CONSENTIMENTO E LGPD: DESAFIOS DIANTE DA HIPERVULNERABILIDADE DO CONSUMIDOR

CONSENT AND LGPD: CHALLENGES IN FACE OF CONSUMERS' HYPERVULNERABILITY

Alexandre Pereira Bonna[1]
Amanda de Moura Cañizo[2]
Giovana Ferreira Calzavara[3]

Resumo: o presente artigo objetiva analisar como a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018) conseguirá garantir o consentimento livre, expresso e informado em um cenário de hipervulnerabilidade do usuário-consumidor. Adota-se a metodologia hipotético-dedutiva, visto que o trabalho tem como escopo categorias jurídicas abstratas, como o consentimento e a hipervulnerabilidade, para posteriormente chegarmos à conclusão de como aquele se efetiva. O estudo evidencia importantes esforços de empresas em suas plataformas digitais, que explicam de forma acessível o tratamento de dados pessoais realizado, bem como possibilitam a escolha efetiva por parte do consumidor em relação à coleta dos seus dados. Tais esforços, como este artigo busca demonstrar, tentam coibir práticas comerciais abusivas recorrentes no meio digital, de forma a garantir a efetividade da aludida lei.

Palavras-chave: proteção de Dados Pessoais; hipervulnerabilidade do consumidor; consentimento; eficácia da LGPD; LGPD.

Abstract: the present article aims to analyze how the Personal Data Protection General Law (Law n. 13.709/2018) will be able to guarantee a free, expressed and informed consent in face of a hypervulnerable consumer-user. A hypothetical-deductive methodology has been adopted, given that the basis of this work lies with abstract legal categories, such as consent and hypervulnerability, in order to, posteriorly, arrive to the conclusion of how this right is made effective. The study shows important efforts taken by companies regarding the design of its digital platforms, in which they explain the processing of personal data performed in an accessible way, in addition to offering the consumer an effective choice with respect to their personal data collection. Such efforts, as this article seeks to demonstrate, try to impede abusive commercial practices recurring in the digital environment, aspiring to guarantee the effectiveness of the referred law.

Keywords: personal Data Protection; ponsumers' hypervulnerability; consent; LGPD's effectiveness; LGPD.

[1] Doutor em Direito pela Universidade Federal do Pará - UFPA com sanduíche pela *University of Edinburgh*, Professor de graduação e pós-graduação do Centro Universitário do Estado do Pará – CESUPA e da FACI-WYDEN. Advogado-Sócio do Escritório Coelho de Souza.
[2] Acadêmica de Direito no Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) de Brasília. Bolsista de Iniciação Científica (PROIC/2021) e integrante do Grupo de Estudos em Direito Internacional Privado e União Europeia na mesma Instituição. Estagiária jurídica na Joyce Dias Advocacia.
[3] Acadêmica de Direito pelo Centro Universitário do Estado do Pará – CESUPA. Estagiária jurídica na Malcher e Pedrosa Advocacia e no Escritório Barroso e Baidek.

Sumário: Introdução. 1. A importância e o cabimento da LGPD. 2. Obtenção do consentimento. 3. Vulnerabilidade nas relações de consumo informacionais 4. Como efetivar o consentimento diante da hipervulnerabilidade do consumidor nas plataformas digitais (aplicativos e plataformas de busca). Conclusão.

INTRODUÇÃO

Sabe-se que com o enorme avanço tecnológico experimentado pela humanidade ao longo dos últimos séculos, foi possível a construção da chamada "sociedade da informação", que recorre ao intenso uso da tecnologia e da inteligência artificial para a coleta, armazenamento, tratamento e manipulação de dados pessoais, os quais são informações que nos diferenciam na sociedade e que estão na esfera privada, como o número do celular, endereço, CPF, conta bancária, preferências, gostos, buscas recentes, compras, etc.

Antes da Lei Geral de Proteção de Dados (Lei n. 13.709/2018), embora existissem diplomas normativos de proteção da privacidade e dos dados pessoais, como a Constituição Federal de 1988, o Código de Defesa do Consumidor (Lei n. 8.078/1990) e o Marco Civil da Internet (Lei n. 12.965/2014), não havia uma lei própria para regular a temática de forma completa, estabelecendo os requisitos para o tratamento de dados pessoais, criando órgãos para efetivar e fiscalizar o respeito aos dados pessoais, etc.

Portanto, seguindo a tendência de outros países, como o México, os EUA e os membros da União Europeia, o Brasil editou a sua LGPD, a qual passou a ter vigência no dia 16/08/2020, com a ressalva apenas em relação ao início de vigência das sanções administrativas, que só começarão a valer no dia 01/08/2021. Embora se saiba que a LGPD possui aplicabilidade para qualquer relação jurídica envolvendo pessoas naturais e/ou jurídicas, é no campo das relações de consumo – que são marcadas pela vulnerabilidade do adquirente de produtos e serviços – que se manifesta o ponto mais sensível de efetividade da referida lei, haja vista que um dos aspectos mais importantes advindos com a nova lei é o consentimento livre, expresso e informado (art. 5º, XII e art. 7º, I, da LGPD) previamente ao armazenamento e tratamentos dos dados do titular.

Nessa linha, considerando que há muitas práticas comerciais abusivas que violam a liberdade do consumidor (como a venda casada), assim como o seu direito a informações claras e acessíveis, somado a um exército de pessoas hipervulneráveis (os idosos, as crianças, os analfabetos, pessoas com deficiência mental, pessoas com saúde debilitada e pessoas sem

conhecimento mínimo de tecnologias), há um grande potencial de inefetividade da aludida lei, se não for objeto de maiores reflexões.

Diante desse contexto, surge o problema de pesquisa do presente artigo, que tem como questão básica: como é possível efetivar o consentimento livre, expresso e informado diante de um cenário de hipervulnerabilidade? Como questões secundárias: a) qual o conteúdo jurídico do consentimento livre, expresso e informado? b) Qual o conceito e a incidência da chamada hipervulnerabilidade? c) Qual a forma mais adequada para requerer o consentimento do consumidor?

A relevância em investigar o referido problema de pesquisa está no fato de que ainda não há jurisprudência sólida e farta sobre os contornos hermenêuticos para o consentimento. Ademais a Autoridade Nacional de Proteção de Dados foi recém criada e ainda não manifestou o seu poder regulamentar, que envolverá diretivas para auxiliar o integral cumprimento da lei. Por fim, é imprescindível realizar um cotejo entre o diploma de proteção do consumidor e o seu pilar da vulnerabilidade com os desafios advindos com a LGPD.

A pesquisa tem como objetivo geral investigar como é possível efetivar o consentimento livre, expresso e informado diante de um cenário de hipervulnerabilidade. Como objetivos específicos refletir sobre o conteúdo jurídico do consentimento livre, expresso e informado, aprofundar o conceito e a incidência da chamada hipervulnerabilidade, assim como desbravar qual a forma mais adequada para requerer o consentimento do consumidor.

O método que será utilizado no presente artigo será o hipotético-dedutivo, haja vista que o trabalho irá partir de categorias jurídicas abstratas (consentimento, hipervulnerabilidade) para alcançar conclusões mais particularizadas (como efetivar o referido aspecto no campo da hipervulnerabilidade).

1. A IMPORTÂNCIA E O CABIMENTO DA LGPD

O maior caso de vazamento de dados da história ocorreu em 2013, na plataforma de busca e rede social *Yahoo!*, comprometendo as informações pessoais de três bilhões de usuários, incluindo senhas, e-mails, telefones celulares, respostas às perguntas de segurança, e mais.[4]

Quase metade da população mundial foi atingida pelo ataque cibernético, e levando em consideração a quantidade de usuários que utilizam as demais redes sociais (instagram,

[4] Disponível em: < https://link.estadao.com.br/noticias/cultura-digital,invasao-de-hackers-afetou-todos-os-3-bilhoes-de-usuarios-do-yahoo,70002026724>. Acesso em 10 dez 2020.

facebook, whastapp), estes números poderiam ter sido ainda mais expressivos. Nessa linha, a proteção de dados pessoais nunca foi um tópico tão sensível e importante quanto hoje.

Na Era Informacional, percebemos um maior intercâmbio de informações[5], seja entre particulares, entre particular e Estado ou particular e empresa. Decerto que a preocupação do direito neste novo modelo econômico, cujo objeto mais valioso se tornou o dado pessoal (*data-driven economy*), seria proteger o indivíduo na relação em que se encontra mais vulnerável, *i.e.*, frente à empresa (enquanto consumidor) ou ao Estado (enquanto cidadão).

