definidos e comunicados aos titulares dos dados.

Sempre que o tratamento é obrigatório e não há possibilidade de dar liberdade de escolha ao titular do tratamento de seus dados para uma finalidade, o consentimento não será a hipótese legal de tratamento.

2.2. Revogação do Consentimento (art. 18, inciso IX da LGPD)

A revogação do consentimento é um direito fundamental que reforça a autonomia e o controle do titular sobre seus dados pessoais. A LGPD estipula que o titular pode retirar seu consentimento a qualquer momento, um processo que deve ser tão fácil quanto foi a concessão. Este direito é vital porque permite que o titular responda a mudanças nas circunstâncias pessoais ou no ambiente regulatório, além de refletir a possibilidade de mudanças na própria forma como as empresas tratam os dados pessoais.

Essencialmente, a revogação não é apenas um mecanismo de controle, mas também pode se manifestar como uma expressão de insatisfação do titular da forma como o controlador está lidando com os seus dados pessoais. Portanto, a capacidade de retirar o consentimento de forma simples e direta reforça a posição do titular como agente ativo na gestão de seus dados pessoais.

2.3. Direito à Eliminação dos Dados Tratados com Consentimento (art. 18, inciso VI da LGPD)

Além do direito de revogar o consentimento, o titular dos dados tem o direito à eliminação dos dados pessoais tratados com base no consentimento anteriormente concedido. Este direito, estipulado no inciso VI, art. 18 da LGPD, assegura que, uma vez revogado o consentimento, o titular pode exigir que seus dados sejam apagados, salvo algumas exceções legais previstas no art. 16 da LGPD.

> Art. 16 da LGPD. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
>
> I – cumprimento de obrigação legal ou regulatória pelo controlador;
>
> II – estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> III – transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
>
> IV – uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2022)

Este mecanismo é importante para a garantia de que os dados não continuem a ser usados uma vez que o fundamento legal para seu tratamento (o consentimento) não exista mais. A eliminação dos dados é uma extensão natural da revogação do consentimento, proporcionando ao titular a certeza de que suas informações não serão mantidas indevidamente após a retirada do consentimento. Este direito é especialmente relevante em cenários onde a confiança entre o titular e o controlador é comprometida ou quando o titular reconsidera os potenciais riscos e benefícios de ter seus dados tratados.

Juntos, os direitos de revogação do consentimento e a eliminação de dados pessoais formam uma estrutura robusta que empodera os indivíduos, permitindo-lhes exercer controle substancial sobre como suas informações pessoais são gerenciadas ao longo do tempo. Esses direitos asseguram que as escolhas do titular sobre sua privacidade sejam respeitadas e cumpridas de forma eficaz.

3. MANIFESTAÇÃO LIVRE, INFORMADA E INEQUÍVOCA

A complexidade do consentimento como base legal para o tratamento de dados pessoais é detalhadamente explorada pela LGPD, que enfatiza três qualidades fundamentais que o consentimento deve possuir para ser considerado válido: ser uma manifestação livre, informada e inequívoca. Esta seção se dedica a aprofundar o entendimento dessas características essenciais, abordando cada uma delas detalhadamente e separadamente para ilustrar como devem ser integralmente aplicadas para garantir a proteção efetiva dos direitos dos titulares dos dados. A relevância deste tema reside não apenas na conformidade legal, mas também na construção de uma relação de confiança entre titulares de dados e controladores, elemento essencial para a sustentabilidade das atividades que dependem do tratamento de dados pessoais.

3.1. Manifestação Livre

De acordo com o "Manual da Legislação Europeia sobre Proteção de Dados" (Edição de 2018), o consentimento para o tratamento de dados pessoais deve ser um ato claro e positivo, que reflete uma vontade livre, específica, informada e inequívoca do titular dos dados. Este ato pode se manifestar tanto por meio de uma declaração quanto por uma ação deliberada do titular. É essencial destacar que o titular tem o direito de retirar seu consentimento em qualquer momento, e, nos casos em que as declarações escritas abordem também outros temas, os pedidos de consentimento devem ser claramente destacados e redigidos em linguagem simples, separados de outras matérias para garantir maior clareza. A validade do consentimento, conforme a legislação de proteção de dados, depende da aderência a todos esses requisitos, sendo responsabilidade do controlador demonstrar que o consentimento foi obtido validamente.

A necessidade de um consentimento claro e positivo é particularmente crítica em situações de desequilíbrio de poder, como no ambiente de trabalho. Nesses contextos, é fundamental que o consentimento seja obtido sem qualquer coação ou pressão, assegurando que a escolha do titular seja autêntica e não influenciada indevidamente. Carloto (2023) salienta a importância do consentimento verdadeiramente livre no tratamento de dados pessoais, afirmando que o titular deve ter total liberdade para escolher quais dados deseja fornecer, sem enfrentar coerção ou consequências adversas pela recusa. O consentimento, conforme regulamentado pela LGPD, deve ser expresso em termos claros e acessíveis, evitando-se linguagem complicada ou cláusulas abusivas para assegurar que seja dado de forma consciente e informada.

A Diretriz 05/2020, do RGPD, enfatiza que a validade do consentimento depende da liberdade com que é dado. O consentimento deve ser uma escolha genuína do titular dos dados, sem qualquer coação ou consequência adversa pela não concessão. Se o consentimento é uma condição não negociável de um contrato, presume-se que não foi dado livremente. É essencial que o titular dos dados possa recusar ou retirar seu consentimento sem sofrer prejuízos.

A ANPD destaca que o consentimento deve ser uma manifestação livre, informada e inequívoca, especificamente para fins determinados. Em casos de dados sensíveis, exige-se que o consentimento seja dado de forma explícita e destacada, não sendo admitido consentimento tácito ou para finalidades genéricas. O titular deve ter uma verdadeira escolha entre autorizar ou recusar o tratamento dos dados pessoais, incluindo o direito de revogar o consentimento a qualquer momento.

A Diretriz 05/2020 da União Europeia apresenta um exemplo relevante para ilustrar as limitações do consentimento quando vinculado à utilização de um serviço. Neste caso, um aplicativo móvel de edição de fotografias requer que os usuários ativem a geolocalização e consintam com o uso de seus dados para publicidade comportamental como condição para acessar o serviço. Dado que nem a geolocalização nem a publicidade comportamental são essenciais para a edição de fotografias, e que o acesso ao serviço depende da aceitação dessas condições, o consentimento obtido não poderia ser considerado livre.

Para que o consentimento seja livre, conforme estipulado nas diretrizes europeias, ele deve ser uma escolha real e voluntária do usuário, sem estar condicionado à prestação de um serviço. A aplicação deveria permitir aos usuários a opção de rejeitar tanto a geolocalização quanto a publicidade comportamental, sem impedir o acesso às funcionalidades principais do serviço de edição de fotos. Esta abordagem garantiria que o consentimento seja dado de forma autônoma, respeitando a liberdade e a escolha dos usuários.

EXEMPLO 2: Cookies de consentimento

Um site de uma faculdade implementa uma ferramenta de gestão de consentimento de cookies que atende plenamente à LGPD. Ao acessar o site pela primeira vez, um banner informativo é exibido, detalhando os diferentes tipos de cookies utilizados: essenciais, de desempenho, de publicidade e a finalidade de cada um. O banner destaca claramente que, enquanto os cookies essenciais são necessários para o funcionamento do site, o consentimento para os cookies de desempenho e publicidade é totalmente opcional e pode ser tanto dado como retirado a qualquer momento. O usuário é informado sobre as consequências de não fornecer consentimento, como a possibilidade de não receber uma experiência personalizada, mas também é assegurado de que tal decisão não afetará sua capacidade de acessar o conteúdo do site. Essa abordagem ressalta o conceito de consentimento livre com liberdade de escolha do titular.

EXEMPLO 3: Vídeos com depoimentos de empregados

Uma empresa brasileira planeja criar uma campanha de endomarketing envolvendo vídeos com depoimentos de seus empregados sobre o ambiente de trabalho. Antes de iniciar as filmagens, a empresa realiza reuniões para explicar o projeto, enfatizando que a participação é inteiramente voluntária. Os empregados interessados são convidados a assinar um termo de consentimento, que esclarece como os vídeos serão utilizados internamente, em eventos, no site da empresa e assegura que qualquer funcionário pode se recusar a participar da atividade de tratamento sem enfrentar repercussões negativas ou alterações em sua relação de trabalho. Este processo demonstra um compromisso com um consentimento verdadeiramente livre, baseado na informação e na liberdade de escolha, alinhado com a LGPD.

EXEMPLO 4: Fotos em revista da prefeitura

Para celebrar o aniversário de uma cidade determinada, a prefeitura deseja publicar a edição especial de uma revista destacando os cidadãos e suas histórias. Antes de fotografar e incluir qualquer cidadão na publicação, a prefeitura organiza sessões de fotos públicas, onde os participantes são informados sobre o propósito da revista e como as fotos serão utilizadas. É fornecido um formulário que solicita o consentimento inequívoco e que detalha os direitos dos participantes, incluindo a opção de não participar e as consequências dessa decisão, como não aparecer na revista. Esse cuidado assegura que o consentimento seja baseado na liberdade de escolha, em conformidade com a LGPD.

3.2. Manifestação Informada

Para que o consentimento seja considerado informado, é primeiramente fundamental que o titular dos dados tenha plena consciência do que está consentindo. A clareza, acessibilidade e simplicidade das informações são requisitos essenciais para que o indivíduo compreenda completamente o escopo e as implicações do tratamento dos seus dados pessoais.

Conforme estipulado pela LGPD, a transparência no tratamento de dados pessoais é um princípio fundamental, conforme definido no art. 6º., inciso VI. Este princípio exige que todos os processos de coleta, uso e compartilhamento de dados pessoais sejam realizados de maneira clara e acessível ao titular dos dados. Reforçando esse princípio, o art. 18, inciso VIII, garante ao titular o direito de ser informado sobre a possibilidade de não fornecer consentimento e as consequências dessa escolha. Essas disposições são vitais para assegurar que os titulares dos dados estejam plenamente informados sobre como seus dados são tratados, promovendo uma cultura de transparência e confiança na gestão de dados pessoais (BRASIL, 2018).

