ARTIGOS ACEITOS PARA PUBLICAÇÃO
DIREITO DIGITAL E SETOR PÚBLICO - 2020.2

ITS RIO

Pós-Graduação em Direito Digital

CEPED UERJ ITS

O CONSENTIMENTO NAS RELAÇÕES *PRIVACY AS A PRODUCT*

Carolina Augusta Borges Vaz Martins

O CONSENTIMENTO NAS RELAÇÕES *PRIVACY AS A PRODUCT*

CAROLINA AUGUSTA BORGES VAZ MARTINS

Resumo: O presente artigo trata da utilização do consentimento como base legal para atividades nas quais o titular fornece seus dados pessoais em troca de brindes, promoções ou outras vantagens. O artigo pretende analisar se a obtenção do consentimento nesse contexto está de acordo com a Lei Geral de Proteção de Dados Pessoais a partir da análise dos aspectos teóricos do consentimento válido. Ao fim, conclui-se que, para que tais atividades não infrinjam a legislação brasileira, seria necessário eleger outra base legal que justificasse o tratamento.

Palavras-chave: Proteção de Dados, LGPD, Bases Legais, *Privacy as a product*, Consentimento, Transparência

Sumário: **1.** Introdução. **2.** Consentimento. **3.** Cuidados do controlador ao obter o consentimento em relações *privacy as a product*. **4.** Conclusão **5.** Bibliografia.

1 INTRODUÇÃO

As liberdades dos indivíduos são protegidas em diversas esferas em âmbito nacional e internacional de forma mais estruturada pelo menos desde o final da Segunda Guerra Mundial. Contudo, o conteúdo dessa proteção em aspectos práticos deve constantemente evoluir e adaptar-se a novas circunstâncias e contextos.

Assim, o conteúdo do direito à privacidade deixou de corresponder apenas a um *right to be left alone* (WARREN e BRANDEIS, 1890) para incluir também o direito a autodeterminação informativa. Em outras palavras, passou-se a entender como pertencente ao direito à privacidade a noção de que as pessoas devem ter controle sobre a circulação de informações relacionadas a elas, determinando quem possui quais informações e para que podem ser usadas (STEINMÜLLER, LUTTERBECK, *et al.*, 1971).

Foi com essa preocupação que surgiram os marcos normativos relacionados à proteção de dados pessoais. Contudo, a maior parte dessas leis ainda é bastante recente. A lei europeia de proteção de dados, a Regulação Geral de Proteção de Dados ("GDPR", na sigla em inglês) está em vigor apenas desde maio de 2018 e a lei brasileira, a Lei Geral de Proteção de Dados Pessoais ("LGPD") desde setembro de 2020, por exemplo. Assim, vê-se um esforço dos entes públicos e privados em adaptar processos já existentes aos termos da lei.

Prática muito comum por lojas ou empresas do mercado brasileiro e mundial é o oferecimento de brindes, descontos e outros tipos de vantagens em troca do fornecimento de dados pessoais. O objetivo das empresas é, usualmente, coletar informações que permitam conhecer melhor os hábitos dos consumidores para então orientar suas atividades de produção e marketing. Essa prática é conhecida como *privacy as a product*, uma vez que considera que o titular[1] "vende" suas informações como se fossem um produto para o uso de um (ou mais) controladores de dados pessoais.[2]

Antes do advento da LGPD, essas práticas apenas eram realizadas de maneira desregulada pelos atores do mercado brasileiro. Contudo, desde o início da vigência da lei, observa-se esforço para continuar o tratamento dos dados de acordo com os termos da nova lei.

A LGPD define tratamento de dados pessoais como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018). Para que a realização de qualquer dessas atividades esteja de acordo com a lei, é necessário verificar se elas estão justificadas por uma das bases legais estabelecidas pela própria LGPD em seu artigo 7º, exceto quando os dados tratados incluírem dados sensíveis,[3] situação na qual o tratamento deverá ser justificado pelas bases legais do artigo 11.