No tocante à atividade empresarial que se volta à coleta de dados pessoais, nota-se um cenário de monopólios e oligopólios[6], que até recentemente não era regulado nem respondia a uma autoridade central em muitos países. Esta lacuna jurídica permitiu a ocorrência de, por exemplo, "ofertas personalizadas" (*personalized offerings*), pelas quais uma empresa poderia coletar os dados pessoais de um indivíduo e ofertar preços diferentes, baseado no local onde mora, nas compras que regularmente faz, em quantas pessoas compõem o núcleo familiar, etc. Nesta senda, a empresa *Staples* já ofertou preços com desconto em áreas que houvesse lojas rivais a um raio de 32km de distância da localização do cliente; a empresa *Office Depot* admitiu ter usado o histórico de busca de seus consumidores bem como suas localizações para determinar o preço de suas ofertas; e a empresa aérea *Orbitz* ficou famosa em 2012 quando se descobriu que ofertava passagens a preço mais alto para usuários da *Apple* do que para usuários *Microsoft*.[7]

> Por mais que ainda não seja possível compreender a total extensão do poder econômico, político e social que decorre dos dados e da sua utilização, já se percebe quão grande ele pode ser. Daí a afirmação de Alec Ross de que as escolhas sobre como vamos gerenciar e administrar os dados na atualidade são tão importantes quanto as decisões sobre o gerenciamento da terra durante a Era Agrícola ou da indústria durante a Era Industrial (FRAZÃO; TEPEDINO; OLIVA, 2020, p. 25).

Dito isso, a regulamentação dos dados surge não só como um importante mecanismo antitruste (em relação aos monopólios e oligopólios formados no mercado tecnológico), mas também como um instrumento de proteção do consumidor hipervulnerável (conceito que será debatido mais à frente no artigo).

---

[5] Tendo o fenômeno do *Big Data* e do *Big Analytics* permitido um processamento de dados em maior escala, mais célere e mais eficaz.

[6] O *Facebook, e.g.*, é uma empresa que detém os quatro aplicativos mais baixados da década; o *Google* compõe 92% das ações do mercado de ferramenta de buscas.

[7] Disponível em: <https://www.theguardian.com/commentisfree/2016/dec/06/cookie-monsters-why-your-browsing-history-could-mean-rip-off-prices>. Acesso em 10 dez 2020.

> Nesse diapasão, "certamente se compreenderá melhor o papel e o alcance da Lei Geral de Proteção de Dados e da sua missão de encontrar um equilíbrio entre inovação e eficiências econômicas, por um lado, e preservação dos direitos dos indivíduos e da própria sociedade, por outro" (FRAZÃO; TEPEDINO; OLIVA, 2020, p. 25).

Criada com vistas a regular o processamento de dados pessoais, é mister, primeiramente, definir o que a lei a entende por "dado pessoal". Em seu artigo 5º, I, a lei conceitua dado pessoal como "informação relacionada a pessoa natural identificada ou identificável". Isto posto, pode se extrair desse dispositivo que estarão sujeitos à LGPD os dados identificados e pseudonimizados[8], mas não os dados anonimizados (v. art. 5º, III, LGPD).

Insta salientar que a lei também trata sobre o "dado pessoal sensível" 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" conforme exposto em seu artigo 5º, II.

Partindo dessa premissa, cabe à LGPD regular esse tratamento[9] realizado por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio[10], do país de sua sede ou do país onde estejam localizados os dados (v. art. 3º, LGPD), desde que a operação de tratamento seja realizada no território nacional (v. art. 3º, I, LGPD), a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional (v. art. 3º, II, LGPD) ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional (art. 3º, III, LGPD).

Por sua vez, a LGPD não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos[11] (v. art. 4º, I, LGPD); para fins exclusivamente jornalísticos e artísticos[12] (v. art. 4º, II, "a", LGPD) ou acadêmicos (v. art. 4º,

---

[8] São aqueles que não podem ser atribuídos a um titular específico sem recorrer a informações suplementares, e desde que essas informações suplementares (i) sejam mantidas separadamente; (ii) e estejam sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular.

[9] "Tratamento: 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" (v. art. 5º, X, LGPD).

[10] Desta feita, o meio pode ser físico ou digital, embora a lei tenha sido desenvolvida em um cenário preocupado precipuamente com o consumidor digital e o mercado de *Big Techs*.

[11] Um indivíduo pode receber diversos dados em uma conversa, *e.g.*, inclusive dados sensíveis, mas alguma violação à esfera íntima da pessoa neste cenário ensejaria o pedido de danos morais (v. art. 186, CCB), mas não incidiria a LGPD.

[12] Vale aqui ressaltar que a LGPD só não incidirá na atividade jornalística por excelência, mas poderá incidir sobre a atividade empresarial. *I.e.*, a LGPD pode incidir sobre empresa jornalística que monitore o padrão de comportamento dos usuários em seu site, que manuseie os dados pessoais dos usuários para fins comerciais. De igual modo a LGPD incidirá caso tal empresa forme banco de dados de seus usuários cuja destinação não esteja clara quanto ao uso, *e.g.*

II, “b”, LGPD); para fins exclusivos de segurança pública (v. art. 4º, III, “a”, LGPD), defesa nacional (v. art. 4º, III, “b”, LGPD), segurança do Estado (v. art. 4º, III, “c”, LGPD) ou atividades de investigação e repressão de infrações penais (v. art. 4º, III, “d”, LGPD); bem como a LGPD não se aplica aos dados pessoais provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei (v. art. 4º, IV, LGPD).

Como visto, a LGPD não se aplica somente às relações jurídicas de consumo, nem tampouco as relações travadas no meio digital. Porém, em harmonia com o objeto do artigo, a presente pesquisa irá se debruças apenas sobre as nuances da aplicação da lei no âmbito consumerista, como explicado na introdução.

2. OBTENÇÃO DO CONSENTIMENTO

Destarte, cumpre analisar o art. 7º, I, da LGPD, segundo o qual uma das formas de legitimação para uso de dados pessoais por agentes de tratamento é mediante o fornecimento de consentimento prévio pelo titular, não se contentando com qualquer tipo de concordância, pois o artigo 5º, XII, reza que o consentimento nos moldes da lei deve se dar por uma manifestação de vontade livre, informada, inequívoca e, por vezes, específica e destacada.

Frise-se que o que é garantido ao titular não é o consentimento em si, mas sim o uso legítimo, transparente e seguro de seus dados, que pode ou não ser realizado mediante a coleta do consentimento a depender da situação apresentada.

Neste sentido, consentir se tornou tarefa difícil em uma sociedade onde temos como mola propulsora a extração de dados pessoais, os quais cada vez mais estão sendo considerados o novo petróleo da economia. Tal assertiva, encontra embasamento no comportamento de entidades denominadas como *Data Brokers*[13], que nada mais fazem do que coletar, processar e vender informações a terceiros, muitas vezes sem interação prévia e/ou conhecimento de seus titulares.

[13] Empresa que coleta, armazena, processa, “enriquece” (com mais variáveis e classificações) dados e os vende para diversos fins. Disponível em: <https://tarciziosilva.com.br/blog/voce-sabe-o-que-sao-data-brokers-quem-te-classifica-e-define-seus-escores-de-credito/>. Acesso em 15 jan. 2021.

Importante salientar que se fala em extração, de maneira cirúrgica, vez que segundo a professora Shoshana Zuboff (2019, p. 17-25 apud FRAZÃO; TEPEDINO; OLIVA, 2020, p. 28) "(...) esta expressão traduz, de forma mais fidedigna, a circunstância de que os dados são normalmente retirados de seus titulares sem o seu consentimento, sem a sua ciência e sem a devida contrapartida". De origem do Latim *Extrahere*, que no português se traduz como "retirar para fora", torna-se preocupante que na sociedade atual a circulação de dados careça de uma aquiescência inequívoca e consciente.

Conforme destaca Bruno Bioni (2021), o consentimento é o vetor central para a coleta de dados até hoje, sendo certo que este subentende um protagonismo do indivíduo, premissa contraditória diante de sua vulnerabilidade diante do meio informacional, como será demonstrado adiante.

Consentir, no sentido em que a LGPD nos aponta, trata-se de um momento de autodeterminação informativa[14], onde o particular faz a manifestação expressa de sua vontade orientando onde, quando, por quem e com qual finalidade suas informações serão utilizadas. Neste sentido, é notória a busca não mais por um consentimento implícito (onde os indivíduos por meio de determinados comportamentos são levados a uma estante de consentimento – a exemplo disso, temos casos onde os titulares preenchem as lacunas de *pop up* que constam com extensos contratos em reduzidas letras e que se assinam com um toque), mas sim a um consentimento informado (entendido de forma restrita) como maneira de antecipação de riscos de violação à privacidade e busca por um caráter preventivo.

