ARTIGO
Doi: 10.4025/rimar.v13i1.66251
Recebido: 11/12/2022
Aprovado: 21/12/2022
Double blind review, SEER/OJS
Editor: Francisco Vieira

PRODUZINDO A VULNERABILIDADE DO CONSUMIDOR: TECNOLOGIAS BIOMÉTRICAS, MARKETING E BIOPOLÍTICA

Producing consumer vulnerability: biometric technologies, marketing, and biopolitics

Renata Couto de Azevedo de Oliveira[1]
0000-0001-5839-8814
✉ renatacouto@yahoo.com

[1] *Programa de Pós-Graduação, Unigranrio*

RESUMO

Este ensaio discute o caso Raia-Drogasil à luz da vulnerabilidade do consumidor e do marketing na era digital, dado o avanço das tecnologias biométricas que podem ser encaradas como um mecanismo de governança dos consumidores. Partimos da definição de vulnerabilidade do consumidor como um estado de fragilidade de indivíduos frente as práticas de mercado que pode se manifestar da produção ao pós-consumo. Argumentamos que todos estamos sujeitos à vulnerabilidade em um mercado no qual o marketing usa a biometria como uma forma de biopoder para fazer predições e, assim, exercer controle. Concluímos que em estratégias de marketing envolvendo dados pessoais sensíveis é mandatório que sejam observadas as obrigações previstas pela LGPD, pois tais estratégias podem acarretar a produção de vulnerabilidade direta e indiretamente para consumidores e para sociedade. Sugerimos que as tecnologias biométricas expandem situações de vulnerabilidade antes reservadas a determinados grupos, universalizando-as. Questionamos a necessidade de dados biométricos para a eficácia das estratégias de marketing.

PALAVRAS-CHAVE: Vulnerabilidade do consumidor, tecnologias biométricas, marketing, biopolítica.

ABSTRACT

This essay discusses the Raia-Drogasil case under the light of consumer vulnerability and marketing in the digital age, given the advancement of biometric technologies that can be seen as a consumer governance mechanism. We start from the definition of consumer vulnerability as a state of fragility of individuals facing market practices that can manifest itself from production to post-consumption. We argue that we are all subject to vulnerability in a market where marketing uses biometrics as a form of biopower to make predictions and thus exercise control. We conclude that in marketing strategies involving sensitive personal data, it is mandatory that the obligations provided for by the LGPD are observed, as such strategies can lead to the production of vulnerability directly and indirectly to consumers and society at large. We suggest that biometric technologies expand vulnerability situations previously reserved for certain groups, universalizing them. We question the need for biometric data for the effectiveness of marketing strategies.

KEYWORDS: Consumer vulnerability, biometric technologies, marketing, biopolitics.

1. Contextualização

No mês de julho de 2021 o Grupo Raia-Drogasil (Grupo RD) figurou em diversos veículos midiáticos graças à nova política de extração de dados dos seus consumidores através de ferramentas de coleta biométrica. O programa de relacionamento que oferece descontos aos consumidores nas farmácias do grupo exigia o cadastro do CPF e se apropriava do histórico de compras daqueles. A esses dados seriam adicionados os biométricos (no caso, a digital dos consumidores), coletados nos pontos de venda. O argumento reproduzido pelos vendedores era de que a coleta da biometria era necessária à adequação aos requisitos da Lei Geral de Proteção de Dados (LGPD, Lei 13. 709/2018, em vigor desde agosto de 2020). Questionado pelo IDEC (Instituto Brasileiro de Defesa do Consumidor) e pelo PROCON-SP, o grupo Raia-Drogasil desistiu do cadastro biométrico dos consumidores.