As bases legais para tratamento de dados contidas na LGPD são: consentimento; cumprimento de obrigação legal ou regulatória; execução de políticas públicas; realização de estudos por órgãos de pesquisa; execução de contrato ou de procedimentos preliminares relacionados a contrato; exercício regular de direitos em processo judicial, administrativo ou arbitral; proteção da vida ou da incolumidade física; tutela da saúde, legítimo interesse do controlador; e proteção do crédito.

Para o tratamento de dados pessoais sensíveis, no entanto, não se pode usar como base legal a execução de contrato, o legítimo interesse do controlador ou a proteção ao

---

[1] "Titular" é definido pelo artigo 5º da LGPD como "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

[2] "Controlador" é definido pelo artigo 5º da LGPD como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

[3] "Dados pessoal sensível" é definido 5º como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

crédito. No entanto, a base legal relacionada a exercício regular de direitos abrange também o exercício desses direitos em contrato para o caso dos dados sensíveis e há também a adição de uma nova base legal, qual seja, a prevenção à fraude.

Dentre as bases legais disponibilizadas pela LGPD, duas parecem, *a priori*, potencialmente adequadas para justificar atividades nas quais dados pessoais são fornecidos pelo titular em troca de descontos, brindes ou vantagens. São elas: execução de contrato e consentimento. Isso porque as demais bases legais se resumem a ditames governamentais (cumprimento de obrigação legal; execução de políticas públicas; estudos por órgãos de pesquisa), ou tratamentos feitos sem necessidade de interação direta com o titular em questão (exercício regular de direitos; proteção da vida; tutela da saúde; legítimo interesse; proteção do crédito; prevenção à fraude), enquanto essas duas dependem de uma ação do titular de dados que autorize o tratamento.

Este artigo pretende analisar a possibilidade de utilização do consentimento do titular como base legal para tratamento de dados coletados por meio do oferecimento de brindes, descontos e outros tipos de vantagens ao titular. Não caberá ao escopo desse artigo pormenorizar a possibilidade de utilização da execução de contrato como base legal para realização das mesmas atividades, quando não houver coleta e tratamento de dados pessoais sensíveis.

A escolha do escopo fundamenta-se na observação prática de que a alternativa mais comum buscada pelos controladores de dados é justamente a obtenção do consentimento. Contudo, a Autoridade Helênica de Proteção de Dados Pessoais alertou para importância de selecionar e informação ao titular de dados pessoais a base legal correta para cada atividade de tratamento de dados pessoais, que está fortemente relacionada ao cumprimento dos princípios da transparência e da finalidade, especialmente ao se considerar que cada base legal possui efeitos diferentes na determinação dos direitos dos titulares (AUTORIDADE HELÊNICA DE PROTEÇÃO DE DADOS PESSOAIS, 2019, p. 1).

De acordo com a Autoridade Helênica, uma vez selecionado o consentimento como base legal, não é possível trocar para outra base pois o titular terá adquirido o direito de revogar seu consentimento, por exemplo. Assim, caso ele opte pela revogação, o titular deveria deixar de tratar os dados pessoais, o que não seria possível caso a base legal verdadeiramente aplicável fosse cumprimento de contratou ou legítimo interesse, por exemplo (AUTORIDADE HELÊNICA DE PROTEÇÃO DE DADOS PESSOAIS, 2019, p. 2).

Assim, este artigo estudará se de fato o consentimento pode ser utilizado como base legal nas relações *privacy as a product* (CAPÍTULO 2) e quais as principais consequências e cuidados que devem ser tomados pelos controladores ao conduzir esse tipo de atividade (CAPÍTULO 3).

2 CONSENTIMENTO

2.1 Regras Gerais do Consentimento

De acordo com as definições da LGPD, o consentimento do titular é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (BRASIL, 2018). Nos termos da lei, não há forma pré-determinada por meio da qual o consentimento deve ser obtido, de modo que o controlador pode escolher o método que melhor convier aos fluxos de suas atividades, normalmente escrito ou verbal. O controlador deve, no entanto, optar por métodos que permitam a fácil demonstração da manifestação de vontade do titular, uma vez que é dele o ônus de provar que o consentimento foi obtido e que estava de acordo com as determinações da lei (BRASIL, 2018).