Além disso, no atual cenário de mudanças, marcado pela crescente importância e uso de tecnologias digitais e plataformas, os estudos de Barzotto, Miskulin e Breda (2020) ressaltam a importância do direito à informação. Esta tendência de regulação

crescente sublinha a previsibilidade e a transparência das informações como direitos fundamentais (BARZOTTO *et al.*, 2020).

No contexto europeu, conforme o RGPD, é essencial que o consentimento dos titulares dos dados seja informado, em conformidade com o princípio de transparência destacado no art. 5º. do regulamento. Esta transparência é fundamental para garantir que os titulares dos dados recebam informações claras antes de dar seu consentimento, permitindo-lhes tomar decisões conscientes e compreender as implicações do seu consentimento, incluindo a possibilidade de revogá-lo. A falta de fornecimento de informações claras e acessíveis pelo responsável pelo tratamento dos dados pessoais compromete a validade do consentimento, tornando-o uma base inválida para o tratamento de dados (EUROPEAN DATA PROTECTION BOARD, 2020).

Por fim, a LGPD, no § 6º do art. 8º., assegura que, caso ocorram modificações nas condições originalmente informadas ao titular, o controlador deve informá-lo de forma clara e específica sobre as alterações, proporcionando ao titular a oportunidade de revogar seu consentimento se não concordar com as mudanças (BRASIL, 2018).

Essas normativas consolidam a importância de um consentimento verdadeiramente livre e informado na gestão de dados pessoais, ressaltando a autonomia do indivíduo e reforçando a proteção de sua privacidade.

EXEMPLO 5: Plataforma de e-commerce de vestuário

Ao se registrar em uma plataforma de e-commerce de vestuário, o cliente encontra opções claramente delineadas para consentir separadamente o uso de seus dados. Uma das opções permite ao cliente consentir com o envio de newsletters que trazem novidades e ofertas, enquanto outra opção se refere à utilização de seus dados para análise de preferências com o objetivo de personalizar as recomendações de produtos. Cada escolha é acompanhada de informações detalhadas sobre como os dados serão usados, permitindo ao cliente compreender plenamente o alcance de seu consentimento. Importante informar que a plataforma assegura que o clien-

te pode revogar seu consentimento a qualquer momento, por meio de uma opção facilmente acessível e previamente informada. Este processo reflete a autonomia do usuário em decidir sobre o uso de seus dados, exemplificando uma prática de consentimento informado e voluntário, sem pressão ou coação, alinhada com os princípios de liberdade e transparência exigidos pela legislação de proteção de dados.

Esta discussão sobre o consentimento informado e sua aplicação prática nos leva à próxima seção, onde será abordada a manifestação inequívoca do consentimento. Examinaremos como este requisito fundamental para a proteção de dados é essencial para garantir a eficácia e a legitimidade do consentimento em todas as suas formas.

3.3. Manifestação Inequívoca

O art. 8º., § 1º da LGPD, estabelece que o consentimento deve ser uma manifestação clara do titular dos dados, **eliminando qualquer forma tácita ou presumida de consentimento**. Esta exigência assegura que o consentimento seja genuinamente voluntário e bem-informado, evitando interpretações errôneas ou consentimento por inércia.

Na prática, o consentimento inequívoco deve ser expresso e por meio de **uma ação direta e positiva do titular dos dados**, como a ativação de um botão de aceitação em um formulário *online*. Ações simples como continuar a usar um site não são suficientes para indicar consentimento; são necessárias ações explícitas e claras, como marcar uma caixa ou selecionar configurações em um menu digital.

O European Data Protection Board (2020) enfatiza que tais ações devem ser voluntárias e realizadas com plena compreensão de suas implicações, destacando a necessidade de consentimentos que não deixem espaço para dúvidas. Além disso, é essencial que os titulares dos dados estejam totalmente cientes do que estão consentindo, o que requer a provisão de informações claras, concisas e facilmente acessíveis.

O consentimento inequívoco exige uma declaração ou ação direta e positiva do titular dos dados que não deixa margem para dúvidas ou interpretações errôneas. Isso significa que a anuência para o tratamento de dados não pode ser inferida de um silêncio passivo ou da inatividade do titular. Por exemplo, a ativação de um botão de aceitação

em um formulário *online* constitui um consentimento inequívoco. Além disso, a legislação enfatiza a necessidade de ações positivas por parte do titular dos dados. Como destacado pelo European Data Protection Board (2020), essas ações podem incluir marcar uma caixa, escolher configurações em um menu digital ou qualquer outra ação que demonstre claramente a decisão do titular de permitir o tratamento de seus dados pessoais. A ação deve ser voluntária e realizada com plena compreensão do que o consentimento implica. (EUROPEAN DATA PROTECTION BOARD, 2020).

Um dos principais desafios na implementação do consentimento inequívoco está em garantir que os titulares dos dados estejam totalmente cientes do que estão consentindo. Isso implica não apenas em prover informações claras e acessíveis, mas também em garantir que estas informações sejam compreensíveis para pessoas sem conhecimento especializado em proteção de dados.

Na prática, a obtenção de consentimento exige um esforço consciente para educar o titular dos dados sobre o uso que será feito de suas informações pessoais. Esse processo envolve a disponibilização de informações que sejam claras, concisas e facilmente acessíveis.

EXEMPLO 6: Pop-Ups explicativos ou formulários interativos

Um exemplo seria a utilização de interfaces de usuário que empregam "pop-ups" explicativos ou formulários de consentimento interativos no primeiro ponto de contato digital. Estas interfaces destacam informações relevantes e requerem uma ação afirmativa do usuário, como clicar em um botão de "Aceito", ao lado de outro botão de "Não aceito", ou um botão que possa permanecer desabilitado até que o usuário consinta. O controlador pode ser criativo, desde que assegure um consentimento livre, informado e inequívoco. Os cookies estritamente necessários podem ser tratados com base no legítimo interesse, conforme descrito pela ANPD no Guia Orientativo de Cookies e Proteção de Dados Pessoais (2022), e, por essa razão, podem estar pré-habilitados. O consentimento pode ser coletado de diversas maneiras, não se limitando a termos escritos. Quando em formato escrito, deve incluir cláusulas destacadas e pode também utilizar ícones interativos, formulários, entre outros recursos para facilitar o entendimento e garantir uma manifestação clara do consentimento.

Quadro 1 — Termos de Consentimento para Pop-Ups e Formulários Interativos

Termo de consentimento	O que é feito	Ação do titular
Pop-ups	Um pop-up explicativo aparece no primeiro contato e diz: "usamos cookies para personalizar o conteúdo e os anúncios", podendo dar opção "sim" e "não" ou "aceito" e "não aceito". Ao clicar em **sim** ou **aceito**, o usuário consente com o uso dos cookies para esta finalidade." Este pop-up apresenta as informações de maneira clara e concisa, garantindo fácil compreensão e o consentimento deverá ser solicitado por finalidade. É importante demonstrar ao titular a possibilidade de escolha, informando-o sobre a opção de não fornecer consentimento e as consequências dessa negativa (art. 18, inciso VIII da LGPD)	Interagir com o pop-up, selecionando "**aceito**" após entender completamente o conteúdo. Em sites com cookies de consentimento é indicado no Guia de Orientação de Cookies e Proteção de Dados Pessoais da ANPD (2022) ter as opções no site: "Aceitar todos os cookies". "Selecionar cookies" (com direcionamento para um banner de segundo nível, que dará opções de consentimento com a habilitação pelo titular por categoria de cookies). E, em destaque: "**Rejeitar cookies não necessários**".
Formulários interativos	Um formulário deve informar que os dados poderão ser tratados para uma finalidade específica, **caso o titular consinta voluntariamente, clicando em 'aceito'. É importante incluir duas opções, como "aceito" ou "não aceito", ou "sim" ou "não", para evidenciar claramente a possibilidade de escolha do titular.**	Expressar consentimento de forma ativa por meio do **clique no botão** correspondente

Fonte: própria autora (2024).

É essencial que os controladores desenvolvam procedimentos internos robustos para documentar e gerenciar os consentimentos obtidos, assegurando que cada consentimento possa ser verificado e, se necessário, revogado de maneira simples e eficiente. Este registro de consentimentos deve ser mantido de forma segura e facilmente acessível para auditorias e revisões regulatórias, garantindo a conformidade contínua com a LGPD e reforçando a transparência da organização perante os titulares dos dados e as autoridades regulatórias. Em linha com estas diretrizes, a ANPD determina que o consentimento seja uma manifestação livre, informada e inequívoca do titular dos dados, específica para fins determinados. O rigor na obtenção do consentimento é ainda mais importante em casos envolvendo dados sensíveis, onde deve ser destacado. Esta abordagem assegura que os titulares dos dados possuam a verdadeira liberdade de escolha, permitindo-lhes autorizar

ou recusar o tratamento de seus dados pessoais em qualquer momento, reforçando assim o direito de revogar o consentimento conforme necessário (ANPD, 2023).

A manifestação inequívoca do consentimento é fundamental para assegurar que os titulares dos dados tenham controle completo sobre como suas informações são utilizadas. Ela representa um compromisso com a transparência e o respeito à autonomia do indivíduo, sendo essencial para a confiança, na forma como os agentes de tratamento tratam os dados pessoais. Para explorar ainda mais como esse controle pode ser efetivamente exercido, a próxima seção discutirá o conceito de granularidade do consentimento.

4. GRANULARIDADE

A granularidade do consentimento, conforme estabelecida na Diretriz 05 de 2020 da União Europeia, consiste na importância de os titulares de dados terem controle sobre o uso de suas informações pessoais. Esta diretriz enfatiza a necessidade de oferecer aos titulares a opção de fazer escolhas específicas e informadas sobre as finalidades para as quais seus dados são utilizados**. Isso implica a possibilidade de consentir com operações de tratamento distintas e separadas, ao invés de serem obrigados a aceitar um pacote completo de finalidades de tratamento** (Diretriz 05 de 2020, União Europeia).

A granularidade baseia-se na premissa de que um consentimento sem liberdade de escolha específica não pode ser considerado genuinamente livre. Essa liberdade torna-se essencial quando diversas operações de tratamento de dados estão vinculadas a múltiplas finalidades. Desta forma, a granularidade do consentimento vai além de uma mera formalidade, estabelecendo-se como um pilar fundamental para a proteção da autonomia do indivíduo em relação ao uso de suas informações pessoais.