O escopo da LGPD é minimizar a coleta de dados pessoais, estabelecendo que tanto a coleta, quanto o tratamento deles sigam exclusivamente a finalidade pré-estabelecida na Política de Privacidade e Termos de Uso que devem ser informadas ao consumidor. Por seu turno o consumidor deve dar seu consentimento de forma específica e destacada sobre todos os usos das suas informações pessoais disponibilizadas (LGPD, art. 11, I). No caso Raio-Drogasil essa exigência não foi observada. De acordo com matéria do The Intercept (2021) a Raia é a maior rede de farmácias do Brasil, com faturamento bruto de R$ 20 bilhões em 2020. São parte do grupo as marcas Raia, Drogasil e Onofre, mas os negócios englobam também a Univers, que administra os programas de benefícios em medicamentos nas lojas da rede, e a Stix, uma plataforma de recompensas (troca de pontos por produtos e descontos em lojas parceiras) de grandes marcas, como Pão de Açúcar, Extra e Itaú. Além disso, a Raia tem um grupo de investimento, o RD Ventures, que em 2020 adquiriu a HealthBit, empresa de *big data* cujo objetivo é usar inteligência artificial para aprimorar o uso dos planos de saúde e prevenção de casos graves em grandes empresas (Saúde Business, 2019).

A política de privacidade da Droga Raia prevê que as informações de seus consumidores podem ser compartilhadas com parceiros do mesmo grupo econômico, parceiros da indústria farmacêutica e consultorias e empresas de tecnologia parceiras sem especificar para o consumidor quais serão as informações compartilhadas e quais são os parceiros do mesmo grupo econômico, além das empresas de tecnologia parceiras. Ao cadastrar sua digital, o consumidor autoriza o compartilhamento das informações de maneira irrestrita entre todas as empresas do grupo Raia-Drogasil (The Intercept, 2021). O Instituto Brasileiro de Defesa do Consumidor (IDEC) levanta algumas hipóteses sobre a exigência da coleta de biometria nas farmácias do grupo Raia-Drogasil (IDEC, 2021). A primeira seria a de prática de seleção adversa, ou seja, na realização da troca econômica, a farmácia teria mais informações do que o consumidor, e essa assimetria levaria a uma tomada de decisão de forma incorreta e desfavorável por aquele. Outra hipótese seria a de que a rede de farmácias estivesse usando a biometria como um segundo mecanismo de identificação dos consumidores para além das receitas, que são retidas em caso de medicamentos de uso controlado. Dessa maneira, a biometria autorizaria a farmácia a manter a identificação dos clientes.

Através da estratégia de marketing da Droga Raia as empresas do grupo coletaram e trataram dados pessoais sensíveis de um número não estimável de consumidores (The Intercept, 2021). Isso representa um risco para os consumidores do grupo de farmácias e para a sociedade em geral, uma vez que todos nós, em dado momento e em determinadas circunstâncias, podemos ser considerados consumidores vulneráveis (Silva, Barros, Gouveia & Merabet, 2021). Estudos recentes em marketing (eg Moutinho, 2021; Du, Netzer,

Schweidel & Mitra, 2020) sinalizam a necessidade de alinhamento dos profissionais da área com as novas tecnologias, principalmente as biométricas, e destacam as oportunidades para o crescimento dos negócios através do uso dos dados coletados na aquisição, desenvolvimento e retenção do consumidor. As preocupações ainda se restringem majoritariamente à privacidade do consumidor, tema que já foi considerado antes pelos praticantes de marketing (eg Patterson, O'Malley, & Evans 2010).

O objetivo desse ensaio é discutir o caso Raia-Drogasil à luz da vulnerabilidade do consumidor e do marketing na era digital, dado o avanço das tecnologias biométricas que se podem ser encaradas como um mecanismo de governança dos consumidores (Ajana, 2010, 2013). Partimos da definição de vulnerabilidade do consumidor como "um estado de fragilidade de indivíduos frente as práticas de mercado que pode manifestar-se em diferentes etapas no processo de produção, comercialização e consumo" (Silva et al., 2021, p.91) e argumentamos que todos estamos sujeitos à vulnerabilidade em um mercado no qual o marketing usa a biometria "como forma de biopoder pelo qual o corpo e o ser vivo são objetos de controle e gestão" (Beer, 2014, p.332). Salientamos que as tecnologias biométricas expandem situações de vulnerabilidade antes reservadas a determinados grupos, universalizando-as. Para tanto contamos com o aporte teórico de Ajana (2013) e Mbembe (2018). Questionamos por fim a necessidade de dados biométricos para a eficácia das estratégias de marketing.