É essencial salientar que o artigo 8º, §5º da LGPD determina que é vedado o tratamento de dados pessoais caso o consentimento, tendo sido a base legal escolhida para a atividade de tratamento, contenha vícios (BRASIL, 2018). Nesse sentido, faz-se relevante detalhar cada um dos aspectos do consentimento para entender exatamente o que é o consentimento que cumpre as exigências da LGPD.

Dado que este é um tema complexo, que a LGPD está em vigor apenas desde 17 de setembro de 2020 (não havendo larga jurisprudência sobre o tema) e que a Autoridade Nacional de Proteção de Dados (ANPD) ainda não está plenamente constituída (apesar de instituída em 27 de agosto de 2020), é útil estudar a experiência das autoridades europeias de proteção de dados pessoais e seus esforços em pormenorizar os aspectos do consentimento. Isso é possível uma vez que as autoridades europeias analisam a GDPR, que inspirou a LGPD e que propõe conceito de consentimento muito semelhante ao da lei brasileira, definindo-o como "qualquer indicação livre, específica, informada e

inequívoca da vontade do titular de dados, por meio da qual ele manifesta concordância com o tratamento de seus dados pessoais"[4] (CONSELHO DA EUROPA, 2016).

Dessa forma, passa-se a explorar cada um dos aspectos do consentimento válido, comuns à LGPD e à GPDR.

2.1.1 Consentimento Livre

A primeira e mais intuitiva exigência para a validade do consentimento é que ele seja livremente concedido pelo titular de dados. Isso porque o consentimento não deve ser adotado como mera formalidade, mas sim como forma de permitir o exercício de escolha dos titulares sobre o tratamento de seus dados pessoais. Assim, cabe ao controlador assegurar-se de que estão sendo garantidas ao titular as condições necessárias para que o seu consentimento seja de fato uma manifestação livre de sua vontade.

Por isso, via de regra, não é possível utilizar o consentimento como base legal para o tratamento de dados pessoais em situações nas quais haja desequilíbrio de poder entre controlador (e/ou operador), e o titular de dados pessoais (EDPB, 2020). Nos casos em que se tente fazer tal utilização o ônus de provar a liberdade do titular no momento de consentir com determinado tratamento (que já cabe ao controlador) deve ser capaz de superar também esse desequilíbrio de forças. O exemplo mais notório de situação de desequilíbrio de poder que impede o tratamento baseado no consentimento é nas relações em que o controlador (e/ou operador) seja empregador do titular, uma vez que a relação entre eles poderia fazer com que o titular se sentisse obrigado a conceder seu consentimento por medo de represálias que afetassem seu emprego (AUTORIDADE HELÊNICA DE PROTEÇÃO DE DADOS PESSOAIS, 2019). Na mesma toada, autoridades públicas somente podem usar o consentimento como base legal de maneira excepcional (EDPB, 2020).

Outra situação em que a liberdade do consentimento é negativamente afetada é quando o acesso a serviços e funcionalidades é condicionado à concessão do consentimento (EDPB, 2020). Isso significa que o controlador não pode "chantagear" o titular a consentir com atividades de tratamento ameaçando impedi-lo de usar serviços que não estejam relacionados com o uso dos dados pessoais.

---

[4] Texto original: "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"

Obviamente, serviços que dependam de dados pessoais para sua execução devem continuar sendo condicionados ao acesso a estes dados, desde que respeitados os princípios de proteção de dados, como a necessidade das informações coletadas. Contudo, funcionalidades ou serviços que independam do tratamento de dados pessoais, devem continuar sendo prestados ao titular, independentemente de possível recusa em fornecer seu consentimento.

Por exemplo, um aplicativo de controle de exercícios físicos que solicite o consentimento do usuário para acesso ao GPS para calcular distâncias percorridas durante corridas ou caminhadas poderá deixar de fazer esse cálculo caso o usuário não conceda seu consentimento, porém não poderá deixar de oferecer outras funcionalidades que independem da utilização dos dados de geolocalização do usuário.