De informado, extraímos que se fazem necessários instrumentos de conhecimento acessível que proporcionem aos sujeitos destes dados entendimento eficaz acerca do que estão permitindo que seja feito com suas informações. Instrumentos estes, que sirvam como meios de auxílio que lhes garantam poder de discernir quais suas variáveis no momento de decisão. Também devem ser garantidas, segundo o artigo 18, VIII, da LGPD, informações sobre a possibilidade de não ser fornecido o consentimento e quais as consequências de tal negativa.

Mister destacar que, inclusive em caso de o titular entender por efetuar o fornecimento de seus dados pessoais, este deve ser advertido sobre a possibilidade de revogá-lo mediante manifestação expressa, do modo mais acessível possível, assim como de forma gratuita, (v. art. 18, IX, LGPD).

---

[14] Surge, na terceira geração de leis de proteção de dados pessoais, o conceito de *autodeterminação informativa*, trazido pela decisão do Tribunal Constitucional Alemão a respeito da Lei do Recenseamento de População, Profissão, Moradia e Trabalho de 1982 e presente no art. 2º, II, da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), de modo a garantir ao indivíduo proteção, a partir da necessidade de prévio consentimento do titular para a coleta, armazenamento e tratamento de informações pessoais.

Isto posto, não é passível de esquecimento o fato de que nos encontramos em uma era de globalização, na qual se nota uma mundialização de conteúdo e de acesso ao mesmo, mas que em contrapartida em nosso País ainda se esbarra com focos de subdesenvolvimento notório. Dito isso, os meios de assessoria devem ter formatação equivalente com esta realidade, posto que a mesma não pode ser usada em desfavor dos indivíduos que dela fazem parte. Seguindo nesta lógica, no artigo 8ª, parágrafo 2º do diploma supracitado, o legislador dispõe que:

> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

Nesta esteira, a finalidade na qual cada base de dado será utilizada é condição *sine qua non* para um consentimento efetivo. Aliado a isso, a Lei nº 13.709/2018 alinha que todos os fins para os quais o controlador dos dados fornecidos queira utilizar estes elementos, devem ser claramente delimitados e em quantidade satisfatória ao titular de maneira prévia ao consentimento, visto que, na ausência da determinação de qualquer objetivo haverá a necessidade de apresentação de novo instrumento visando aceite. A norma ainda adverte em seu artigo 8º, parágrafo 4º:

> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

Sob esta perspectiva, a exteriorização de vontade deve ser feita de maneira expressa por parte do titular dos dados, adquirindo assim a conotação de inequívoca. Tal expressão, tem que encontrar forma na qual não restem dúvidas de que o titular está concordando com aquela utilização. Desta forma, a LGPD elenca que este ato de escolha deve ser feito de maneira escrita ou por outro meio que demonstre a manifestação de vontade do titular (por exemplo: áudio, vídeo). Sendo que, caso a forma escolhida seja a escrita, deve esta constar em cláusula destacada das demais. Infere-se, portanto, que na omissão do titular, não mais podem ser retiradas conclusões de consentimento, mas tão somente de seus atos feitos de maneira positivada.

Demais disso, no que tange ao adjetivo livre, este busca efetivar um consentimento granular, de modo que as autorizações do indivíduo devem ser, o máximo possível, fragmentadas quanto ao fluxo de seus dados pessoais. Interessante observar que “o leque de opções dessas ferramentas oxigena processos de tomadas de decisões antes sufocados pela lógica binária *take-it* ou *leave-it*” (BIONI, 2021, p. 278).

Isso acaba por ampliar seu poder de barganha, ainda que o fornecimento de certos dados pessoais possa ser uma condicionante para o acesso a algum produto ou serviço. Nesse cenário,

“o cidadão deve ser informado a esse respeito e sobre os meios pelos quais ele pode exercer seus direitos, dentre os quais a revogação do consentimento.” (BIONI, 2021, p. 279).

Ademais, há de se salientar que o caráter livre da manifestação de vontade é tamanho, que pode vir a ser revogado a qualquer momento, sem necessidade de motivação alguma. Sendo este, realizado por procedimento isento de custos e que tenha a forma mais facilitada possível a realidade do titular. Este entendimento é reiterado, pelo artigo 8, parágrafo 5º do mesmo diploma legal supramencionado:

> § 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.

Somado a isso, no que tange ao tratamento de dados pessoais sensíveis (v. art. 11, I, da LGPD), o consentimento ainda ganha mais dois requisitos, quais sejam: ser destacado e específico.

Como destacado, faz-se necessário que o consentimento seja garantido de forma separada. Sendo assim, corporificado em instrumento *a priori*[15] apartado das demais cláusulas contratuais[16].

No que tange a ser específico, este exige mais assertividade do titular, *i.e.*, uma carga participativa maior. Neste sentido, a LGPD impõe este requisito nas hipóteses de envolvimento de terceiros sem relação direta com o titular (v. art. 7º, §5º); condição de vulnerabilidade do titular (v. art. 14, §1º); transferência internacional para país sem mesmo nível de do Brasil (v. 33, VIII). Dentre as quais, interessa ao presente artigo a condição de vulnerabilidade do titular, no que se entende crianças e adolescentes; caso em que o consentimento também deverá ser fornecido em destaque pelos pais.

Por fim, diante de todos os elementos que devem ser considerados para que o consentimento seja outorgado de forma válida, mostra-se relevante a análise da hipervulnerabilidade – a qual será objeto de análise minuciosa no tópico seguinte – do fornecedor do dado frente ao operador do mesmo, como maneira de garantir que a disponibilização ocorra sem embaraços.

---

[15] A forma pela qual isto será garantido na internet ainda carece de um maior posicionamento pela ANPD, no sentido de definir se será feito por meio de texto em negrito, se haverá necessidade de oferecimento de outra *checkbox* ou se será disponibilizado em tópico próprio da política de privacidade, por exemplo.

[16] O consentimento destacado aparece em 4 ocasiões na LGPD: (i) para consentimento por escrito de dados pessoais (art. 8º, § 1º); (ii) para dados sensíveis (art. 11, I); (iii) para transferência internacional de dados pessoais (art. 33, II, "a"); e (iv) para coleta de dados de crianças e adolescentes (art. 14, §1º).

3. VULNERABILIDADE NAS RELAÇÕES DE CONSUMO INFORMACIONAIS

Tendo em vista que o objeto da pesquisa diz respeito aos desafios de efetividade do consentimento diante da vulnerabilidade do consumidor no meio informacional, especificamente diante de plataformas digitais mantidas por particulares, é importante registrar que o Poder Privado é tão ou mais ameaçador que o Poder Público em matéria de violação de direitos. Nesse sentido:

> Em razão das modificações sociais e da evolução tecnológica, a discussão sobre os danos causados pelo processamento e fluxo de dados na sociedade não se restringe mais à ameaça do enorme poder do Estado, expresso na figura do "Big Brother" de Orwell, mas abrange hoje também o setor privado, que utiliza massivamente dados pessoais para atingir os seus objetivos econômicos (MENDES, 2014, p. 83).

As modificações sociais citadas *supra* se referem à passagem ocorrida na década de 70, de uma economia voltada para produção em massa para a "economia da informação pessoal" ou da "massa customizada"[17]. Este novo modelo econômico é flexível e se pauta na customização da oferta, de modo que as empresas passam a investir em uma produção e em um *marketing* personalizados para cada consumidor. Isto é, "adquirem a capacidade de ofertar produtos especializados, singularizados e altamente qualificados, em função do mercado e do consumidor, bem como de direcionar-lhe a sua publicidade" (MENDES, 2014, p. 89).

Ocorre que, para atingir estes objetivos, a coleta de dados pessoais é essencial, e, sob esta perspectiva, reitera-se que o novo insumo de produção se tornou o dado pessoal, possibilitando o estabelecimento de um imperativo de vigilância no mercado.

> Antigamente, o termo vigilância era utilizado para se referir a fenômenos específicos de controle, relacionados a investigações policiais e a serviços de inteligência governamentais. Atualmente, com o enorme processamento de dados pessoais pelas empresas para a análise detalhada e tomada de decisão, a vigilância tornou-se uma característica do cotidiano na sociedade contemporânea. (...) A consequência disso é a classificação das pessoas em categorias de acordo com a avaliação de seus riscos e a discriminação do acesso a determinados bens e serviços, de modo a afetar significativamente as suas chances de vida (MENDES, 2014, p. 91).