2. Marketing Ontem e Hoje

Coletar dados sempre foi uma atividade essencial ao marketing, mas a coleta e análise desses dados em um mercado hiper digital se tornou ainda mais lucrativa e necessária à sobrevivência das organizações. Atualmente, quando o assunto é coletar e tratar dados dos consumidores, quanto mais dados, melhor, pois as corporações extraem deles valor através de análises complexas, rigorosas e complementares (Kanashiro, Bruno, Evangelista & Firmino, 2013). Essas mesmas corporações oferecem aos consumidores a participação em programas de benefícios (eg descontos) e a participação em plataformas de recompensas, que permite aos consumidores acumularem pontos para compras e trocas em lojas parceiras, além da promessa de comunicação que seja relevante para o consumidor (por exemplo, uma mulher que compra um teste de gravidez provavelmente receberá promoções de fraldas em alguns meses) (The Intercept, 2021).

No passado as prioridades do capitalismo nascente (como o escoamento da produção em massa) fomentaram o desenvolvimento do marketing e de suas ferramentas visando conhecer mercados e consumidores e fazer com que algumas empresas vencessem a corrida pelos escassos recursos dos consumidores (Pridmore & Zwick, 2011). A crença que orientava o marketing era a de identificar as necessidades sempre mutantes dos clientes visando satisfazê-los e a de subordinar a eficiência da produção às descobertas sobre o que os aqueles queriam (Kotler, 1972). Isso significa dizer que ao invés de fazer com que os clientes queiram o que é produzido por determinada empresa, o marketing possibilitava que essa empresa produzisse o que o cliente queria (Pridmore & Zwick, 2011, p.269). A era pré-digital do marketing foi marcada por uma lógica corporativa voltada para as massas na qual os profissionais de marketing acreditavam que deveriam entender as motivações, os hábitos e desejos dos consumidores para então segmentá-los em estratos mais ou menos estáveis e realizar as operações necessárias visando alcançá-los e satisfazê-los (Darmody & Zwick, 2020, p.4).

Essa crença ainda serve de base ao discurso do marketing ancorado na vigilância dos consumidores, uma vez que o esforço de marketing para conhecer melhor os anseios dos consumidores e atendê-los é considerado legítimo, quase como um serviço público ou uma política social relevante (Pridmore & Zwick, 2011, p.270). Contudo, existe uma contradição sobre a qual se sustenta o discurso do marketing atualmente: por um lado,

capacitação e autonomia dos consumidores, enquanto, por outro, há total controle e manipulação de suas decisões, estendendo-se pela totalidade de suas vidas (Darmondy & Zwick, 2020, p.1). A abundância de dados e poderosas ferramentas e habilidades analíticas impulsionaram a reorganização do marketing e ao contrário do defendido por Kotler, a produção não se subordinou aos sempre mutáveis padrões de consumo. Ao contrário, os profissionais de marketing superaram a dicotomia produção-consumo e se concentram em fabricar consumidores como mercadorias (Zwick & Denegri-Knott, 2009). Isso significa que a economia pós-fordista se pauta na disciplina do consumo combinada com tecnologias de vigilância que configuram os mercados temporal e espacialmente, oferecem diversas formas de conhecimento e flexibilizam a conexão produção-consumo (Pridmore & Zwick, 2011, p.272).