A granularidade do consentimento também é essencial para garantir a liberdade do titular ao consentir com o tratamento de dados, uma vez que sua função é impedir que finalidades distintas sejam forçosamente associadas (EDPB, 2020). Em outras palavras, o consentimento não pode ser um pacote de "tudo ou nada", pois isso também poderia induzir o titular a concordar com o tratamento de seus dados pessoais para finalidades que ele, a princípio, não estaria de acordo, apenas por ter interesse na realização da atividade para outras finalidades. Por exemplo, este é o caso dos antigos termos de consentimento que, de uma só vez, solicitavam que o titular concordasse com comunicações relacionadas ao serviço e com o envio de e-mail marketing. O controlador deve encontrar maneiras de possibilitar que o consentimento seja obtido separadamente para cada uma das finalidades das atividades de tratamento a respeito das quais esteja consultando o titular.

Por fim, quando o consentimento for de fato livre, o controlador deve ser capaz de demonstrar que o titular poderá recusar conceder seu consentimento ou retirá-lo a qualquer tempo sem prejuízo. De acordo com a European Data Protection Board ("EDPB"), "prejuízos" nestes casos incluem o aumento de custos, desvantagens claras, enganação, coerção ou consequências negativas significativas (EDPB, 2020). Não se considera prejuízo, no entanto, as situações nas quais o titular deixa de receber vantagem quando o tratamento de seus dados pessoais era estritamente necessário para viabilizar tal vantagem.

2.1.2 Consentimento Específico

Apesar de a LGPD não definir consentimento com base na exigência de que este seja específico, como faz a GDPR, ela estabelece a necessidade de cumprir com esse critério em seu art. 8º, §4º, ao determinar que "o consentimento deverá referir-se a finalidades determinadas".

Exigir que o consentimento seja específico significa que, no momento da coleta desse consentimento, é necessário especificar a finalidade da atividade de tratamento de dados pessoais para a qual aquele consentimento é solicitado (EDPB, 2020). Tal finalidade deve ser descrita de maneira suficientemente detalhada para dar real visibilidade ao titular de como sua informação será usada. Assim, indicações vagas não são capazes de garantir o cumprimento dessa exigência para a validade do consentimento (WP, 2013, p. 16).

Esse aspecto do consentimento também se associa a sua já mencionada característica granular. Ou seja, deve ser obtido um consentimento diferente para cada uma das finalidades de tratamento para as quais sejam utilizados dados pessoais (EDPB, 2020). Mais de uma operação de tratamento de dados, todavia, pode ser realizada visando a mesma finalidade, caso em que o mesmo consentimento poderá ser utilizado para realização do tratamento em todas essas operações (EDPB, 2020, p. 14).

De maneira similar, caso o controlador já tenha legalmente coletado os dados pessoais do titular e deseje realizar atividade de tratamento para novos propósitos, ele deverá obter e armazenar novo consentimento que esteja de acordo com as disposições da legislação (EDPB, 2020).

A granularidade do consentimento é essencial para garantir a possibilidade de consentir somente com atividades cujos propósitos o titular esteja de acordo. Isso por sua vez ajuda a impedir que haja alargamento da função inicialmente indicada pelo controlador (fenômeno conhecido como "*function creep*"), levando a perda de controle do titular sobre seus dados pessoais (EDPB, 2020, p. 14).

2.1.3 Consentimento Informado

A validade do consentimento está diretamente ligada à compreensão do titular a respeito da atividade de tratamento de dados pessoais com a qual está consentindo. Por óbvio, somente é possível expressar vontades a respeito daquilo que se compreende. Disso decorre que o controlador deve fornecer informações sobre o tratamento de dados ao titular de dados.