Além disso, uma abordagem granular ao consentimento garante que cada finalidade de tratamento de dados receba um consentimento específico, o que se alinha à exigência de especificidade no consentimento, assegurando que cada operação de tratamento seja claramente delineada e consentida de forma independente. A importância da especificidade será discutida mais a fundo na seção 6, que aborda o consentimento específico.

Esta metodologia para o cumprimento das normas de consentimento válido implica uma clara separação das finalidades de tratamento de dados, exigindo um consentimento específico para cada uma delas, reforçando assim a governança de dados e respeitando a autonomia dos titulares.

Por exemplo, em uma situação em que um varejista solicita consentimento para usar dados de clientes tanto para envio de publicidade por e-mail quanto para compartilhamento com outras empresas do grupo, a granularidade é comprometida

se essas finalidades não forem claramente separadas no pedido de consentimento. Nesse cenário, o consentimento coletado não é considerado válido devido à falta de especificidade. Portanto, seria necessário obter consentimentos separados para cada finalidade de tratamento, garantindo que cada consentimento seja informado e específico à finalidade a que se destina, conforme as diretrizes da União Europeia (Diretriz 05 de 2020, União Europeia).

EXEMPLO 7 (GRANULARIDADE 1): Aplicativos de saúde

Em um aplicativo de saúde, os usuários recebem a oportunidade de fornecer consentimentos distintos para diversas finalidades. Eles podem escolher permitir o monitoramento de seus dados de saúde para melhorar a funcionalidade do aplicativo, concordar com o compartilhamento desses dados com pesquisadores médicos para estudos científicos, ou ainda aceitar receber promoções de saúde via comunicações de marketing. Cada uma dessas opções é solicitada de forma separada, assegurando que os usuários compreendam e controlem especificamente como cada tipo de dado será utilizado.

EXEMPLO 8 (GRANULARIDADE 2): Plataforma *online* de cursos

Durante a inscrição, uma plataforma de cursos *online* oferece opções separadas de consentimento para receber recomendações personalizadas, compartilhar progresso com mentores e usar dados em pesquisa de melhoramento de serviços. Essas opções são claramente delineadas, permitindo que os usuários decidam de forma independente sobre cada tipo de uso dos seus dados, exemplificando a aplicação da granularidade no consentimento.

EXEMPLO 9 (GRANULARIDADE 3): Plataforma de e-commerce

Quando um usuário configura sua conta em uma plataforma de e-commerce, ele deverá encontrar opções claras para consentir separadamente ao acesso de seus dados de navegação e geolocalização por parceiros de publicidade. Cada opção é explicada detalhadamente dentro das configurações do usuário, ilustrando o uso específico e as consequências de sua escolha, permitindo assim que o usuário tenha controle total e detalhado sobre como seus dados pessoais são compartilhados e utilizados.

EXEMPLO 10 (GRANULARIDADE 4): Portal de desenvolvimento profissional *online*

Ao se registrar em um portal de desenvolvimento profissional *online*, os usuários são apresentados a diversas opções de consentimento que diferenciam claramente os usos de seus dados. As opções incluem a permissão para análise de atividades de aprendizado para recomendações personalizadas de treinamentos e suporte especializado, ou aceitação do uso de suas informações em estudos acadêmicos para aperfeiçoar os programas oferecidos. Cada opção é descrita detalhadamente, proporcionando aos usuários a capacidade de fazer escolhas informadas e independentes sobre o tratamento específico de seus dados.

Esses exemplos destacam claramente a eficácia de um consentimento granular ao proporcionar aos usuários a transparência necessária para fazer escolhas informadas e exercer controle significativo sobre seus dados pessoais. Ao diferenciar as opções de consentimento para diversas finalidades de tratamento de dados, as plataformas não só aderem às normas de proteção de dados, mas também cultivam uma relação de confiança e transparência com os usuários.

É importante ressaltar a interconexão entre a granularidade do consentimento e a necessidade de finalidades específicas, conforme discutido na seção 1.4. Conforme estipulado por regulamentações como a LGPD e o RGPD, é essencial que as intenções de coleta e uso dos dados pessoais sejam claramente articuladas, legítimas e específicas desde o início. Este requisito assegura que os titulares dos dados compreendam e consintam com cada uso de suas informações, reforçando a confiança e a transparência entre os usuários e os controladores de dados.

A granularidade do consentimento complementa a exigência de finalidades determinadas ao permitir que o titular dos dados dê seu consentimento de maneira segmentada para diferentes atividades de tratamento. Esse modelo oferece aos indivíduos a oportunidade de especificar exatamente quais aspectos do tratamento de dados pessoais eles aceitam ou recusam, proporcionando um nível superior de autonomia e proteção. Este enfoque garante que cada escolha seja feita com pleno conhecimento do contexto e dos objetivos específicos pelos quais seus dados são coletados e tratados.

5. DESEQUILÍBRIO DE PODER EM RELAÇÕES ASSIMÉTRICAS

A dinâmica entre autoridades públicas e indivíduos frequentemente envolve um desequilíbrio significativo de poder, o que cria desafios específicos para a utilização do consentimento como base legal no tratamento de dados pessoais. O RGPD da União Europeia, em seu Considerando 43, explicita que o consentimento pode não ser considerado livre e válido em situações em que existe um desequilíbrio claro de poder, especialmente quando uma das partes é uma autoridade pública (Comissão Europeia, 2016). Isso ocorre porque, nessas circunstâncias, o consentimento pode ser influenciado por uma pressão implícita, comprometendo sua voluntariedade essencial.

Além disso, a Comissão Europeia adverte que o consentimento não deve ser a base legal para o tratamento de dados pessoais se não for possível consentir separadamente para diferentes operações de tratamento, ou se a execução de um contrato ou a prestação de um serviço depender desse consentimento, exceto quando estritamente necessário (Comissão Europeia, 2016). Esta diretriz ressalta a complexidade de empregar o consentimento em contextos de desequilíbrio de poder, como frequente ocorre nas relações entre autoridades públicas e cidadãos, e sugere a necessidade de outras bases legais para o tratamento de dados nessas situações. Essa abordagem busca garantir que o tratamento de dados pessoais seja justo e respeite a autonomia dos indivíduos, reforçando a importância de bases legais alternativas que não comprometam a liberdade dos titulares dos dados.

> A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consen-

> timento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução. (COMISSÃO EUROPEIA, 2016).

A Diretriz 05/2020 do European Data Protection Board reforça essa perspectiva, destacando a necessidade de que as autoridades públicas empreguem bases legais mais apropriadas devido ao desequilíbrio inerente de poder. Contudo, essa diretriz também reconhece que, em circunstâncias controladas e específicas, onde se cumprem os requisitos para um consentimento válido, este ainda poderá ser utilizado.

O contexto brasileiro, por meio da LGPD, reflete preocupações similares, quando se deve tentar buscar bases legais alternativas ao consentimento, promovendo uma proteção mais robusta e eficaz dos dados pessoais. Essa abordagem é essencial para assegurar que a autonomia e a liberdade do titular dos dados sejam preservadas, especialmente em interações com o poder público.

Esta seção investiga a aplicação do consentimento em relações assimétricas e discute as implicações legais e práticas para garantir que qualquer consentimento obtido esteja em conformidade com os princípios fundamentais de autonomia e liberdade.

5.1. Do Consentimento nas Relações com o Poder Público

No contexto da administração pública, onde o desequilíbrio de poder é particularmente acentuado, o consentimento frequentemente não é a hipótese legal mais adequada para o tratamento de dados pessoais. Como já mencionado anteriormente no Considerando 43 do RGPD, este documento destaca as complicações inerentes quando o controlador é uma entidade governamental, reforçando a dificuldade de obter um consentimento verdadeiramente livre nessas condi-

ções. A Diretriz 05/2020 do European Data Protection Board complementa essa perspectiva, enfatizando a necessidade de que o Poder Público utilize bases legais mais adequadas para o tratamento de dados, evitando depender do consentimento em face do claro desequilíbrio de poder (European Data Protection Board, 2020).

No mesmo sentido, consoante o Guia do Poder Público da ANPD do Brasil, o consentimento frequentemente não se apresenta como a base legal mais adequada para o tratamento de dados pessoais por parte do Poder Público, sobretudo quando tal tratamento é exigido para o cumprimento de obrigações e atribuições legais. Nessas circunstâncias, a autoridade pública exerce prerrogativas estatais específicas que, devido ao desequilíbrio intrínseco da relação, impedem que o cidadão exerça efetivamente sua liberdade de escolha sobre a utilização de seus dados pessoais. Entretanto, em situações em que a utilização dos dados não é compulsória e a ação governamental não se fundamenta em prerrogativas estatais típicas derivadas de obrigações legais, o consentimento pode ser admitido como uma base legal legítima para o tratamento de dados pessoais pelo Poder Público (ANPD, 2023).

Essas diretrizes e regulamentações são fundamentais para assegurar que o tratamento de dados pessoais seja conduzido de maneira justa e respeite a autonomia dos indivíduos, especialmente nas interações com o poder público. Estabelecem que, sob circunstâncias controladas e onde se verifiquem os requisitos para um consentimento válido, este ainda pode ser considerado apropriado. Por exemplo, em situações em que o tratamento de dados não é obrigatório e o indivíduo possui genuína capacidade de escolha, fica evidente que o consentimento pode constituir uma alternativa viável e legítima, fortalecendo a governança de dados e honrando a autonomia dos titulares.

Um exemplo específico dessa aplicação ocorre quando uma municipalidade solicita o consentimento dos cidadãos para receber atualizações via e-mail sobre obras de manutenção rodoviária. Neste caso, o consentimento é uma opção válida porque a participação é claramente voluntária e recusar-se a dar consentimento não prejudica o acesso a serviços essenciais. Este exemplo ilustra como, mesmo dentro do contexto de poder público, pode existir uma situação em que o consentimento

se mantém como uma base ou hipótese legal legítima e ética de tratamento, desde que as condições de livre escolha e independência sejam rigorosamente observadas (EUROPEAN DATA PROTECTION BOARD, 2020).