Não há mais como elaborar experiências relevantes para os consumidores em tempos de marketing digital com base em dados produzidos tradicionalmente. Justifica-se dessa maneira a vigilância e, com ela, a datificação da vida humana (sua quantificação e tradução em dados) (Lupton, 2016). Um exemplo de dados que são úteis nesse processo são os de saúde, produzidos em tempo real e transmitidos por meio de tecnologias biométricas vestíveis (Oliveira, 2021). No contexto do capitalismo de vigilância (Zuboff, 2015) e comunicativo (Dean, 2008), no qual trocas comunicativas são consideradas elementos básicos da produção capitalista e as interações contínuas através das TIC produzem quantidades obscenas de dados, os consumidores talvez não estejam cientes da quantidade de informações coletadas pelas empresas e o que é feito com elas (Tadajewski, Denegri-Knott & Varman, 2018, p.30).

A coleta desses dados está na mira dos profissionais de marketing (ou *market seekers*, eg gerentes de produto e branding, designers de experiência de consumo), sempre em busca de oportunidades dentro do mercado altamente competitivo e visando conhecer e interagir com os consumidores intimamente, além de controlar os ambientes de comunicação e consumo (Darmody & Zwick, 2020, p.2-5). Por não serem capazes de processar e extrair valor da vasta quantidade de dados coletada, outros atores entram em cena: os *market finders* (Darmody & Zwick, 2020), que atuam subsidiariamente executando tarefas tecno-analíticas como, por exemplo, mineração de dados, corretagem de informações, inteligência de mercado e *consumer insights*, empregando monitoramento automático, detecção e produção de perfis com o objetivo de gerar *data doubles* (duplicata digital de cada consumidor capturada em dados e espalhada por conjuntos de sistema de informações, de acordo com Haggerty & Ericson, 2000). Esse é o cenário mais amplo no qual o marketing se localiza atualmente.

3. Tecnologias Biométricas

Biometria é a "identificação ou verificação automatizada de uma pessoa feita por comparações de características físicas, fisiológicas ou comportamentais com um modelo digital armazenado" (Shugan, 2004, p.472-473). Trata-se na verdade tanto de uma ciência, quanto de um conjunto de tecnologias focadas na medição de características humanas fisiológicas ou comportamentais, denominadas "traços biométricos" (Andronikou, Yannopoulos & Varvarigou 2008). Esses traços são características humanas variáveis interpessoalmente a ponto de distinguir as pessoas e invariáveis ao longo de um período (Jain et al, 2004). Dados biométricos podem incluir desde digitais, DNA, impressão palmar, íris, retina, atividade cerebral, odor corporal, até marcas, tatuagens, voz, assinatura, entre outros, incluindo gênero, etnia, idade, peso, esses últimos considerados *soft biometrics*, sem alta variabilidade interpessoal.

O Marketing Science Institute (MSI, 2020) lista como prioridade de pesquisa os estudos sobre dados biométricos e as questões éticas relacionadas como uma chave para o presente e para o futuro imediato, uma vez que ao longo dos últimos anos, cada vez mais

dados biométricos foram coletados e processados por produtos disponíveis no mercado, como *smartphones* que usam digitais e reconhecimento facial, assistentes pessoais que reconhecem padrões vocais e *smart watches* que processam batimentos cardíacos. A adoção de sistemas biométricos por diversas indústrias é ampla e estima-se um mercado global avaliado em US$ 35,5 bilhões (DeKeyser, Bart, Gu, Liu, Robinson & Kannan 2021).

Além das possibilidades de identificação, o uso comercial dessas tecnologias, combinadas com inteligência artificial, possibilitam que as organizações que as utilizam gerem perfis de identificação (quem é essa pessoa?), físico (que tipo de pessoa é essa?), emocional (o que essa pessoa está sentindo?), comportamental (o que essa pessoa está fazendo?) e cognitivo (o que essa pessoa está pensando?) (DeKeyser et al, 2021). Apesar dos perfis de identificação serem os mais comuns, tecnologias como *eye tracking* são usadas na formação de perfis cognitivos para o varejo, com o intuito de identificar atenção dos consumidores que entram em lojas de varejo (eg Wästlund, Otterbring, Gustafsson & Shams 2015). Emojis, emoticons stickers, gifs animados e os famosos ícones de reação do Facebook permitem o acesso cada vez maior de nossas emoções aos atores humanos e não humanos das corporações que operam as plataformas-laboratórios (Bruno, Bentes & Faltay, 2019).