[17] Isso ocorreu porque "o modo de produção de massa mostrou-se instável diante de variações abruptas do mercado, pois, em razão do grande investimento inicial necessário, quaisquer interrupções ou diminuições bruscas na produção poderiam causar grande prejuízo. O modelo flexível, por outro lado, mesmo em contextos instáveis, permite a manutenção do nicho produtivo, a adaptabilidade às demandas e às variações do mercado e a utilização plena da linha de produção implantada, em razão de sua produção flexível" (MENDES, 2014, pp. 86 e 87).

A empresa Decolar.com, por exemplo, foi condenada, em 2018, ao pagamento de R$ 7.500.000,00 (sete milhões e quinhentos mil reais) por praticar *geopricing* e *geoblocking* ao diferenciar o preço de acomodações e negar oferta de vagas existentes em razão da localização geográfica do consumidor. Houve ainda, neste caso, discriminação de oferta com base na etnia do consumidor, visto que a empresa favoreceu argentinos em detrimento de brasileiros.[18]

Tais práticas são consideradas abusivas e causam desequilíbrio no mercado e nas relações de consumo, sendo vedadas pelo art. 39, IX e X, do CDC. Ademais, como o consumidor teve suas oportunidades diminuídas em razão de informações armazenadas em bancos de dados e utilizadas de forma discriminatória, se o caso em apreço tivesse ocorrido sob a vigência da LGPD, estaria em violação direta ao artigo 6º, IX, que prevê a não-discriminação como um princípio a nortear as atividades de tratamento de dados pessoais.

Sob esta perspectiva, a relação jurídica de consumo poderá ser definida como aquela firmada entre consumidor e fornecedor, a qual possui como objeto a aquisição de um produto ou a contratação de um serviço (BOLZAN, 2014, p. 49).

No campo dos dados pessoais, esta relação estará configurada quando do oferecimento de informações pessoais do consumidor aos fornecedores de serviços no mercado de consumo na forma de destinatários finais, seja mediante aceite de termos de uso, políticas de privacidade, ou pelo preenchimento de cadastros para realização de compras ou criação de perfis.

Em tal conjuntura, assim como em qualquer das relações de consumo, o consumidor se encontra na figura de parte vulnerável, sendo certo que a compreensão deste princípio "(...) é pressuposto para o correto conhecimento do Direito do consumidor e para a aplicação da lei, de qualquer lei, que se ponha a salvaguardar o consumidor" (MORAES, 2009, p. 13).

Com efeito, há tempos não se pode falar mais no poder de barganha antes presente entre as partes negociais, nem mesmo em posição de equivalência nas relações obrigacionais existentes na sociedade de consumo (TARTUCE; ASSUMPÇÃO, 2015, p. 62).

Isto posto, em razão de ser característica tão evidente, acabou-se por chegar em subespécies de vulnerabilidade, dentre as quais: (i) a vulnerabilidade técnica, a qual é demonstrada pela carência de conhecimento técnicos do consumidor sobre o produto ou serviço ofertado, sendo de monopólio do fornecedor a totalidade das informações acerca dos bens vendidos ou do serviço prestado; (ii) a vulnerabilidade jurídica ou científica, em que percebemos a carência do consumidor de conhecimentos jurídicos técnicos, o que lhe dificulta

---

[18] BRASIL. *Decolar.com é multada por prática de geo pricing e geo blocking*. Disponível em: <https://www.justica.gov.br/news/collective-nitf-content-51>. Acesso em: 10 dez. 2020.

entender cláusulas de contratos e discutir os termos em uma posição de paridade, bem como, no âmbito jurisdicional, uma vulnerabilidade pela habitualidade da litigância de que goza o fornecedor; (iii) a vulnerabilidade fática, segundo a qual uma circunstância torna o consumidor vulnerável, podendo ser econômica ou concorrencial; e, por último, (iv) a vulnerabilidade informacional, configurada pelos sistemas informatizados, pela posição desigual do consumidor diante da linguagem hermética das máquinas.

Neste sentido, Fabrício Bolzan (2014, p. 168) leciona:

> Quer a vulnerabilidade informacional seja considerada como modalidade autônoma de vulnerabilidade, quer como subespécie da vulnerabilidade técnica, o importante é deixar bem clara a sua relevância no mundo contemporâneo, em que o consumidor é constantemente persuadido em sua liberdade de opinião pelas técnicas agressivas da oferta e por ser o fornecedor o manipulador e conhecedor dessas informações, evidenciando uma relação completamente díspar e merecedora da proteção do mais frágil também no aspecto da informação.

Como se observa, "a vulnerabilidade do consumidor nesse processo de coleta e tratamento de dados pessoais é tão patente que se cunhou a expressão 'consumidor de vidro' para denotar a sua extrema fragilidade e exposição no mercado de consumo (...)" (MENDES, 2014, p. 93), à medida que suas informações pessoais passam a determinar as suas oportunidades de vida.

E, mesmo que respeitada a LGPD (porquanto pensada como um instrumento jurídico para diminuir tal vulnerabilidade), o consumidor ainda enfrenta desafios na compreensão de como se dará o tratamento de seus dados pessoais, pois de nada adianta a transparência formal se não for, de fato, clara, precisa e facilmente acessível (v. art. 6º, VI, LGPD), especialmente em relação aos consumidores hipervulneráveis (*i.e.*, aqueles consumidores que são também hipossuficientes, nos termos do art. 39, IV, do CDC: os idosos, as crianças, os analfabetos, os pessoas com deficiência mental, pessoas com saúde debilitada, e, especificamente no campo digital, defende-se neste artigo, a inclusão daqueles sem conhecimentos mínimos de informática/internet).

A hipervulnerabilidade é a situação social fática e objetiva de agravamento da vulnerabilidade da pessoa física consumidora, por circunstâncias pessoais aparentes ou conhecidas do fornecedor (SCHMITT, 2014, p. 233), que geram a necessidade de oferecer maior proteção a estes indivíduos, inclusive no meio digital. Neste sentido:

> O modus de vida atual não deixa margem de dúvidas acerca das dificuldades desses sujeitos de direitos, ante a potencialização de lesões aos seus interesses, advindas do crescimento do comércio eletrônico e do incremento do ambiente virtual na vida de relação, onde a velocidade das mudanças impõe barreira quase intransponível àqueles

> dotados de uma natural fragilidade física, psicológica ou até mental (SCHWARTZ, 2016).

É comum, por exemplo, instituições financeiras obterem acesso ao banco de dados do INSS com vistas a oferecer empréstimo consignado a recém-aposentados de maneira imprecisa e irregular. Como efeito disso, o INSS editou a instrução normativa nº 100, impedindo o contato de instituições financeiras com aposentados nos primeiros 180 dias contados da concessão do benefício, bem como inaugurou uma força-tarefa, com o apoio da Polícia Federal e do Ministério Público Federal, para apurar como estaria ocorrendo este vazamento de dados.[19]

Na Inglaterra, em janeiro de 2020, houve um dos maiores vazamentos de dados governamentais da história do país, no *Department of Education* (Ministério da Educação) 28 milhões de crianças tiveram seus nomes, idades e endereços compartilhados com empresas de apostas *online*, que utilizaram estes dados para aumentar o número de apostadores jovens em suas plataformas ilegalmente. [20]

À luz dos exemplos expostos, reitera-se a situação especialmente vulnerável em que estas pessoas se encontram no mercado atual, sendo imperativo, em especial, que os comércios eletrônicos desenvolvam suas plataformas pensando nos consumidores hipervulneráveis, de modo a promover a inclusão destes indivíduos no mercado digital com acuidade.

4. COMO EFETIVAR O CONSENTIMENTO DIANTE DA HIPERVULNERABILIDADE DO CONSUMIDOR NAS PLATAFORMAS DIGITAIS (APLICATIVOS E PLATAFORMAS DE BUSCA)

Como visto *supra*, diversos empecilhos podem dificultar que o consumidor exerça o consentimento, desde características pessoais (como é o caso dos consumidores hipervulneráveis) a pressões sociais (à medida que, conforme indaga Laura Schertel Mendes (2014, p. 41), “o exercício de sua privacidade informacional requer abdicar de facilidades do mercado de consumo") ou a falhas na prestação de informações por parte da empresa.