A Diretriz 05/2020 do European Data Protection Board fornece outro exemplo ilustrativo da aplicação adequada do consentimento em contextos onde o equilíbrio de poder pode ser questionável. Este exemplo destaca a gestão eficaz dessa dinâmica para assegurar que o consentimento seja verdadeiramente voluntário e não resultante de coerção:

> Uma escola pública solicita aos estudantes consentimento para utilizar as suas fotografias em uma revista estudantil impressa. O consentimento, nestas situações, seria uma verdadeira escolha desde que não fosse negado aos estudantes o ensino ou os serviços a que têm direito e estes pudessem recusar a utilização das referidas fotografias sem ficarem prejudicados (EUROPEAN DATA PROTECTION BOARD, 2020, p. 9).

A Autoridade Nacional de Proteção de Dados (ANPD), em seu guia orientativo sobre o Tratamento de Dados Pessoais pelo Poder Público, enfatiza a importância do consentimento granular, alinhado à Lei Geral de Proteção de Dados (LGPD). O guia destaca a aplicação deste princípio com o exemplo de uma universidade pública, enfatizando a necessidade de os estudantes poderem tomar decisões informadas e específicas sobre cada aspecto do tratamento de seus dados pessoais, assegurando a aderência aos princípios de proteção de dados estabelecidos pela legislação (ANPD, 2021, p. 13).

Dentro deste contexto, um exemplo prático dessa aplicação ocorre durante o processo de inscrição para um evento organizado por uma universidade pública. Os estudantes são solicitados a fornecer informações básicas de cadastro, como nome e número de matrícula, especificamente para a concessão da gratuidade da inscrição, um benefício exclusivo para estudantes. Adicionalmente, os estudantes têm a opção de fornecer seu e-mail, caso desejem receber informações sobre outros eventos organizados pela universidade. É esclarecido que o fornecimento do e-mail é facultativo e que a recusa não impede a participação no evento. Esta clareza e transparência na comu-

nicação garantem que os estudantes possam exercer seu direito de escolha de maneira consciente e livre, sem qualquer prejuízo à sua participação no evento principal.

Além disso, é importante ressaltar que as informações sobre outros eventos são rotineiramente divulgadas na página da universidade na internet, garantindo que todos os estudantes, independentemente de fornecerem ou não seu e-mail, tenham acesso a essas informações (ANPD, 2021, p. 13). Esta prática demonstra o compromisso da universidade com os princípios de transparência e consentimento informado, respeitando a autonomia e a liberdade de escolha dos titulares dos dados.

> Estudante realiza inscrição para participar de um evento organizado por uma universidade pública. O procedimento é realizado *online*, ocasião em que são solicitadas informações básicas de cadastro, como nome e número de matrícula, este para o fim específico de concessão da gratuidade da inscrição, benefício exclusivo para estudantes. Adicionalmente, o estudante tem a opção de fornecer e-mail, caso queira receber informações de outros eventos organizados pela universidade. Uma mensagem esclarece que o fornecimento do e-mail é facultativo e a recusa não impede a participação no evento. Ademais, as informações sobre os outros eventos são rotineiramente divulgadas na página da universidade na Internet (ANPD, 2021, p. 13).

Este cenário demonstra como a prática da universidade está alinhada com os requisitos da LGPD, especificamente com o art. 8º, § 4º, que estipula que o consentimento deve se referir a finalidades determinadas, proibindo autorizações genéricas para o tratamento de dados pessoais. Ao oferecer a opção de fornecer o e-mail de maneira clara e destacada, a universidade assegura que o consentimento seja dado de forma livre, informada e inequívoca, respeitando a autonomia e a liberdade de escolha do titular dos dados.

Conforme o art. 18, inciso VIII, da LGPD, que garante ao titular o direito de ser informado sobre a possibilidade de não fornecer consentimento e sobre as consequências da sua negativa, a universidade informa claramente que a recusa em fornecer o e-mail não impede a participação no evento. Esta prática

não apenas respeita, mas também promove os princípios de transparência e de proteção adequada dos dados pessoais.

Em cenário descrito pela ANPD em um exemplo educacional, evidencia-se que o consentimento obtido nas universidades pode ser considerado nulo por motivos significativos. Primeiramente, os estudantes estão em uma posição onde não podem efetivamente aceitar ou recusar o tratamento de seus dados pessoais, devido à natureza compulsória deste tratamento por parte das instituições de ensino. Em segundo lugar, a solicitação de consentimento é feita para uma finalidade excessivamente genérica, o que contraria as exigências de especificidade e clareza da Lei Geral de Proteção de Dados (LGPD):

> Universidade pública solicita de novos estudantes o fornecimento de dados pessoais necessários para fins de cadastro e matrícula. O procedimento é realizado *online* e, para prosseguir para as etapas seguintes, com a escolha de disciplinas e horários, o estudante deve "aceitar" as condições estipuladas para o tratamento de seus dados. Essas condições são descritas de forma genérica, com a indicação de que os dados poderão ser utilizados para "fins educacionais e outros correlatos". Uma mensagem indica que, caso não fornecido o consentimento, a matrícula não será concluída e o estudante não terá acesso ao curso e a serviços como os de assistência estudantil e empréstimo de livros na biblioteca. (ANPD, 2023).

Para alinhar suas práticas com a LGPD, as universidades devem então tomar medidas claras e definidas: precisam informar de maneira explícita e detalhada as finalidades específicas para as quais os dados dos estudantes serão utilizados, assegurando que estas finalidades sejam legítimas e claramente compreendidas pelos titulares. Além disso, é essencial identificar uma base legal adequada para o tratamento dos dados que não dependa exclusivamente do consentimento, visando respeitar a autonomia e a liberdade dos estudantes. Finalmente, em cumprimento ao princípio da necessidade, as universidades devem limitar a coleta de dados estritamente ao necessário para alcançar essas finalidades específicas, evitando qualquer excesso na solicitação de informações pessoais (ANPD, 2023). É importante destacar que este é um erro comum tanto em instituições públicas quanto privadas. Para ser válido, o consentimento deve ser sempre

uma manifestação livre, informada e inequívoca, independente de se tratar do Poder Público ou de entidades privadas. A principal diferença reside no desequilíbrio de poder, que em algumas situações pode comprometer a autonomia de vontade do indivíduo. Essa autonomia refere-se à capacidade dos indivíduos de se autodeterminarem, ou seja, de fazerem escolhas livres e conscientes sobre suas próprias vidas, incluindo o tratamento de seus dados pessoais.

Portanto, embora a utilização do consentimento por autoridades públicas seja geralmente desaconselhada devido ao desequilíbrio de poder, existem situações delineadas onde ele pode ser adequadamente aplicado, desde que não haja consequências negativas para os titulares dos dados que optem por não consentir. Compreender essas nuances é importante para assegurar que a proteção de dados pessoais em contextos públicos seja realizada de maneira justa e conforme a lei.

5.2. Desequilíbrio de Poder nas Relações de Trabalho

Nesta conjuntura, onde a proteção jurídica desempenha um papel fundamental na defesa dos direitos dos trabalhadores, a necessidade de um consentimento verdadeiramente livre torna-se especialmente significativa. É fundamental enfatizar que, para ser considerado válido, o consentimento deve ser uma "manifestação livre, informada e inequívoca", conforme definido pela legislação brasileira (BRASIL, 2018).

Barzotto e Pereira da Cunha (2020) identificam uma lacuna significativa nas relações trabalhistas relacionadas à privacidade e ao tratamento de dados pessoais e sensíveis. Refletindo sobre essa lacuna, esta seção explora os requisitos para um consentimento válido em relações de trabalho, enfatizando a importância de integrar valores éticos e humanísticos no Direito para garantir que as relações laborais respeitem a dignidade e a autonomia dos trabalhadores.

O Grupo de Trabalho do Art. 29, estabelecido pela Diretiva 95/46/CE da União Europeia, exercia um papel consultivo independente em questões de proteção de dados e privacidade antes de ser sucedido pelo Comitê Europeu de Proteção de Dados (CEPD), instituído pelo RGPD. Este comitê ampliou e reforçou as diretrizes sobre a

privacidade e proteção de dados pessoais, continuando a missão do Grupo de Trabalho do Art. 29 dentro de um contexto legal mais atualizado e abrangente oferecido pelo RGPD. No Parecer 2/2017, sobre o processamento de dados no ambiente de trabalho, o Grupo de Trabalho do Art. 29 destacou uma preocupação significativa com o consentimento para o tratamento de dados de saúde por empregadores. Conforme apontado no Parecer 2/2017, sobre o processamento de dados pessoais no ambiente de trabalho, o Grupo de Trabalho do Art. 29 identifica um problema significativo no que tange ao consentimento para o tratamento de dados sensíveis de saúde por parte dos empregadores. A realidade das relações de trabalho é marcada por uma dependência financeira dos empregados em relação aos empregadores, criando um campo desequilibrado onde o consentimento pode não ser verdadeiramente livre. Esse desequilíbrio questiona a legalidade e a legitimidade do consentimento em tais circunstâncias, especialmente quando empregadores equipam seus trabalhadores com dispositivos de monitoramento da saúde e atividade física, não só no local de trabalho, mas, por vezes, também fora dele. O tratamento desses dados sensíveis está restrito pelas normas vigentes, o que coloca em xeque a validade de qualquer consentimento dado em um contexto em que a liberdade de escolha do empregado é comprometida.

Essa dinâmica tem levado as empresas a tratar cada vez mais os dados dos seus empregados, muitas vezes de forma excessiva, descumprindo princípios da LGPD, como a inclusão de fotografias, para garantir a prestação fiável dos serviços. No entanto, a posição vulnerável dos empregados poderá impedir que eles ofereçam um consentimento livre para o tratamento de seus dados pessoais pelo empregador. Se o tratamento de dados não é proporcional, o empregador não tem fundamento jurídico. Como aponta o mesmo Grupo de Trabalho (2017), essa relação desequilibrada frequentemente invalida a possibilidade de um consentimento genuíno e livre. Portanto, em contextos em que o consentimento dificilmente pode ser considerado livre e informado, as organizações devem buscar outras hipóteses legais para o tratamento de dados pessoais, a fim de assegurar a conformidade com as diretivas de proteção de dados.