Os mais entusiasmados com os dados biométricos alegam que as tradicionais fontes de produção de dados, como *surveys*, CRM e fluxo de cliques, podem sofrer com vieses de mediação (Verhulst et al., 2019), destacar processos conscientes e explícitos (Plassmann, Venkatraman, Huettel & Yoon, 2015) e fazer com que as organizações confiem excessivamente nos dados disponíveis, provocando o chamado efeito *streelight*, isto é, um tipo de viés observacional que ocorre quando as pessoas apenas procuram algo onde é mais fácil procurar (Du et al. 2021). Apesar das muitas oportunidades associadas ao uso das tecnologias biométricas, como, por exemplo, apoio à contratação, suporte e gerenciamento de funcionários, fortalecimento de segurança, personalização do *marketing mix* e melhorias do bem-estar e da saúde (DeKeyser et al, 2021), dois exemplos abaixo mostram seus potenciais problemas. É importante lembrar que a predição do comportamento humano é reflexo da crença da verdade objetiva contida na grande quantidade de dados (“dataísmo”, segundo van Dijck, 2014) produzida pelos consumidores e tratada através de algoritmos capazes de não apenas de predizer, como também de “modificar o comportamento humano como um meio [de] produzir receita e controle de mercado” (Zuboff, 2015, p.75).

Como grupo Raia-Drogasil é dono da HealthBit, cujo objetivo é colaborar com o departamento de Recursos Humanos das organizações na redução dos custos com planos de saúde através de análises realizadas com dados biométricos dos empregados das empresas, citamos como primeiro exemplo o estudo de Charitsis (2019), que se destaca ao examinar “a intersecção entre autovigilância, bem-estar corporativo e saúde, destacando as desigualdades socioeconômicas propagadas pela ideologia do dataísmo” (p.139). A parceria entre a plataforma FitBit Care e a Humana (planos de saúde) levou a primeira para dentro de várias organizações como solução de saúde e resultou em privilégios para os empregados capazes de se engajar em atividades que geram dados desejáveis. Podemos inferir que as análises da HealthBit pautadas em perfis biométricos emocionais e físicos fomentariam desigualdades na medida em que poderiam desencadear demissões baseadas nos altos custos dos planos de saúde desses funcionários e performances não alinhadas com as metas da empresa. Segundo Charitsis (2019, p.143), “no capitalismo, uma das maiores tragédias que os trabalhadores individuais podem vivenciar é a incapacidade de vender sua força de trabalho”.

O segundo exemplo é o relato de Sasha Costanza-Chock, professora do MIT, pesquisadora, designer e ativista da área de comunicação. Ela se declara “uma pessoa transgênero não-binária que se apresenta como mulher” (Costanza-Chock, 2018). Sua

experiência no aeroporto de Detroit com scanner de ondas milimétricas que faz a triagem de segurança revela como um sistema que trabalha com perfis biométricos físicos pode apresentar vieses. Após o passageiro ter seu corpo escaneado, o agente de segurança informa ao sistema se a pessoa é um homem ou uma mulher. No caso de Sasha, ainda que o agente opte por "mulher", o *scanner* destaca áreas que são estatisticamente diferentes da norma de um corpo considerado feminino. Em seguida, Sasha enfrenta o constrangimento de uma revista pessoal. A experiência da autora sinaliza que os dados, modelos e algoritmos utilizados na implementação do scanner são binários e heteronormativos, mas poderiam ser aprimorados através de iniciativas de *design justice* (Costanza-Chock, 2018).