Esse dever não pode ser cumprido de forma displicente. Há um conteúdo mínimo e uma forma correta para que essas informações sejam transmitidas ao titular de dados pessoais. No que tange o conteúdo, a EDPB estabelece que o informativo deve conter: identidade do controlador, finalidade de cada uma das atividades de tratamento de dados realizada, detalhamento dos dados que serão tratados, indicação de como exercer o direito de retirada do consentimento, detalhamento no caso de tomada de decisão automatizada, bem como riscos relacionados a possíveis transferências de dados pessoais (EDPB, 2020, p. 15). Na LGPD, lista similar se encontra no artigo 9º, com possibilidade de futura regulamentação adicional pela ANPD (BRASIL, 2018).

Além disso, o titular deve receber as informações acima especificadas por meio de simples acesso e de forma inteligível, utilizando linguagem clara. O controlador deve entender a qual público está se dirigindo ao fornecer tais informações e adaptar sua linguagem de maneira a garantir o entendimento dos titulares.

2.1.4 Consentimento Inequívoco

A LGPD não determinou formas específicas pelas quais o consentimento deve ser obtido, permitindo que o controlador opte por formatos escritos, verbais, eletrônicos ou analógicos da maneira que melhor convier ao fluxo de tratamento de dados estabelecidos pelo controlador (BRASIL, 2018).

Contudo, independente do meio escolhido, não deve restar dúvidas de que o titular de dados pessoais concordou com a atividade de tratamento de dados que baseia sua legalidade no consentimento desse titular. Para isso, é necessário que o consentimento seja obtido por meio de ação específica, e que não se confunda com outras ações do titular. Por exemplo, se o consentimento for obtido pelo preenchimento de *checkbox*, deve haver um *checkbox* específico em que o titular dê seu consentimento, que não pode ser unificado com *checkboxes* que se refiram a outros assuntos, por exemplo, o *checkbox* em que se declara não ser um robô.

2.2 Aplicação das regras gerais do consentimento aos tratamentos *Privacy as a Product*

A obtenção do consentimento em relações *privacy as a product*, ou seja, em relações nas quais o titular fornece dados pessoais em troca de vantagens como brindes ou descontos, deve observar as disposições acima para ser válida. Ou seja, deve-se garantir que o consentimento em questão seja livre, específico, informado e inequívoco.

No que diz respeito às exigências para que o consentimento seja "específico", é possível que o controlador encontre formas pela qual o titular manifeste, de maneira não vaga, sua concordância em relação a cada um dos usos dos dados coletados. Embora não baste inserir um checkbox dizendo apenas, por exemplo, "concordo com o tratamento dos meus dados pessoais para fins de marketing", o controlador pode ser mais específico redigir o texto da seguinte maneira: "concordo com o tratamento das respostas de pesquisa dadas por mim para determinação de estratégias de marketing". Assim, nesse exemplo, estaria satisfeito o requisito, o que demonstra que não há nenhum impedimento inerente a este requisito que o impeça de ser satisfeito em relações *privacy as a product.*

Em relação às exigências para um consentimento "informado", também é possível que o controlador siga todos os requisitos previamente apresentados quando do tratamento de dados coletados em troca de brindes, vantagens ou promoções. Para isso, ele deve elaborar aviso contendo todo o conteúdo mínimo detalhado acima em linguagem clara e que não pretenda enganar (ou dissimular) o porquê de aquela coleta de dados ser benéfica ao ponto de oferecer brindes e outras vantagens aos titulares. Também é necessário que o controlador diferencie e detalhe o uso feito dos dados cadastrais e de outros tipos de dados que venham a ser coletados (ex: respostas a questionários), pormenorizando também a relevância do uso de dados sensíveis, quando esse for o caso.

No que tange a necessidade de o consentimento ser inequívoco, basta que o controlador elabore maneiras de tonar a manifestação do titular, em qualquer forma, uma declaração assertiva e cumpra os requisitos de que ela seja apartada de outras ações do titular. Isso também é possível nas relações *privacy as a product*.

Em suma, não há nenhuma característica relacionada às exigências de que o consentimento seja específico, informado e inequívoco que impeça, *per se*, o tratamento de dados pessoais em relações *privacy as a product*. Basta que o controlador se atente e encontre formas de cumprir todos eles. O mesmo, contudo, não é verdade em relação ao aspecto de liberdade do consentimento.