Em um exame das dinâmicas laborais contemporâneas, torna-se evidente a presença de um desequilíbrio significativo nas relações de poder entre empregadores e

empregados. Tal realidade não é uma mera observação empírica, mas sim um fenômeno reconhecido e documentado por entidades jurídicas de prestígio. O Grupo de Trabalho do Art. 29, uma autoridade precursora na discussão sobre proteção de dados na União Europeia, já havia sinalizado esta assimetria. Além disso, o CEPD, uma entidade constituída sob a égide do RGPD da União Europeia, também ratifica esta observação.

Esta assimetria no poder tem implicações profundas e multifacetadas, especialmente no que tange ao tratamento de dados pessoais no âmbito laboral. Os empregadores, detentores de uma posição de autoridade e controle, muitas vezes têm a capacidade de influenciar, direta ou indiretamente, as decisões e escolhas de seus empregados, os quais são subordinados. Esta dinâmica não apenas compromete a autonomia dos trabalhadores, mas também coloca em xeque a legitimidade e a eficácia do consentimento como mecanismo de proteção de dados.

Complementando esta análise, o Parecer 2/2017 do Grupo de Trabalho do Art. 29 destaca que os empregados raramente estão em posição de consentir, recusar ou revogar livremente o tratamento dos seus dados devido à dependência inerente à relação empregador-empregado. O parecer enfatiza que, em geral, o consentimento não é considerado uma base jurídica apropriada para o tratamento de dados no local de trabalho, sendo preferível invocar outros fundamentos, como o legítimo interesse do empregador. Contudo, ressalta-se que o legítimo interesse por si só não é suficiente para sobrepor-se aos direitos e liberdades dos empregados, sendo necessário um teste de proporcionalidade para assegurar que o tratamento de dados seja necessário e minimamente invasivo (GRUPO DE TRABALHO DO ART. 29, 2017).

Neste panorama, a preocupação do Grupo de Trabalho do Art. 29 e do CEPD com a desigualdade de poder é um reflexo da necessidade de se garantir que as práticas de coleta e tratamento de dados no ambiente de trabalho sejam justas, transparentes e, acima de tudo, respeitosas com relação aos direitos dos empregados. Esta problemática se revela especialmente crítica em um contexto em que a proteção de dados pessoais é considerada não apenas uma questão legal, mas também um direito fundamental.

Portanto, a análise deste desequilíbrio de poder, amplamente reconhecido por autoridades respeitadas na área de proteção de dados, é fundamental para

a compreensão das complexidades envolvidas no tratamento de dados pessoais nas relações laborais. Ela exige uma abordagem jurídica que não somente reconheça a existência dessa disparidade, mas que também busque formas de mitigá-la. Assim, promove-se práticas laborais que sejam equânimes, transparentes e alinhadas com os princípios de justiça e proteção de dados, abrindo caminho para uma maior equidade nas relações de trabalho.

A Diretriz 05 de 2020 do CEPD nos apresenta um exemplo de consentimento válido nas relações de trabalho em que uma equipe de filmagem está programada para realizar gravações em uma seção específica de um escritório. Neste contexto, o empregador solicita aos empregados que ocupam essa área o consentimento para serem filmados, considerando que poderiam aparecer ao fundo das cenas. Aqueles que optam por não participar não enfrentam penalidades; em vez disso, são realocados para mesas equivalentes em outras partes do edifício durante o período das filmagens. Este procedimento assegura que o consentimento dos empregados seja voluntário e respeita suas decisões pessoais, sem impor consequências adversas àqueles que escolhem não consentir.

Neste cenário de discussão sobre a assimetria de poder nas relações laborais, o CEPD reitera sua preocupação com a liberdade do consentimento dos trabalhadores em um ambiente marcado por dependência. Esta ênfase, que se alinha com análises anteriores, destaca como o medo de represálias ou de consequências negativas pode comprometer a genuinidade do consentimento dos trabalhadores. Tal realidade sublinha as dificuldades de utilizar o consentimento como base legal nas relações de trabalho, exceto em situações de tratamentos opcionais. Exemplos de tais situações incluem atividades de endomarketing, fotos e vídeos de eventos corporativos como celebrações do Dia das Mães, Dia dos Pais, Natal, além de listas de aniversariantes do mês, entre outras. Essas atividades, por não causarem prejuízo econômico ou jurídico ao trabalhador, não fazerem parte do contrato de trabalho e nem serem determinadas por lei, apresentam contextos em que o consentimento pode ser considerado livre.

Desta forma, reconhece-se que, nestas relações, a possibilidade de um consentimento ser dado de maneira completamente livre e desimpedida é frequentemente

comprometida. Portanto, torna-se imperativo reexaminar as práticas de coleta de dados e consentimento nas relações de trabalho, assegurando que os direitos dos trabalhadores sejam protegidos de maneira efetiva e que o tratamento de seus dados pessoais seja conduzido de forma ética e transparente, conforme preconizado pelo RGPD e refletido em legislações correlatas, como a LGPD, no Brasil.

Consequentemente, as cláusulas genéricas no contrato de trabalho que dependem exclusivamente do consentimento são consideradas nulas. É imperativo que as empresas estabeleçam um aviso de privacidade claro para os empregados, elucidando as finalidades da coleta de dados, as bases legais para seu tratamento, os tipos ou categorias de dados coletados, os direitos dos titulares, informações sobre compartilhamentos e transferência internacional de dados, além de indicar o encarregado de proteção de dados ou DPO e seu canal de contato. Ainda que os agentes de menor porte possam manter apenas um canal de contato, a resolução 2 da ANPD (2022) recomenda como boa prática a nomeação de um encarregado de dados.

No presente cenário, a PwC Grécia sofreu uma multa de €150.000, sanção que ilustra as consequências do uso inadequado do consentimento nas relações de trabalho (AUTORIDADE DE PROTEÇÃO DE DADOS HELÊNICA, 2020). A multa, imposta por violações ao art. 83 do RGPD, destaca a criticidade da conformidade normativa. A decisão de usar o consentimento como a única base legal para processar os dados pessoais dos empregados mostrou-se inadequada, especialmente em um contexto em que as obrigações de tratamento de dados são extensivas e reguladas. Esta escolha resultou em falhas significativas no atendimento aos princípios de justiça e transparência prescritos pelo RGPD, uma vez que os funcionários não foram adequadamente informados sobre como seus dados eram tratados.

A Hellenic Data Protection Authority (DPA) salientou que a PwC BS processou de forma ilegal os dados pessoais dos seus empregados ao adotar uma base jurídica imprópria e ao não comunicar de forma transparente a natureza do tratamento dos dados, criando a falsa impressão de que o processamento se baseava no consentimento (European Data Protection Board, 2019). Essa conduta destaca a importância da transparência e da escolha correta das bases legais na gestão dos dados pessoais.

Ademais, a ausência de um aviso de privacidade adequado aos empregados agravou a situação, uma vez que não foram providas informações claras e precisas sobre as finalidades da coleta e as bases legais do tratamento, contrariando as exigências das legislações pertinentes, como a LGPD e o RGPD, o que fere o princípio da transparência (EUROPEAN DATA PROTECTION BOARD, 2019). Tal falha ressalta a necessidade das empresas assegurarem que todas as práticas de tratamento de dados sejam justas, transparentes e respeitem os direitos dos envolvidos.

Esta penalidade evidencia a seriedade das consequências para organizações que não aderem às diretrizes de proteção de dados, destacando a necessidade de uma abordagem criteriosa e fundamentada na seleção de bases legais adequadas para o tratamento de dados pessoais, especialmente em contextos marcados por desequilíbrio de poder intrínseco, como nas relações entre empregadores e empregados. Além disso, ressalta a importância de prover aos empregados comunicações claras e transparentes sobre o uso de seus dados, assegurando que as políticas de privacidade e os procedimentos de consentimento estejam em conformidade integral com a legislação aplicável. Portanto, é essencial que as organizações revisem e ajustem suas práticas para garantir que os direitos fundamentais dos trabalhadores sejam respeitados e protegidos em todas as circunstâncias, consolidando a ética e a legalidade como pilares da gestão de dados pessoais no ambiente de trabalho.

6. CONSENTIMENTO ESPECÍFICO E DESTACADO

A LGPD do Brasil estabelece requisitos mais rigorosos para o consentimento no tratamento de dados pessoais sensíveis e de crianças e adolescentes, categorias consideradas particularmente vulneráveis. Conforme o art. 11, esse tratamento só é permitido sob condições estritamente definidas, exigindo um consentimento que seja claramente destacado de outras autorizações e focado em finalidades específicas. Tal abordagem garante um nível de proteção mais elevado do que o exigido para o tratamento de dados pessoais em geral.

O art. 11 da LGPD determina que o tratamento de dados pessoais sensíveis deve ocorrer somente sob condições específicas e com um consentimento que seja claramente destacado das demais autorizações e voltado para finalidades precisas. Esta abordagem destina-se a proporcionar um nível de segurança e exigência superior em comparação ao tratamento de dados pessoais comuns.

Dados Pessoais Sensíveis:

> Art. 11 da LGPD: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir**, de forma específica e destacada,** para finalidades específicas;"

Por sua vez, o art. 14 trata do consentimento para dados de crianças e adolescentes, exigindo que, **quando esta for a hipótese legal de tratamento**, este seja fornecido por um dos pais ou pelo responsável legal, e apenas após uma clara e completa informação sobre as operações de tratamento de dados em questão. Esta exigência visa assegurar que o consentimento seja consciente e adequado à sensibilidade desses dados.

Dados Pessoais de Crianças e de Adolescentes.

Art. 14 da LGPD:

> o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente. § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o **consentimento específico e em destaque** dado por pelo menos um dos pais ou pelo responsável legal.

Esses requisitos têm como objetivo garantir que os dados considerados mais sensíveis ou que possam impactar significativamente os direitos dos titulares sejam tratados com maior cautela e transparência. Isso reflete a importância de proteger esses indivíduos dentro do contexto legal brasileiro.

Para alcançar isso, o consentimento deve ser **"específico", ou seja, relacionado a finalidades claramente definidas e justificadas que sejam facilmente compreensíveis para o titular dos dados**, evitando o uso de termos genéricos ou ambíguos. Além disso, deve **ser "destacado", o que significa que deve ser claramente distinguido de outros termos ou condições**, assegurando que o titular dos dados pessoais esteja plenamente ciente da importância e das implicações de conceder tal consentimento.