Nesse cenário, perceptível a necessidade de se tratar as medidas de proteção de dados adotadas no meio digital, porquanto latente a complexidade que permeia o fluxo das informações coletadas neste âmbito. Nesta tônica, Bruno Bioni apresenta a pesquisa *Mental*

---

[19] Disponível em: < https://gauchazh.clicrbs.com.br/grupo-de-investigacao/noticia/2019/05/origem-do-acesso-a-informacoes-sigilosas-de-aposentados-provoca-duvidas-cjvhbnqdr02s001ma7siuce80.html>. Acesso em: 16 dez. 2020.

[20] Disponível em: < https://www.dailymail.co.uk/news/article-7904287/Betting-firms-granted-access-database-28-MILLION-children.html>. Acesso em: 16 dez. 2020.

Models, realizada pelas universidades de *Stanford* e *Carnegie Mellon*, por meio da qual se extrai que "64% dos entrevistados consideraram ser invasiva a vigilância sobre as suas as atividades *online*" (2021, p. 242).

A partir dessa constatação, o presente artigo propõe apresentar formas através das quais as empresas poderão mitigar a vulnerabilidade do consumidor no meio digital e promover a manifestação de um consentimento adequado às previsões trazidas pela LGPD[21].

No que toca à coleta de dados realizada por *websites*, o primeiro termo que virá à mente de muitos usuários é, por certo, de difícil compreensão – os *cookies*, cada vez mais conhecidos. Em uma pesquisa citada pelo autor Bruno Bioni (2021, p. 250-252), conduzida pela Universidade de Bochum, constatou-se um aumento exponencial no uso de avisos de *cookies* desde a implementação da GDPR, na Europa. Na mesma pesquisa, chegou-se à conclusão de que a maioria dos sites: não ofertavam opções de recusa de coleta de dados (recusa do uso de *cookies*), não fragmentavam opções para o consentimento de coleta de dados distintos (*cookies* funcionais, de marketing, etc.), as opções utilizavam um modelo *opt-out*, bem como tanto o *layout* quanto a escrita da página eram de difícil compreensão.

Sobre o tema, pode-se partir, primeiramente, de um desenho simples de coleta de dados pessoais, sendo estes não sensíveis e dos quais seja necessária a manifestação do consentimento do usuário na plataforma de busca.

Assim sendo, ressalte-se que, para que o consentimento exercido pelo consumidor seja inequívoco (v. art. 5º, XII, LGPD), a empresa não poderá tratar os dados do titular automaticamente, sem sua manifestação expressa. Na esfera digital, por exemplo, se o usuário não clicar no botão de aceite de *cookies* e permanecer navegando no *site*, esse ato não configura uma espécie de "consentimento tácito", vez que não é abarcado pela lei. Da mesma sorte que uma plataforma que colocasse o aceite prévio do usuário (configurando opção *opt-out*) em seus termos de uso estaria em desacordo com a previsão legal.

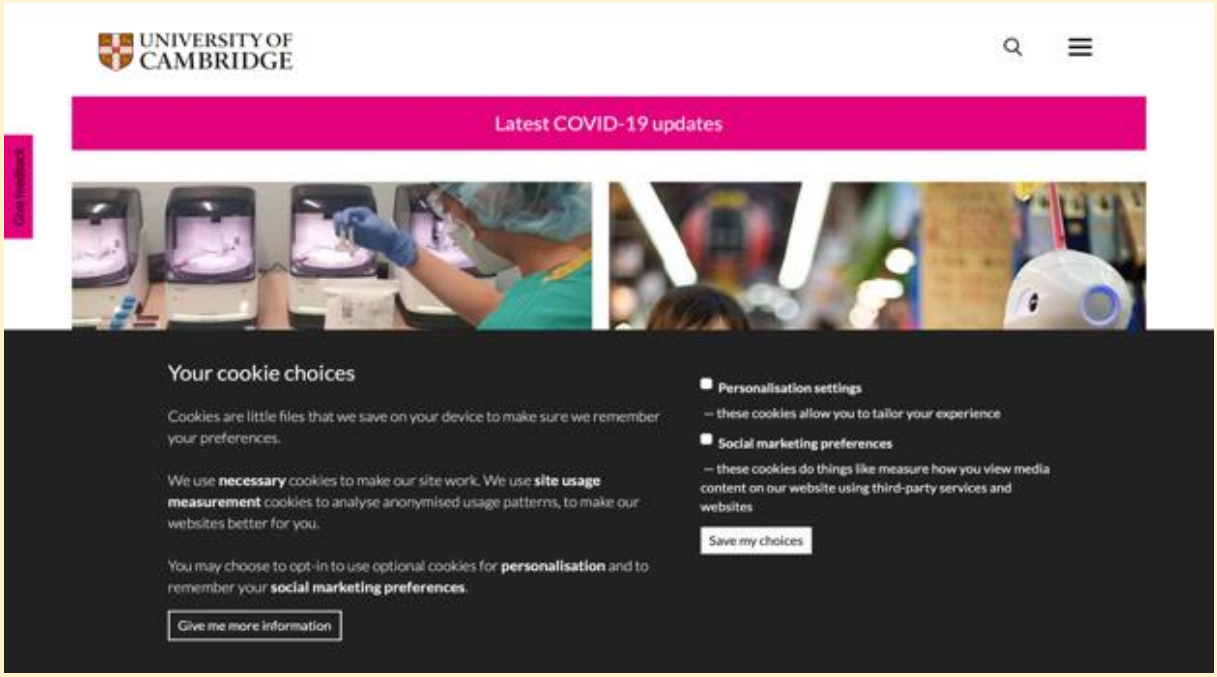
No mais, concernente ao adjetivo livre (art. 5º, XII, LGPD), é mister promover a fragmentação das opções de coleta de dados pessoais, de modo a tornar o consentimento granular. Isso poderia ser alcançado disponibilizando ferramentas de personalização.

Além disso, como visto em tópico anterior, o art. 5º, XII, da LGPD prevê que o consentimento também deve ser informado. Desta feita, incumbe à empresa apresentar suas

[21] Valendo ressaltar o art. 8º, § 2º, da LGPD: "cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei", bem como o § 3º do mesmo artigo, que veda o tratamento de dados pessoais realizado com vício de consentimento.

políticas de privacidade e tratamento de dados pessoais, junto ao termo de aceite, de forma clara e acessível.

Considerando o exposto, destacam-se aqui os esforços realizados pela *Cambridge University* (Universidade de Cambridge) em sua plataforma digital[22]:



Na imagem, observa-se que está definido de forma simples e didática o conceito de *cookies*[23], bem como o motivo do *site* utilizá-los (assim definindo a finalidade do tratamento de dados pessoais)[24]. Ademais, é dada a opção (*opt-in*) ao usuário de escolher as formas que poderão ser utilizadas para o tratamento de seus dados[25], respeitando o direito ao consentimento inequívoco.

Os termos de uso e as informações técnicas continuam ao alcance do titular dos dados (em *give me more information*), como devem estar, mas o resumo simplificado e as caixas destacadas de *opt-in* favorecem uma abordagem mais clara e preocupada com a privacidade do consumidor.

---

[22] Disponível em: <https://www.cam.ac.uk>. Acesso em: 28 dez. 2020.

[23] "*Cookies* são pequenos arquivos que salvamos no seu aparelho para lembrarmos de suas preferências". Tradução livre.

[24] "Nós usamos *cookies* necessários para fazer o nosso site funcionar. Nós usamos *cookies* de medição de uso no *site* para analisar padrões de uso anonimizados, para deixar nossos *websites* melhores para você". Tradução livre.

[25] "Você pode escolher (opção *opt-in*) usar *cookies* opcionais para personalização e para lembrar suas preferências de *social marketing*. As configurações de personalização são *cookies* que permitem que você customize sua experiência. As preferências de *social marketing* são *cookies* que fazem coisas como medir como você conteúdos midiáticos no nosso *website*, usando serviços e *websites* de terceiros". Tradução livre.

Na oportunidade, vale mencionar o *site globo.com*, que não oferece ao usuário a possibilidade de personalizar a concessão do uso de seus dados pessoais, como no exemplo acima, dificultando a autodeterminação informativa do consumidor.