Os casos acima confirmam a existência de vieses e a reprodução deles e apontam como tecnologias biométricas podem produzir desigualdade, exclusões e injustiças. Como a LGPD tem por finalidade a proteção dos direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural (art.1º, LGPD), o emprego das tecnologias biométricas no mercado brasileiro deve ser observado de perto. Fernando Capez, diretor executivo do Procon-SP, declarou que a exigência de coleta da identificação biométrica dos consumidores no caso Raia-Drogasil para a concessão de descontos contraria os princípios de tratamento de dados contidos no art. 6, I, II e III da LGPD, violando os critérios de necessidade, adequação e finalidade trazidos pela lei. Além disso, Capez lembra que o consentimento obtido dos consumidores no caso Raia-Drogasil não foi precedido de informações claras e inequívocas acerca da utilização dos dados biométricos (CONJUR, 2021b).

4. Proteção de Dados

Dados pessoais são informações relacionadas a pessoas naturais identificadas ou identificáveis (LGPD, art. 5º. I). Segundo o site CONJUR (2021a) é identificável a pessoa natural que possa ser identificada direta ou indiretamente, especificamente por apontamento a um identificador, que pode ser um nome, um número de identificação, dados de localização ou outros elementos específicos relacionados a essa pessoa. A LGPD traz um rol taxativo dos dados pessoais considerados sensíveis: dados 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* (grifo nosso), quando vinculado a uma pessoa natural (LGPD, art. 5º., II). As bases para o tratamento dos dados pessoais estão previstas também no artigo 7º da LGPD, enquanto no artigo 11 da mesma Lei encontram-se aquelas que autorizam o tratamento dos dados pessoais sensíveis.

Segundo Mendes (2016, p.7), "o direito básico do consumidor à proteção de dados pessoais envolve uma dupla dimensão: (i) a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e (ii) a atribuição ao consumidor da garantia de controlar o fluxo de seus dados na sociedade". O alcance dessa proteção é importante no caso Raia-Drogasil, uma vez que os consumidores desconhecem que o grupo engloba empresas de tecnologia como a HealthFit e o possível impacto de seus serviços. Apesar da associação "privacidade-segurança" ainda ser uma preocupação recorrente de boa parte das pessoas, inclusive acadêmicos e profissionais de marketing, a abordagem jurídica mais atual e que encontra suporte em algumas legislações de proteção de dados (inclusive na LGPD) é aquela que transfere o foco da privacidade e do segredo para os possíveis efeitos do processamento dos dados coletados e das informações geradas e seu consequente impacto para a autonomia humana (Zanatta, 2017). Estudiosos na área de Direito no Brasil (eg Bioni, 2019; Doneda, 2006) enfatizam que a proteção de dados pessoais deve se pautar pelo princípio da autodeterminação informacional, que consiste na "capacidade do cidadão de controlar suas informações, em um contexto de expansão das técnicas de uso de

informações pessoais, metadados, e fracasso dos modelos de *notice-and-consent*[i]" (Zanatta, 2017, p.178)

Obrigações antidiscriminatórias e informacionais precedem a LGPD, estando consolidadas no Brasil desde o Código de Defesa do Consumidor (CDC, Lei 8.078/1990) e da Lei do Cadastro Positivo (Lei 12.414/2011). Contudo, a LGPD traz uma dimensão complementar à informacional e à antidiscriminatória, qual seja, a dialógica, de caráter relacional e pedagógico, que funciona como uma obrigação de "explicar como um determinado processo técnico funciona" (Zanatta, 2019, p.4). Outro ponto importante da legislação é reconhecer que mesmo dados anonimizados podem ser considerados como pessoais se utilizados para a formação de perfis, com base no parágrafo 2º do art. 12 da LGPD (Zanatta, 2019, p.7). Isso aponta que o foco está não no dado em si, mas nas consequências do seu tratamento para o consumidor.