De forma paralela, o Considerando 32 do RGPD sublinha que o consentimento deve ser um ato voluntário, explícito e específico, refletindo **uma aprovação inequívoca do titular** dos dados para o tratamento de suas informações pessoais. Esta manifestação deve ser evidente e ativa, **realizada por meio de uma ação ou um ato positivo claro** — como a seleção de uma opção em um site, um clique em um botão ou uma declaração verbal ou escrita — garantindo que o consentimento seja consciente e deliberado.

É essencial notar que **nem o silêncio nem as opções pré-marcadas constituem formas válidas de consentimento**. Além disso, o consentimento deve abranger todas as atividades de tratamento para o mesmo propósito e, quando houver múltiplas finalidades, é necessário obter consentimentos individuais para cada uma delas.

De acordo com o RGPD, o consentimento constitui uma das hipóteses legais para o processamento de dados pessoais e deve ser dado de forma livre, específica, informada e inequívoca. O consentimento livre implica que não deve haver pressão ou influência indevida, comprometendo sua validade. Além disso, deve ser específico e informado, fornecendo ao titular dos dados informações claras sobre a identidade do controlador, os tipos de dados que serão processados e os propósitos específicos do processamento. Isso evita a extensão não autorizada dos objetivos iniciais. Também é essencial que o consentimento seja inequívoco, exigindo uma

declaração clara ou uma ação afirmativa como uma opção explícita, e não pode ser deduzido por inação ou silêncio do titular dos dados (RGPD Info, 2024).

Essas orientações têm como objetivo garantir que os indivíduos controlem plena e inequivocamente como seus dados são usados, fortalecendo a proteção da privacidade no contexto regulatório. A necessidade de obter o consentimento sem comprometer a usabilidade do serviço sublinha a importância da transparência e de um equilíbrio entre a coleta do consentimento e a experiência do usuário. Estes princípios são essenciais para assegurar que o processamento de dados pessoais seja feito de maneira justa e transparente, permitindo que o titular dos dados tenha autonomia e controle sobre suas informações pessoais.

O art. 8º., § 4º, da LGPD determina que o consentimento deve ser obtido para finalidades determinadas, enquanto o art. 7º., inciso I, que traz as hipóteses legais de tratamento de dados pessoais apenas dispõe que o tratamento destes só pode ocorrer com o consentimento do titular. Por outro lado, o art. 11 enfatiza que o tratamento de dados pessoais sensíveis requer condições mais restritas, necessitando um consentimento específico e destacado. Essa diferenciação na legislação visa proporcionar uma proteção mais robusta aos dados considerados sensíveis, exigindo uma clara manifestação de vontade por parte do titular dos dados, garantindo-se maior segurança jurídica e proteção da privacidade.

A LGPD do Brasil também estabelece de forma clara a distinção entre o tratamento de consentimento para dados pessoais comuns e dados sensíveis ou de crianças e adolescentes. Enquanto a LGPD demanda consentimento específico para finalidades claras em dados comuns, ela impõe um consentimento ainda mais rigoroso e destacado para dados sensíveis e de menores, alinhando com salvaguardas reforçadas. Para dados comuns, exige-se consentimento para finalidades determinadas. Para dados sensíveis e de crianças e adolescentes, a legislação requer um consentimento específico e destacado, proporcionando salvaguardas adicionais para estas categorias de dados que precisam de maior proteção. Essa diferenciação assegura que o tratamento dos dados ocorra com maior consciência e proteção, refletindo a seriedade e sensibilidade envolvidas (IAPP, 2020).

A LGPD estabelece requisitos específicos para consentimento em casos de dados pessoais sensíveis e de menores, reforçando a proteção para essas categorias vulneráveis. O art. 11 da LGPD especifica que o tratamento desses dados sensíveis deve acontecer apenas sob condições específicas, com um consentimento claramente separado das outras autorizações e destinado a finalidades precisas. Por outro lado, o art. 14 regula o consentimento para dados de crianças e adolescentes, exigindo que seja fornecido por um dos pais ou pelo responsável legal, após fornecimento completo e claro das informações sobre o tratamento de dados proposto. Estes requisitos são projetados para assegurar que os dados sensíveis ou que possam impactar significativamente os direitos dos titulares sejam tratados com a devida cautela e transparência, refletindo a necessidade de proteger esses indivíduos no contexto legal brasileiro.

O consentimento deve ser "específico", ou seja, vinculado a propósitos claros e justificados, compreensíveis pelo titular e livre de termos ambíguos. Além disso, deve ser 'destacado', garantindo que se distinga de outras condições ou termos, assegurando que o titular dos dados esteja plenamente ciente da importância e das implicações de seu consentimento.

Específico: o consentimento deve ser relacionado **a finalidades precisas, claras e justificadas, que sejam compreensíveis para o titular dos dados**. Deve-se evitar termos genéricos ou ambíguos; o objetivo do tratamento dos dados sensíveis deve ser diretamente relacionado à necessidade da coleta desses dados.

Destacado: O consentimento deve ser obtido de maneira que se destaque dos demais termos ou condições **e não pode ser apenas uma parte de um documento mais amplo sem a devida ênfase.** Isso é importante para garantir que o titular dos dados esteja plenamente ciente da importância e das implicações de conceder tal consentimento.

EXEMPLO 11: Consentimento Específico em aplicativo de saúde

Um aplicativo de monitoramento de saúde solicita o consentimento dos titulares antes de iniciar a coleta de dados biométricos para análise de saúde. Durante o processo de configuração, o aplicativo apresenta uma tela de consentimento onde detalha como os dados serão usados para monitorar a saúde do usuário e melhorar

a personalização do serviço principal oferecido onde a hipótese legal de tratamento não era consentimento. A caixa de diálogo é projetada para garantir visibilidade e compreensão, com informações claras e a opção de aceitar ou recusar o tratamento específico dos dados coletados.

EXEMPLO 12: Consentimento Específico em aplicativo educacional

Um aplicativo educacional destinado ao aprendizado de crianças e de adolescentes oferece adicionalmente jogos e atividades que envolvem o processamento de dados pessoais. Antes de iniciar o cadastro, o aplicativo apresenta uma interface clara e acessível para coletar o consentimento de pelo menos um dos pais ou do responsável legal, detalhando como os dados serão usados para personalizar a experiência educacional. A tela de consentimento requer uma ação afirmativa dos pais, como marcar uma caixa que não esteja pré-selecionada, para assegurar que o consentimento seja específico e informado, em total conformidade com as exigências da LGPD para dados de menores.

6.1. Do Tratamento de Dados Pessoais Sensíveis

Conforme o art. 11 da Lei Geral de Proteção de Dados (LGPD), o Brasil adota um regime rigoroso para o tratamento de dados pessoais sensíveis. Esses dados incluem informações sobre origem racial ou étnica, convicções religiosas, opiniões políticas, filiação sindical, organizações de caráter religioso, filosófico ou político, bem como dados relacionados à saúde, vida sexual e dados genéticos ou biométricos. Tais informações demandam um consentimento que deve ser específico e claramente distinto de outras autorizações e estritamente vinculado a finalidades bem definidas.

O art. 11 estabelece: "O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, **de forma específica e destacada, para finalidades específicas**" (BRASIL, 2018). Este consentimento específico e destacado visa proporcionar uma proteção superior, garantindo que o tratamento dos dados sensíveis seja realizado com a máxima transparência e segurança, respeitando a sensibilidade e a importância desses dados.

Desta forma, a LGPD estipula que o consentimento para o tratamento de dados pessoais sensíveis deve ser nitidamente diferenciado de outras autorizações, garantindo que tanto o titular dos dados quanto, quando aplicável, seu responsável legal, estejam plenamente cientes da relevância e sensibilidade dos dados em questão. Tal exigência reforça a necessidade de um consentimento cuidadosamente elaborado e claramente definido para prover proteção adequada e assegurar a conformidade com a LGPD.

EXEMPLO 13: Consentimento específico e destacado em dados sensíveis de saúde

Em uma clínica de telemedicina, o processo de obtenção de consentimento é cuidadosamente planejado para cumprir as normas de privacidade e proteção de dados.

Na primeira visita ao serviço, o paciente é direcionado para uma página de consentimento exclusiva, na qual os usos específicos dos dados são detalhados, abrangendo não apenas a concretização do contrato principal (que não é consentimento), mas outros tratamentos adicionais, como diagnóstico e acompanhamento e que precisam de consentimento do titular.

A página se destaca visualmente do restante do site, capturando efetivamente a atenção do titular. O formulário de consentimento requer uma ação afirmativa do paciente, como a seleção de uma opção não pré-marcada, para autorizar especificamente o uso de seus dados pessoais sensíveis. Quando o paciente é menor de idade, a clínica assegura que o consentimento seja fornecido por um dos pais ou pelo responsável legal, que também é informado detalhadamente sobre o tratamento dos dados do menor. Esta metodologia, conforme as diretrizes da LGPD, reforça a confiança dos pacientes, assegurando que os dados pessoais e sensíveis dos pacientes são tratados com total transparência e baseados em um consentimento válido e claramente destacado.

6.2. Do Tratamento de Dados Pessoais de Crianças e Adolescentes

A LGPD estabelece um marco significativo na proteção de dados pessoais, dedicando especial atenção aos dados de crianças e adolescentes. Embora a LGPD não

os classifique explicitamente como sensíveis, a legislação impõe um regime de proteção rigoroso similar para eles, exigindo um **consentimento específico e destacado dos pais ou responsáveis legais**, conforme estipulado no art. 14. Este procedimento destaca a vulnerabilidade desse grupo etário e visa garantir sua integridade e privacidade.

No contexto do tratamento de dados pessoais de crianças e adolescentes, a LGPD exige que o consentimento seja especificamente concedido e claramente destacado por ao menos um dos pais ou responsável legal. Esta exigência enfatiza o compromisso da legislação em priorizar o **melhor interesse dos menores**, **proporcionando um nível elevado de proteção para seus dados.**

A legislação também obriga os controladores a assegurar total transparência sobre a coleta, uso e direitos associados aos dados de crianças e adolescentes, exigindo que as informações sejam apresentadas de forma acessível para facilitar decisões informadas por parte dos responsáveis. Medidas de segurança robustas são requeridas e é proibido condicionar a participação em atividades ao fornecimento de mais dados pessoais do que o estritamente necessário para cada finalidade.