Já a plataforma digital do jornal *The Guardian*[26] segue o exemplo da *Cambridge University*, porquanto oferece uma explicação acessível a respeito do conceito de cookies[27] e como eles serão utilizados no site.[28] Além de possibilitar ao usuário o gerenciamento dos seus dados pessoais[29], fortalecendo a posição do consumidor nesta relação. Na imagem abaixo, nota-se de pronto a intenção valorável da empresa com a escolha do título "A Escolha É Sua" (*It's Your Choice*):

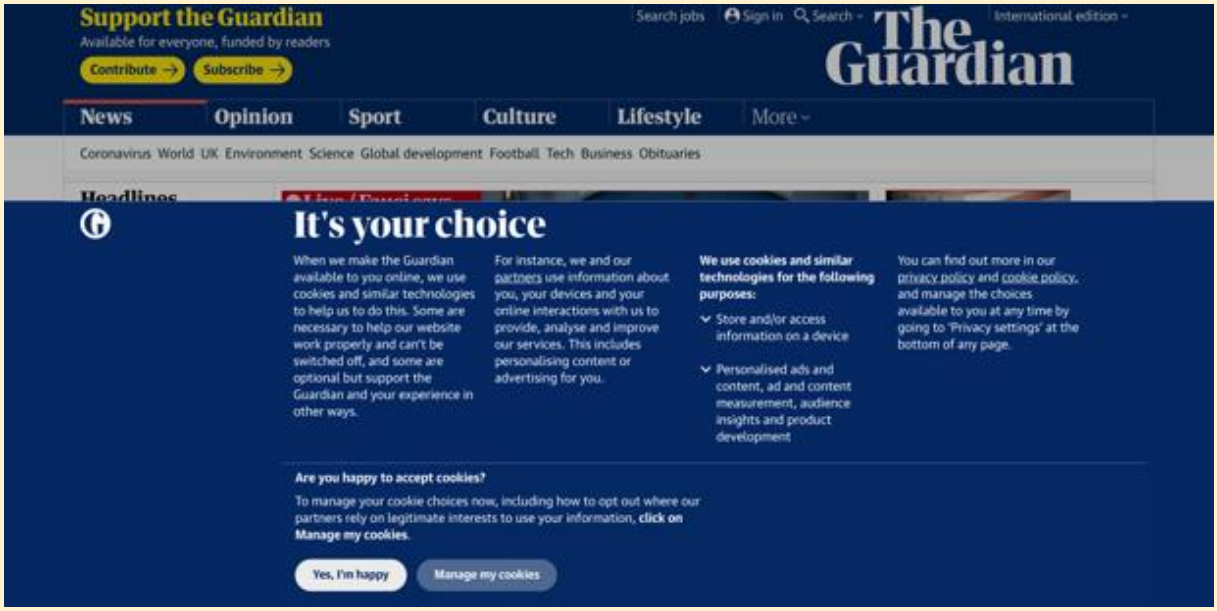
---

[26] Disponível em: <https://www.theguardian.com/international>. Acesso em: 29 jan. 2021.

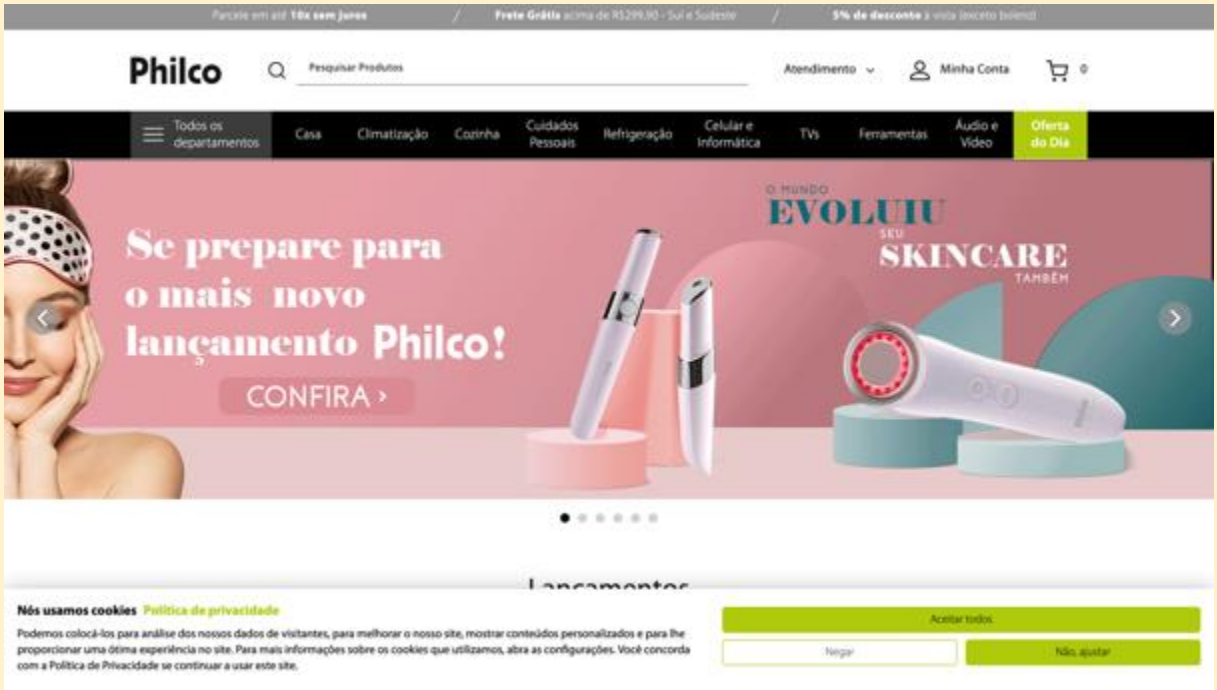
[27] "Quando tornamos o *The Guardian* disponível para você *online*, nós usamos *cookies* e tecnologias similares para nos ajudar. Alguns são necessários para ajudar o nosso site a funcionar propriamente e não podem ser desligadas, e algumas são opcionais, mas apoiam o *The Guardian* e a sua experiência de outras formas. Por exemplo, nós e nossos parceiros usamos informações sobre você, seus aparelhos e suas interações *online* conosco para providenciar, analisar e melhorar nossos serviços. Isso inclui conteúdo personalizado ou anúncios direcionados a você."

[28] "Nós usamos cookies e tecnologias similares com os seguintes objetivos: (i) armazenar e/ou acessar informação em um aparelho; (ii) criar anúncios e conteúdo personalizados, medir engajamento em anúncios e conteúdo, analisar o insight da audiência e desenvolver melhores produtos. Você pode descobrir mais na nossa Política de Privacidade e Política de Cookie e gerenciar as escolhas disponíveis para você a qualquer tempo clicando em 'Ajustes de Privacidade' no final da página".

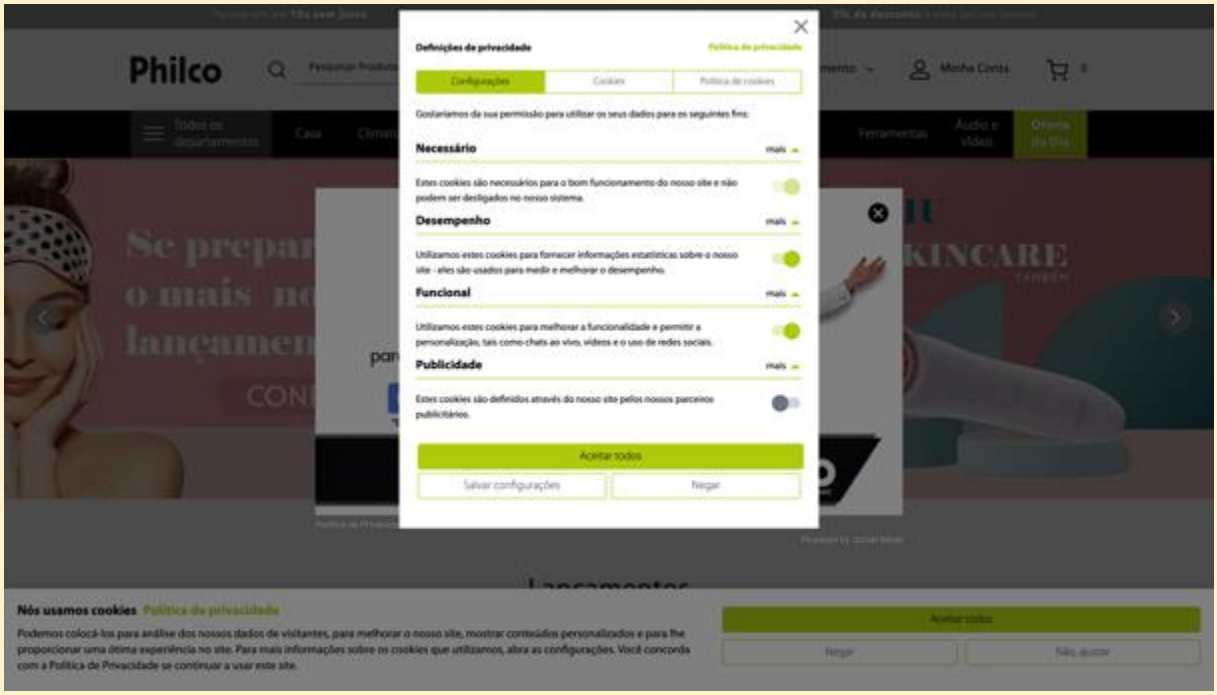
[29] "Você está feliz de aceitar cookies? Para gerenciar suas escolhas de cookie agora, incluindo como escolher sair dos ajustes que permitem que nossos parceiros utilizem suas informações com interesse legítimo, clique em 'Gerenciar meus cookies'".