Ainda que a coleta de dados não ocorra em situações de desequilíbrio de poder entre controlador e titular e que não haja condicionamento "tudo ou nada" para induzir o titular a concordar com múltiplas finalidades para o tratamento de seus dados, o funcionamento das relações *privacy as a product*, em sua essência, viola o requisito de que a recusa em consentir não opere em desfavor do titular de dados pessoais.

Ao recursar-se em fornecer seu consentimento para coleta de seu CPF durante uma compra de farmácia para obter desconto em determinados medicamentos, o titular

será obrigado a pagar um valor maior (e, por vezes, muito maior) do que a pessoa que concordou em compartilhar seu dado. Da mesma forma, aquele que não consente e não fornece respostas a questionários de marketing em troca de brindes, estará em desvantagem em relação aquele que o faz.

Ainda que, em um primeiro momento, pareça que o titular que não fornece seu consentimento em situações como as acima descritas não "perdem" nada, mas simplesmente "deixam de ganhar", não se pode esquecer que a questão está sendo analisada sob a perspectiva da liberdade do titular. Oferecer 50% de desconto em produtos que custa 100 reais, por exemplo, é uma forma extremamente persuasiva de induzir o titular de dados a consentir com atividades de tratamento com as quais ele preferiria não consentir; e levanta o questionamento de qual o valor real destes dados para as empresas. A liberdade do titular fica ainda mais prejudicada ainda em situações, por exemplo, de medicamentos de uso contínuo e/ou quando a situação econômica do titular for tal que o desconto de fato faça diferença em seu orçamento.

Todavia, mesmo que não se considere que a recusa em consentir opera em detrimento do titular de dados pessoais nas relações *privacy as a product*, o consentimento nessas situações ainda seria inválido e as operações de tratamento de dados pessoais ainda seriam ilegais pelo fato de que não existe a possibilidade de revogação do consentimento. Isso porque, já tendo disponibilizado a vantagem em troca do consentimento, o controlador não mais teria interesse em revogar a autorização dada pelo titular.

3 CUIDADOS DO CONTROLADOR AO OBTER O CONSENTIMENTO EM RELAÇÕES PRIVACY AS A PRODUCT

No entanto, diante da falta de doutrina e jurisprudência sobre o tema e devido ao fato de que a ANPD ainda não começou suas operações, ainda não há clara interpretação sobre as exigências do consentimento no Brasil. Assim, caso os controladores optem por manter atividades de tratamento de dados que funcionem na lógica de *privacy as product* coletando o consentimento do titular para tal, todas as outras garantias e princípios da LGPD devem ser cumpridos pelo legislador.

Dentre elas, destaca-se a necessidade de cumprir com o princípio da transparência. Ou seja, o titular deve ter pleno conhecimento de quais as finalidades para as quais são utilizados seus dados pessoais. Sobre esse tema, destaca-se o caso da Drogaria Araújo, que, antes mesmo do vigor da LGPD, foi inicialmente multada em mais de R$ 7 milhões

por condicionar descontos ao fornecimento do CPF pelos consumidores sem informá-los de que seus dados pessoais eram usados para abrir cadastros. O Ministério Público Estadual de Minas Gerais ("MPMG") argumentou que a Drogaria Araújo falhou em comunicar aos consumidores qual seria a verdadeira finalidade do uso dos seus dados pessoais, violando o princípio da transparência e informação previstos no Código de Defesa do Consumidor (artigos 4º e 6º) (G1 MINAS, 2018). O caso foi encerrado com um Termo de Ajuste de Conduta ("TAC").