É essencial que sejam feitos esforços razoáveis para verificar que o consentimento foi efetivamente concedido por um responsável legal, utilizando tecnologias disponíveis para garantir a autenticidade desse consentimento. Esta precaução é essencial para prevenir o abuso e o uso indevido dos dados.

Texto do art. 14 da LGPD:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o **consentimento específico e em destaque** dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
>
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
>
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança. (BRASIL, 2018)

Apesar de os dados de crianças e adolescentes não serem automaticamente classificados como sensíveis pela LGPD, eles são tratados com um nível de proteção comparável ao dos dados sensíveis, necessitando de salvaguardas equivalentes. Tal abordagem demonstra o desejo do legislador de proporcionar uma proteção elevada, levando em consideração a capacidade limitada desses jovens de consentir independentemente.

Finalmente, a LGPD define um paradigma de cuidado e proteção dos dados de crianças e adolescentes, reconhecendo a sensibilidade particular desse grupo e a necessidade de medidas de proteção adicionais. Este enfoque reflete uma preocupação genuína com a segurança e privacidade desses indivíduos vulneráveis e alinha o Brasil com padrões internacionais de proteção de dados, promovendo uma abordagem consistente e rigorosa no tratamento de suas informações pessoais.

EXEMPLO 14: Fotos de alunos no Instagram de uma escola

Considerando uma escola privada que pretende utilizar fotos de seus alunos em eventos escolares para postagem em seu perfil oficial do Instagram, com o

objetivo de promover atividades extracurriculares, um procedimento meticuloso é implementado. A escola envia uma comunicação clara e detalhada aos pais ou responsáveis, explicando como as imagens serão utilizadas e destacando a finalidade de cada uso.

É solicitado o consentimento por meio de um formulário digital, **que ressalta a natureza opcional da autorização e assegura que a não participação na iniciativa não afetará a inclusão dos alunos nas atividades escolares. O formulário também orienta os pais sobre como podem revogar o consentimento a qualquer momento**, sublinhando a importância da autonomia na gestão dos direitos digitais dos alunos. Esta prática não só cumpre as diretrizes da LGPD, mas também reforça o controle parental sobre a exposição das imagens dos filhos, assegurando que o consentimento seja voluntário e previamente informado.

6.2.1. Os dados de crianças e adolescentes podem ser tratados sob que hipóteses legais de tratamento?

As exceções previstas no art. 14 da LGPD permitem a coleta de dados sem consentimento prévio em situações específicas, tais como para contato com os pais em casos de necessidade urgente ou para proteção da criança. Essa flexibilidade é essencial para permitir ações rápidas em situações que exigem uma resposta imediata para proteger o bem-estar do menor

O Enunciado 1 da ANPD, publicado em 22 de maio de 2023, esclarece que o tratamento de dados pessoais de crianças e adolescentes pode ocorrer com base em qualquer uma das hipóteses legais previstas nos arts. 7º ou 11 da LGPD. Contudo, deve sempre garantir o melhor interesse dos menores, conforme avaliação em cada caso concreto, seguindo o estabelecido no art. 14. Esta orientação destaca a necessidade de ponderar cuidadosamente o bem-estar das crianças e adolescentes ao tratar seus dados, priorizando suas necessidades e direitos

Para ilustrar a aplicação prática do Enunciado, considere o salário-família, um benefício previdenciário que auxilia trabalhadores de baixa renda no sustento de seus dependentes. A concessão deste benefício implica o tratamento de dados pessoais

dos beneficiários e de seus dependentes, enquadrado como "cumprimento de obrigação legal ou regulatória pelo controlador", conforme o art. 7º, inciso II, da LGPD. Esta base legal, fundamentada na Lei 4.266 de 1963, especifica que o tratamento de dados é necessário para cumprir uma obrigação legal, dispensando o consentimento dos pais ou responsável legal para o tratamento de dados de crianças e adolescentes.

Este exemplo demonstra como as diretrizes da LGPD e do Enunciado 1 da ANPD devem ser aplicadas na prática, assegurando que o tratamento de dados pessoais de crianças e adolescentes, seja em contextos governamentais ou privados, seja conduzido de forma a proteger e promover seus melhores interesses, independentemente da base legal aplicada.

6.2.2. Princípio do Melhor Interesse

O tratamento de dados pessoais de crianças e adolescentes, seja em contextos governamentais ou privados, deve ser conduzido de forma a proteger e promover seus melhores interesses, independentemente da base legal aplicada. O princípio do melhor interesse da criança e do adolescente é fundamental e deve prevalecer em todas as atividades de tratamento de dados pessoais que envolvam menores de idade. Este princípio implica uma avaliação criteriosa de como os dados pessoais das crianças e adolescentes devem ser coletados, utilizados e compartilhados, assegurando que tais ações sempre protejam seus direitos fundamentais e promovam seu bem-estar.

De acordo com o art. 14 da LGPD, o tratamento de dados de crianças e adolescentes deve ocorrer sob consentimento específico e destacado, fornecido por pelo menos um dos pais ou responsáveis legais. Esta disposição legal reconhece a realidade das diversas configurações familiares existentes e se adapta às dificuldades práticas de obter consentimento de ambos os pais ou responsáveis simultaneamente.

Ademais, o art. 14 também impõe a obrigação de que qualquer tratamento de dados pessoais de crianças e adolescentes seja realizado considerando suas condi-

ções específicas de desenvolvimento. Cada decisão sobre o tratamento desses dados deve passar por um processo de avaliação de benefícios aos menores e de riscos que considere as vulnerabilidades associadas à idade e à capacidade de entendimento dos menores, garantindo que a privacidade e a proteção de seus dados pessoais não sejam comprometidas.

Nesse contexto, a coleta e o uso desses dados devem ser realizados de modo a respeitar o melhor interesse das crianças e adolescentes envolvidos. Isso envolve:

- ✓ A minimização da coleta de informações, coletando apenas os dados estritamente necessários para a concessão do benefício.
- ✓ Processamento das informações de forma transparente e segura.
- ✓ Priorização dos direitos dos menores, garantindo proteção contra qualquer forma de discriminação ou exploração.

Além disso, é fundamental que existam avisos de privacidade, sendo as práticas de coleta de dados previamente comunicadas de maneira clara e acessível, utilizando linguagem e métodos apropriados para a compreensão dos pais ou responsáveis legais, e, sempre que possível, adaptadas para serem compreendidas também pelos próprios menores.

Este enfoque cuidadoso e detalhado, que alinha a autorização de tratamento de dados pessoais à observância dos direitos das crianças e adolescentes, está em conformidade não apenas com a LGPD, mas também com normativas internacionais de proteção de dados e direitos humanos, como a Convenção sobre os Direitos da Criança, que também enfatiza o melhor interesse do menor como um princípio fundamental.

EXEMPLO 15: Plataforma *online* de aprendizado para crianças – progresso do aluno

Considere uma plataforma *online* desenvolvida para o aprendizado de crianças. Para personalizar a experiência e monitorar o progresso do aluno, a

plataforma deseja coletar dados sobre o desempenho e as preferências de leitura das crianças. Aqui, o princípio do melhor interesse se manifesta no processo de obtenção de consentimento e a plataforma deve fornecer previamente aos pais ou responsáveis legais informações claras e detalhadas sobre quais dados serão coletados, como serão usados para beneficiar adicionalmente e diretamente a aprendizagem da criança e quais as medidas adotadas para proteger esses dados.

O consentimento também deve ser de fácil compreensão, garantindo que os pais possam tomar uma decisão que priorize o bem-estar e o desenvolvimento educacional das crianças ou adolescentes. A opção de revogação do consentimento a qualquer momento também deve ser clara e acessível, reforçando a proteção dos direitos da criança e do adolescente e o respeito pela sua autonomia e privacidade. Este exemplo ilustra como o consentimento, quando baseado no melhor interesse das crianças, deve sempre facilitar o controle parental e a compreensão do uso dos dados em contextos que beneficiam o desenvolvimento infantil.

6.3. Salvaguardas Adicionais

A LGPD estabelece requisitos rigorosos para o tratamento de dados sensíveis e de crianças e adolescentes, exigindo um consentimento específico e em destaque e a adoção de salvaguardas adicionais robustas. Esta Seção detalha práticas essenciais que, somadas ao consentimento específico e destacado, asseguram a proteção desses dados sensíveis:

> **Transparência:** essencial para qualquer prática de tratamento de dados, a transparência deve ser particularmente rigorosa quando se trata de dados sensíveis e de menores de idade. Os controladores devem fornecer previamente informações claras e acessíveis sobre os propósitos de coleta, processamento e armazenamento de dados, assim como sobre as medidas de segurança implementadas para proteger esses dados. A transparência deve ser mantida em todas as comunicações e documentos relacionados, garantindo que os titulares dos dados e, quando aplicável, seus responsáveis legais possam entender e gerenciar o uso de suas informações.

Finalidade Restrita: a coleta e o uso de dados devem ser limitados estritamente às finalidades que foram explicitamente autorizadas pelos titulares dos dados. Qualquer mudança nas finalidades originais de tratamento deve ser comunicada aos titulares de forma clara, requerendo um novo consentimento, se necessário. Isso garante que os dados não sejam utilizados de maneira incompatível com as expectativas do titular e com o que foi legalmente consentido.

Medidas de Segurança Robustas: a proteção de dados sensíveis e de crianças requer a implementação de robustas medidas técnicas e administrativas de segurança da informação que mitiguem os riscos e aumentem a confiança dos titulares dos dados na organização. Estas medidas são projetadas para prevenir acessos não autorizados, vazamentos e outras formas de tratamento inadequado dos dados. É essencial que essas medidas sejam revistas e atualizadas regularmente para enfrentar novos desafios e ameaças emergentes.

Documentação e Conformidade: é essencial manter registros detalhados de todas as operações de tratamento de dados para garantir a conformidade com a LGPD. Esses registros devem incluir informações sobre as finalidades do tratamento, natureza do dados, categoria de titulares e destinatários, hipóteses legais de tratamento, prazos de conservação e medidas de segurança aplicadas. A documentação detalhada é essencial não apenas para auditorias e verificações de conformidade regulatórias, mas também para responder a possíveis questionamentos por parte dos titulares dos dados.