Na mesma linha, destaca-se a plataforma digital da empresa *Philco*[30], que também fornece ao titular de dados um quadro de resumo sobre as definições de privacidade, bem como garante ao usuário que este faça a configuração destas definições com base nos dados que este entenda por querer compartilhar. Observe-se:



[30] Disponível em: https://philco.com.br>. Acesso em 17 fev. 2021.



De sorte que estes modelos focados no empoderamento do usuário, com *layout* que favorece a compreensão, também poderiam ser adequados aos consumidores hipervulneráveis, desde que a empresa ou instituição tomasse algumas medidas para se adequar a esta realidade. Por exemplo, vale promover a compatibilização da plataforma digital com aplicativos utilizados por pessoas com deficiência, como o *EyeFy*, que converte os textos em sons para deficientes visuais. Outrossim, que se adaptasse todas as informações (incluindo as técnicas, presentes nos Termos de Uso e na Política de Privacidade completa) de maneira apropriada a idosos, em fontes maiores, *e.g.*, à luz do disposto no art. 55-J, XIX, LGPD: "compete à ANPD garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento".

A ideia como um todo parte do conceito de *Privacy by Design*, no que se entende que "a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais" (BIONI, 2021, p. 263).

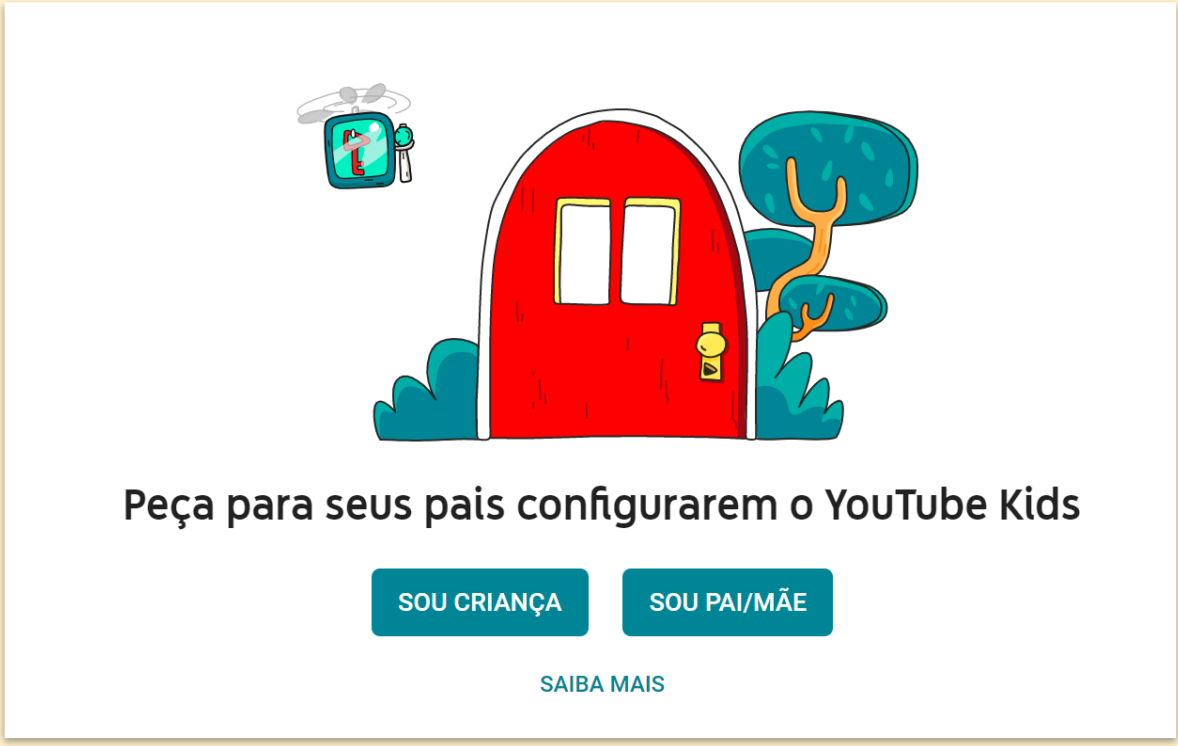
Nessa tônica, considerando a hipervulnerabilidade dos idosos, sugerimos a adoção de ferramentas como a *Platform for Privacy Preferences* (P3P), enquanto possibilitaria a pré-configuração de preferências de privacidade mais protetivas em dispositivos móveis, como a opção *standard* pelo modo de busca privado (que não permite a coleta de dados pessoais). Essa medida promoveria a anonimização *by default* do idoso nas plataformas de busca, reduzindo a

sua vulnerabilidade, pelo menos no que tange aos dados em que o consentimento é requisito necessário para coleta e tratamento.

No que concerne à proteção dos dados pessoais de crianças e adolescentes, havendo a necessidade, devem ser tomadas medidas para se certificar de que os dados coletados contariam com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, realizando todos os esforços razoáveis para essa verificação (v. art. 14, § 1º e § 5º, da LGPD).

Neste sentido, uma boa alternativa para garantir que a especificidade fosse respeitada seria a proposta por Bruno Bioni, quando dispõe que poderia haver uma "(...) dupla verificação do consentimento, como seria o caso em que o titular dos dados dá o 'concordo' em um *website* e, posteriormente, o confirma por *e-mail*." (2021, p. 281). Tal hipótese poderia ser aplicada de uma maneira em que, no momento em que a criança efetuasse o aceite, o *website* disparasse um e-mail ao endereço eletrônico dos pais, de forma que a plataforma só fosse habilitada no momento em que os responsáveis ratificassem a concordância dos menores.

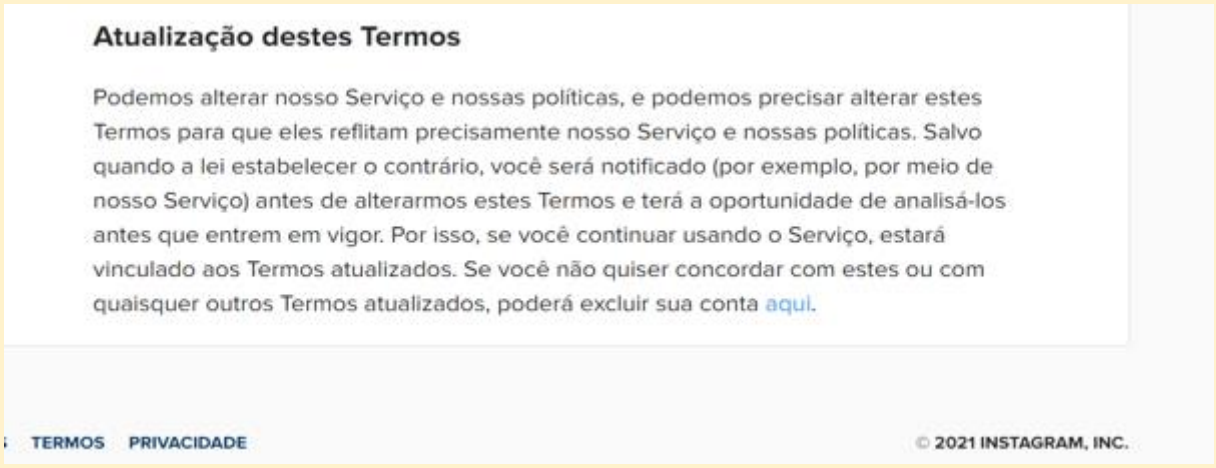
Como exemplo de plataforma que está tentando se adequar a esta realidade, podemos destacar o *Youtube Kids*. Mire-se:



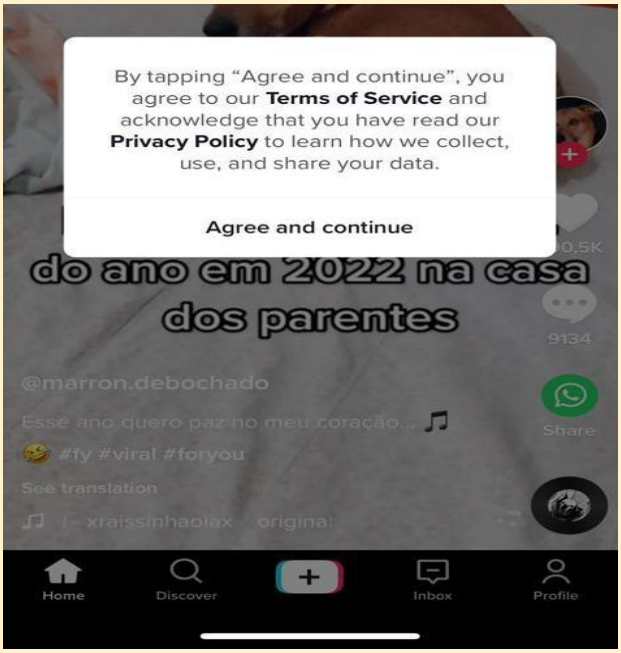
Outra alternativa, similar à sugerida para os idosos para validação deste consentimento, seria que os dispositivos móveis fornecidos a crianças viessem equipados também com sistema P3P. Desta forma, como Bruno Bioni afirma "(...) o próprio *browser* procederia a uma análise automatizada das políticas de privacidade das aplicações acessadas, verificando-se a sua (in)compatibilidade com as preferências de privacidade pré-configuradas" (2021, p. 268).

No mais, destaque-se outra peculiaridade do consentimento relacionado a crianças e adolescentes, no que toca ao adjetivo livre: os controladores não deverão condicionar a participação desses titulares em jogos, aplicativos ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade (v. art. 14, § 4º, LGPD).

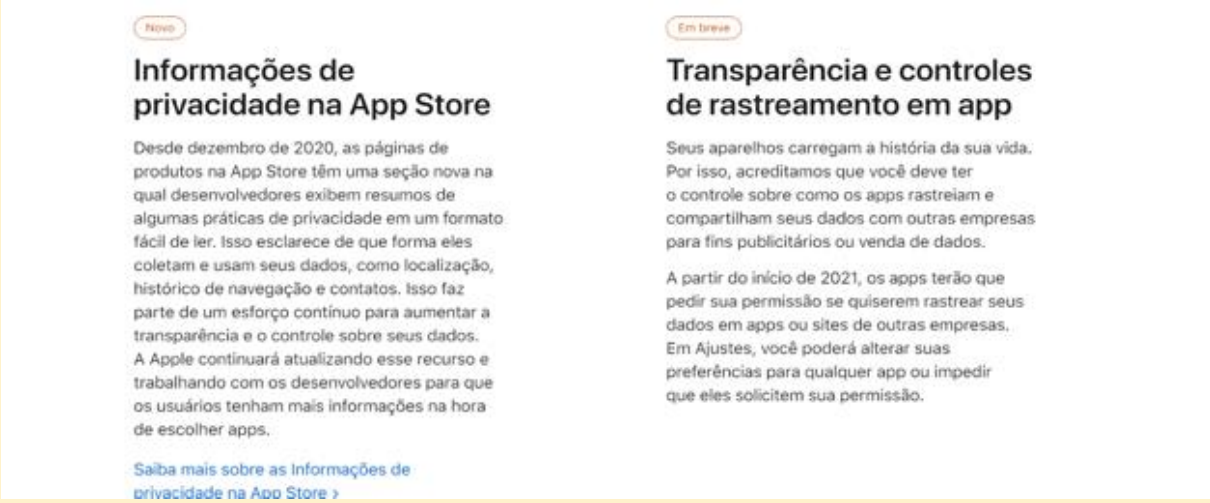
Em sentido contrário, analisando os Termos de Uso do aplicativo Instagram, verificamos que a plataforma condiciona o seu acesso ao aceite total das diretrizes impostas, prejudicando o requisito do consentimento livre deste usuário (v. art. 5º, XII, da LGPD). Não obstante, ao aplicativo exibir toda a sua política de privacidade (um total de 13 páginas) buscando a concordância do indivíduo para ingresso na rede social, certo que o consumidor não se verá propenso a examinar todo o teor do documento.



Outro aplicativo que segue com a mesma desídia em relação a coleta de dados é o da rede do *TikTok*. Vejamos:



No entanto, embora a privacidade ainda seja muitas vezes mitigada nos meios digitais, vale mencionar o empenho da empresa *Apple* no ano de 2020, porquanto ofereceu aos seus usuários novas ferramentas para restringir a coleta de dados pessoais realizada por plataformas de buscas e aplicativos utilizados em dispositivos *IOS*. Nessa linha, a nova seção de Informação e Privacidade da *Apple* trouxe, dentre outras funções, (i) a limitação do acesso a fotos armazenadas no dispositivo, à medida que se torna escolha do usuário os arquivos que poderão ser compartilhados com os aplicativos; (ii) a possibilidade de exclusão do *ID Apple* e das informações relacionadas a ele de maneira definitiva dos bancos de dados dos aplicativos; (iii) e a restrição ao rastreamento do histórico de pesquisa do usuário por anunciantes.



CONCLUSÃO

O trabalho explicou a importância e o cabimento da LGPD, assim como os contornos do direito ao consentimento livre, expresso e informado. Em seguida, fez um aprofundamento sobre a vulnerabilidade e hipervulnerabilidade nas relações consumeristas.

Por fim, desbravou os desafios envolvendo a efetividade do consentimento no campo da hipervulnerabilidade, apresentando exemplos de empresas que já adaptaram suas plataformas eletrônicas à LGPD, com vistas a responder a problemática principal da presente pesquisa: como efetivar o consentimento diante da hipervulnerabilidade do consumidor, considerando as facilidades do mercado que estará abrindo mão.

Vive-se um novo tempo no trato dos dados pessoais, não sendo mais um campo sem lei e regras. Devendo os agentes que tratam e armazenam os dados pessoais entenderem que não é mais suficiente formulários-padrão com textos inacessíveis e de difícil compreensão,

considerando que o Brasil é um país emergente com grande parte de sua população sem conhecimentos mínimos de tecnologia.

Para além das tradicionais relações jurídicas entre fornecedor e consumidor, este agora mais fragilizado pelos costumes do mercado digital, cabe às empresas desenvolverem novas ferramentas, e, assim, alcançar melhores resultados na efetivação do consentimento do consumidor hipervulnerável. Nesse contexto, o presente artigo destacou importantes esforços de empresas em suas plataformas digitais, que explicaram de forma mais fácil e acessível o tratamento de dados pessoais realizado, bem como oportunizaram possibilidades de escolha por parte do consumidor em relação à coleta dos seus dados. Consideramos estes exemplos como possíveis modelos a serem aplicados para uma fiel adequação à LGPD, garantindo melhores condições aos consumidores hipervulneráveis no cenário informacional.

REFERÊNCIAS

BIONI, Bruno. **Proteção de Dados Pessoais**: A Função e os Limites do Consentimento. 3ª ed. São Paulo: Forense, 2021.

BOLZAN, Fabrício. **Direito do Consumidor Esquematizado**. 2ª ed. São Paulo: Saraiva, 2014.

BRASIL. **Lei 13709, de 14 de agosto de 2018**. Institui a Lei Geral de Proteção de Dados no Brasil. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >. Acesso em: 30 maio 2020.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. 1ª ed. Brasília: Saraiva, 2014.

MORAES, Paulo Valério Dal Pai. **Código de Defesa do Consumidor**: o princípio da vulnerabilidade no contrato, na publicidade, nas demais práticas comerciais. 3ª ed. Porto Alegre: Livraria do Advogado, 2009.

SCHMITT, Cristiano Heineck. **Consumidores Hipervulneráveis**: a proteção do idoso no mercado de consumo. São Paulo: Atlas, 2014

SCHWARTZ, Fábio. **A Defensoria Pública e a proteção dos (hiper)vulneráveis no mercado de consumo**. Conjur, 2016. Disponível em: < https://www.conjur.com.br/2016-jul-19/protecao-hipervulneraveis-mercado-consumo>. Acesso em: 27 dez. 2020.

TARTUCE, Flávio; AMORIM, Daniel Assumpção Neves. **Manual de Direito do Consumidor**: direito material e processual. 5ª ed. São Paulo: Método, 2016.

TEPEDINO, Gustavo; FRAZÃO, Ana; DONATO, Milena Oliva. **Lei Geral de Proteção de Dados Pessoais e Suas Repercussões no Direito Brasileiro**. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020.