Na mesma toada, foi sanciona em 1º de dezembro de 2020, lei estadual do Estado de São Paulo que determina, em seu artigo 1º, que farmácias e drogarias estão obrigadas a informar de forma clara e adequada, "sobre a abertura de cadastro ou registro de dados pessoais e de consumo, que condiciona a concessão de determinadas promoções". O artigo 2º da lei é ainda mais enfático ao estabelecer que "Nas farmácias e drogarias deverão ser afixados os dizeres 'PROIBIDA A EXIGÊNCIA DO CPF NO ATO DA COMPRA QUE CONDICIONA A CONCESSÃO DE DETERMINADAS PROMOÇÕES' em tamanho de fácil leitura e em local de passagem e fácil visualização" (SÃO PAULO, 2020). Assim, não fica claro se a intenção da lei é proibir o tratamento *privacy as a product* em farmácias em geral ou apenas impedir que haja tratamento para finalidades ocultas sobre as quais o titular de dados pessoais não tenha conhecimento prévio.

Apesar de ambos os casos se referirem a drogarias, ponto comum entre eles é a necessidade de informar precisamente ao titular todos os usos feitos dos dados fornecidos por ele em troca de vantagens. Não é possível realizar qualquer uso adicional dos dados sem que isso esteja explícito no momento da coleta.

4 CONCLUSÃO

Neste artigo, analisou-se a validade do consentimento obtido por controladores que coletem dados pessoais mediante o oferecimento de brindes, promoções ou outros tipos de vantagens. Concluiu-se que o consentimento não é a base legal adequada para justificar esse tipo de atividade de tratamento de dados, uma vez que a recusa do consentimento opera em detrimento do titular de dados pessoais, causando-lhe desvantagens que afetam diretamente sua liberdade em consentir com o tratamento.

Como consequência, os controladores, caso optem por seguir com as operações *privacy as a product*, devem deixar de coletar o consentimento do titular para não induzir

o titular a erro, acreditando que possui controle sobre a atividade de tratamento e, ao mesmo tempo, encontrar outra base legal alternativa que justifique a realização da atividade. Caso contrário, atuarão em desacordo com a legislação brasileira, o que pode implicar na aplicação de multas e sanções previstas tanto pela LGPD quanto por outras normas, como por exemplo, a legislação consumerista.

5 BIBLIOGRAFIA

AUTORIDADE HELÊNICA DE PROTEÇÃO DE DADOS PESSOAIS. Summary of Hellenic DPA's Decision No 26/2019. **Hellenic DPA**, 2019. Disponivel em: <https://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/DECISIONS/SUMMARY%20OF%20DECISION%2026_2019%20(EN).PDF>. Acesso em: 27 Novembro 2020.

BRASIL. **Lei Nº 13.709/18 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília: Congresso Nacional. Disponível em: https://bit.ly/2Zj5EDc. Acesso em: 01 de dezembro de 2020.

CONSELHO DA EUROPA. **Regulation (EU) N. 679/2016**. General Data Protection Regulation (GDPR). Estrasburgo: Parlamento Europeu e Conselho. Disponível em: https://gdpr-info.eu/. Acesso em: 04 de dezembro de 2020.

EDPB. **Guidelines 05/2020 on consent under Regulation 2016/679**. Version 1.1. ed. Bruxelas: European Data Protection Board, 2020.

G1 MINAS. **G1**, 2018. Disponivel em: <https://g1.globo.com/mg/minas-gerais/noticia/2018/12/05/drogaria-araujo-e-multada-em-mais-de-r7-milhoes-por-condicionar-descontos-a-fornecimento-de-cpf.ghtml>. Acesso em: 06 Dezembro 2020.

SÃO PAULO. **Lei n. 17.301 de 01 de dezembro de 2020**. São Paulo: Assembleia Legislativa do Estado de São Paulo. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/lei/2020/lei-17301-01.12.2020.html. Acesso em: 02 de dezembro de 2020.

STEINMÜLLER, W. et al. Grundfragen des Datenschutzes. **Anlage zu BT-Drucks**, v. VI/3826, 1971.

WARREN, S.; BRANDEIS, L. The Right to Privacy. **Harvard Law Review**, v. Vol. IV, n. 5, Dezembro 1890.

WP. **WP 29 Opinion 3/2013 on purpose limitation**. 00569/13/EN. ed. Bruxelas: Article 29 Data Protection Working Party, 2013.