Essas práticas não apenas cumprem as exigências legais, mas também promovem um ambiente de tratamento de dados que protege integralmente a privacidade e os direitos dos indivíduos mais vulneráveis. Ao seguir estas diretrizes, as organizações podem assegurar que estão tratando dados pessoais de maneira justa, transparente e segura, alinhada com os princípios éticos e legais da proteção de dados no Brasil.

Essas práticas, entre outras, complementam o consentimento específico e em destaque, quando tratados dados sensíveis ou de crianças e adolescentes, fortalecendo a proteção de dados sensíveis e de menores e reforçando a confiança dos titulares dos dados, assegurando que o tratamento ocorra de maneira justa, transparente e em estrita conformidade com a LGPD.

CONSIDERAÇÕES FINAIS

Este guia, intitulado "Guia de Consentimento como Hipótese Legal de Tratamento da LGPD", é o resultado do pós-doutorado da professora Selma Carloto na Universidade Federal do Rio Grande do Sul (UFRGS), sob a supervisão da professora Luciane Cardoso Barzotto. Ele oferece uma análise sobre o consentimento dentro do arcabouço legal estabelecido pela LGPD.

Cada seção deste guia foi elaborada com o intuito de auxiliar na compreensão do consentimento como hipótese legal de tratamento, desde sua definição até os direitos do titular relacionados a ele. Foram incorporadas diretrizes da União Europeia e interpretações, garantindo que o guia esteja em conformidade com as melhores práticas internacionais.

Exploramos os fundamentos do consentimento, incluindo sua definição, destaque e ônus da prova, bem como aspectos importantes como a granularidade e o desequilíbrio de poder em relações assimétricas.

Focando na manifestação livre, informada e inequívoca, examinamos cada aspecto dessas três dimensões, destacando sua relevância na garantia de uma proteção efetiva dos dados pessoais. Além disso, dedicamos seções ao consentimento específico e em destaque, com foco no tratamento de dados pessoais sensíveis e de menores de idade.

Portanto, este guia oferece uma visão detalhada sobre o consentimento na LGPD, servindo como uma ferramenta útil para entender o consentimento como base legal para o tratamento de dados pessoais.

REFERÊNCIAS

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. Manual da Legislação Europeia sobre Proteção de Dados. Edição de 2018. Disponível em: https://fra.europa.eu/pt/publication/2022/manual-da-legislacao-europeia-sobre-protecao-de-dados-edicao-de-2018. Acesso em: 19 nov. 2023.

ANPD - Autoridade Nacional de Proteção de Dados. (2022). Cookies e Proteção de Dados Pessoais. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf. Acesso em: 14 abr. 2024.

ANPD - Autoridade Nacional de Proteção de Dados. (2023). Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público (Versão 2.0). Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 20 nov. 2023.

ANPD - Autoridade Nacional de Proteção de Dados. Conselho Diretor. Enunciado CD/ANPD n. 1, de 22 de maio de 2023. Diário Oficial da União: seção 1, p. 129, ed. 98, 24 maio 2023. Disponível em: https://www.in.gov.br/web/dou/-/enunciado-cd/anpd-n-1-de-22-de-maio-de-2023-485306934. Acesso em: 25 fev. 2024.

ANPD - Autoridade Nacional de Proteção de Dados. Guia do Poder Público. 2.0. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 03 mai. 2024.

BARZOTTO, Luciane Cardoso; MISKULIN, Ana Paula Silva Campos; BREDA, Lucieli. Condições transparentes de trabalho, informação e subordinação algorítmica nas relações de trabalho. Futuro do trabalho: os efeitos da revolução digital na sociedade. Brasília: ESMPU, p. 211-223, 2020.

BARZOTTO, Luciane Cardoso; PEREIRA DA CUNHA, Leonardo Stocker. Proteção de Dados Pessoais e Consentimento do Empregado: Jurisprudência Trabalhista e a Lei Geral de Proteção de Dados (LGPD). In: DORNELES, Leandro do Amaral D. de; BARZOTTO, Luciane Cardoso (Org.). O Direito do Trabalho em Tempos de Mudança. Porto Alegre: UFRGS EDITORA, 2020.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em: 9 set. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Resolução CD/ANPD n. 2, de 27 de janeiro de 2022. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022. Acesso em: 26 abr. 2024.

CALDEIRA, Cristina. A proteção de Dados Pessoais e o Impacto nas Transferências Internacionais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). Direito & Internet IV: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

CARLOTO, Selma. Lei Geral de Proteção de Dados. 4. ed. São Paulo: LTr, 2023.

COMISSÃO EUROPEIA. 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 (Regulamento Geral sobre a Proteção de Dados) RGPD – General Data Protection Regulation (Regulamento Geral de Proteção de Dados Pessoais). Disponível em:<https://eur-lex.europa.eu/legal-content/PT/TXT/ HTML/?uri=CELEX:02016R0679=20160504-&from-EN>. Acesso em: 9 nov. 2023.

COMITÊ EUROPEU DE PROTEÇÃO DE DADOS OU CONSELHO EUROPEU. Diretrizes 05/2020 relativas ao consentimento na acepção do Regulamento 2016/679. Adotadas em 4 de maio de 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf. Acesso em: 10 nov. 2023.

DE LUCCA, Newton; ZOCATELLI QUEIROZ, Renata Capriolli. Inteligência Artificial e a Proteção de Dados Pessoais à Luz da Lei Geral de Proteção de Dados. In: CARLOTO, Selma (coord.). Inteligência Artificial e Novas Tecnologias nas Relações de Trabalho, Volume 2. Editora Mizuno, 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011.

EUROPEAN DATA PROTECTION BOARD. Diretrizes 05/2020 relativas ao consentimento na acepção do Regulamento 2016/679. Adotadas em 4 de mai. de 2020, p. 9. Disponível em: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf>. Acesso em: 10 nov. 2023.

EUROPEAN DATA PROTECTION BOARD. Company fined 150,000 euros for infringements of the GDPR. 2019. Disponível em: https://www.edpb.europa.eu/news/national-news/2019/company-fined-150000-euros-infringements-gdpr_en. Acesso em: 03 maio 2024.

GRUPO DE TRABALHO DO ART. 29. Parecer 2/2017 sobre o tratamento de dados no local de trabalho. [S.l.], 8 jun. 2017. Adotado em 8 de junho de 2017. Disponível em: 20170608_parecer_2_wp249_gt29 (uc.pt). Acesso em: 20 abril. 2024.

IAPP. Impactos operacionais da LGPD no Brasil: Parte 1 — Processamento, direitos e DSARs. (2020). Disponível em: https://iapp.org/news/a/processing-rights-and-dsars-under-brazils-lgpd/. Acesso em: 26 abr. 2024.

LIMA, Cíntia Rosa Pereira; PEROLI, Kelvin. A Aplicação da Lei Geral de Proteção de Dados no Brasil no Tempo e no Espaço. In: LIMA, Cíntia Rosa Pereira de (Coord.). Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almedina, 2020. p. 69-100. E-book.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD). Disponível em: https://RGPD-info.eu/. Acesso em: 26 abr. 2024.

Selma Carloto

Autora

Autora de diversas obras de Compliance Trabalhista, Lei Geral de Proteção de Dados, Inteligência Artificial e ESG e coordenadora e autora de obras de Inteligência Artificial nas Relações de Trabalho e Manual de Relações de Trabalho em Visual Law. Mestre em Direito pela Universidade de São Paulo (USP). Doutora em engenharia da informação, Inteligência Artificial, pela Universidade Federal do ABC (UFABC) e doutorado em Direito do Trabalho na UBA. Pós-doutora em Direito do Trabalho pela Universidade Federal do Rio Grande do Sul (UFRGS). Professora autora das disciplinas: Proteção de Dados; Compliance Trabalhista e Lei Geral de Proteção de Dados da Fundação Getúlio Vargas (FGV) Escola de Direito Rio. Professora da FGV de MBA e pós-graduação. Diretora do Instituto Nacional de Proteção de Dados (INPD) e presidente da Comissão de Temporalidade do INPD. DPO certificada pela Exin: https://app.exeed.pro/badge/89752 . Contato: selmacarloto@hotmail.com e instagran @ selmacarloto

Livros publicados pela LTr Editora:

– ESG+i – Governança Ambiental, Social e Corporativa – 4ª edição

– Lei Geral da Proteção de Dados: Incluindo vários modelos, segurança da informação e fases de implementação – 4ª edição

– Compliance Trabalhista – 5ª edição – Obra Ilustrada em Visual Law, incluindo as fases de implementação e normas da ISO

– Lei Geral de Proteção de Dados Comentada: Com Enfoque nas Relações de Trabalho

– Lei Geral de Proteção de Dados e Segurança da Informação – Perguntas e Respostas – 2ª edição – Volume I

– Manual Prático de Adequação à LGPD com Enfoque nas Relações de Trabalho – 2ª edição

– O Compliance Trabalhista e a Efetividade dos Direitos Humanos dos Trabalhadores – 2ª edição

Luciane Cardoso Barzotto

Supervisora

Professora do Programa de Pós-Graduação em Direito da Universidade Federal do Rio Grande do Sul (UFRGS). Desembargadora do Tribunal Regional do Trabalho da 4ª Região. Mestre e Doutora em Direito pela Universidade Federal do Paraná (UFPR). Líder do grupo de pesquisa de Direito e Fraternidade da Universidade Federal do Rio Grande do Sul (UFRGS). Presidente da Academia Sul-Rio-Grandense de Direito do Trabalho (ASRDT) e integrante da Academia Brasileira de Direito do Trabalho (ABDT). E-mail: lucicard@terra.com.br.

Guia de Consentimento como Hipótese Legal de Tratamento da Lei Geral de Proteção de Dados Pessoais (LGPD)

REALIZAÇÃO

CENTRO DE PESQUISAS JUDICIAIS DA AMB

AMB Associação dos Magistrados Brasileiros

ANPT

INPD INSTITUTO NACIONAL DE PROTEÇÃO DE DADOS

PPG DIREITO UFRGS
UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

LTr