Uma das consequências que pode causar vulnerabilidade do consumidor é a perfilização, uma forma de tratamento automatizado que consiste "no uso de dados pessoais para avaliação de certos aspectos relacionados à pessoa natural, em particular a análise e predição de aspectos comportamentais" (eg performance no trabalho, preferências de consumo, situação econômica e de crédito, saúde etc.) (Zanatta, 2019, p.6). Bioni (2019, p.80) aponta que por vezes os processos automatizados usam perfis que não necessariamente identificam pessoas, mas grupos (*grouping*). Caso uma pessoa esteja catalogada em um grupo, decisões serão tomadas a seu respeito ainda que sem individualizá-la. É o que ocorre com a *differential privacy* da Apple[ii] e nos casos relatados por O'Neil (2016) sobre empresas de recrutamento de pessoas que usam bases de dados de agências de crédito, que modelam estatisticamente perfis com base em sistemas de pontuação de crédito e outras informações. Assim, dados biométricos podem ser tratados e incluídos na formação de perfis que serão usados em caráter antecipatório e decisório, produzindo uma iminência de insegurança, ansiedade, discriminação e desigualdades (em suma, um estado latente de vulnerabilidade) caso haja má-fé em sua coleta e posterior tratamento, como no caso Raia-Drogasil.

5. Vulnerabilidade do Consumidor e Biopolítica

Interações com o mercado são geralmente favoráveis aos envolvidos, sejam eles produtores, consumidores, trabalhadores e/ou sociedade como um todo. Contudo, existem aquelas que poderiam ser descritas como pertencentes ao *dark side of marketing,* ou seja, pertencentes à faceta desnecessária, indesejada, e muitas vezes ilegítima das trocas (Daunt & Geer, 2017), produzindo resultados negativos diretos e indiretos e de amplo alcance, para além da figura do consumidor (Silva et al., 2021). A ubiquidade das tecnologias biométricas evidenciou para alguns pesquisadores o conflito entre a excelência técnica dos desenvolvedores de software, por um lado, e a criação de experiências valiosas para o consumidor por parte dos profissionais de marketing, por outro lado (Puntoni, Reczek, Giesler & Botti, 2020). A abordagem nesses casos reconhece experiências entre consumidores e inteligência artificial (IA) com resultados problemáticos, incluindo casos de atribuição incorreta de identidade e categorizações que podem gerar limitações de escolha e liberdade para consumidores vulneráveis (ou, ainda, exacerbá-las) (Puntoni et al., 2020, p.138).

Ao contrário de boa parte dos trabalhos sobre vulnerabilidade que apostam em uma perspectiva neoliberal, focando na agência dos consumidores e explorando suas estratégias de enfrentamento (Dunnett, Hamilton & Piacentini, 2018, p.368), nossa abordagem é menos conciliatória. A literatura sobre vulnerabilidade do consumidor é bem estabelecida e a definição mais tradicional sobre o tema é a de Baker, Gentry e Rittenburg (2005), segundo a qual vulnerabilidade é

> "[...] um estado de impotência que surge de um desequilíbrio nas interações do mercado ou no consumo de mensagens e produtos de marketing. Ocorre quando o controle não está nas mãos de um indivíduo, criando uma dependência de fatores externos (por exemplo, profissionais de marketing) para criar justiça no mercado. A vulnerabilidade real surge da interação de estados individuais, características individuais e condições externas dentro de um contexto em que os objetivos de consumo podem ser prejudicados e a experiência afeta as percepções pessoais e sociais de si mesmo" (Baker, Gentry & Rittenburg, 2005, p. 134).

Elegemos a definição de vulnerabilidade de Silva e autores (2021, p.91) que a descrevem como "um estado de fragilidade de indivíduos frente às práticas do mercado, que pode se manifestar em diferentes etapas no processo de produção, comercialização e consumo". No trabalho dos autores é mapeado o corpo teórico sobre vulnerabilidade do consumidor nos últimos 25 anos. As contribuições sobre o tema são divididas em três grandes áreas: (i) estudos que focam nas condições que levam à vulnerabilidade (eg Baker et al, 2005; Baker & Mason, 2012), (ii) estudos que focam nas questões éticas (eg Smith & Cooper-Martin, 1997; Jones & Middleton, 2007) e por fim, (iii) aqueles que encaram a vulnerabilidade como resultado dos sistemas de marketing (eg Nason, 1989; Schultz II & Holbrook, 2009). O caso Raia-Drogasil estaria situado na interseção dessas áreas, caso elas estivessem organizadas como um diagrama de Venn, uma vez que envolve questões prévias dos consumidores (por exemplo, necessidade de desconto, falta de informação sobre proteção de dados) que aumentam a ocorrência de vulnerabilidade, assim como questões éticas e potenciais resultados negativos direitos e indiretos sobre os consumidores e sociedade em geral decorrentes do sistema de marketing.

Nosso argumento principal é que as tecnologias biométricas podem produzir resultados negativos para os consumidores envolvidos no caso RD e para a sociedade em geral, uma vez que são instrumentos de exercício de biopoder. A apreensão mais ampla de biometria como mediação da vida e sua relação com conceitos como identidade e biopolítica (eg Ajana, 2013; Beer, 2014) ganha contornos que parecem ser ignorados pela maioria das pesquisas de marketing e pelos profissionais focados em proporcionar experiências de consumo notáveis. Ajana (2013) defende em seu trabalho que o corpo assume papel central nas sociedades datificadas que buscam controlar e gerenciar identidade, deslocamento, cidadania e acesso. As tecnologias biométricas autorizam que sejam feitas suposições sobre as pessoas e isso permite que suas identidades sejam objeto de governança (Beer, 2014). Quando o marketing opta por usar estratégias que se baseiam em dados biométricos ou perfis criados a partir deles, suas ações carregam a marca de governamentalidade e da biopolítica, tornando-se assim biopolítico. Zwick e Bradshaw (2018) entendem marketing biopolítico como "um modo de governar os consumidores que visa encontrar (ou criar ativamente) oportunidades para a participação do consumidor (por exemplo, no processo de inovação de novos produtos e comunicação da marca) com o objetivo de criar valor para a empresa" (Zwick & Bradshaw, 2018, p.430, nossa tradução).

O conceito de biopolítica é central nos trabalhos de Ajana (2013) e Zwick e Bradshaw (2018). Esse conceito está relacionado à gestão da vida, englobando nossos corpos, capacidades intelectuais e sociais, e os qualificando em termos de capacidades produtivas. Em entrevista para Beer (2014), Ajana defende que essa gestão da vida ocorre através de diversos meios e técnicas, entre os quais a biometria. Chamamos atenção para a possibilidade dessa gestão, que inicialmente é relacionada aos grupos considerados mais vulneráveis, abranger a sociedade como um todo. Nesse sentido, nos inspiramos também em Mbembe (2018) e seu "devir negro". Em seu livro, o autor comenta a fusão entre o capitalismo e o animismo, que transforma seres humanos em coisas animadas, dados numéricos e códigos. E segue afirmando que

> "[pela] primeira vez na história humana, o substantivo negro deixa de remeter unicamente à condição atribuída aos povos de origem africana durante a época do primeiro capitalismo. [...] Essa nova condição fungível e solúvel, à sua institucionalização enquanto padrão de vida e à sua generalização pelo mundo inteiro, chamamos o *devir negro do mundo*" (Mbembe, 2018, p.16, itálico no original)

Mbembe considera que o negro e a raça não são elementos fixos, mas de sentido existencial, referente a uma série de experiências dilacerantes para pessoas apanhadas nas redes de dominação, "inventado para significar exclusão, embrutecimento e degradação, ou seja, limite sempre conjurado e abominado" (Mbembe, 2018, p.17). Dessa maneira seria possível que a condição subalterna reservada aos negros fosse extrapolada a outros, como imigrantes e desempregados, graças à reinvenção de discriminações, hierarquias e assimetrias (Pelbart, 2018). Somando-se ao devir negro do mundo, Ajana (2013, 2010) e seu trabalho sobre identidade e biometria investiga o uso cada vez mais comum dessa tecnologia em um mundo móvel globalizado visando "proteger e gerenciar a singularidade da identidade, a fim de combater o roubo e fraude de identidade, crime e terrorismo, trabalho e emprego ilegais e para governar com eficiência vários domínios e serviços, incluindo asilo, imigração e bem-estar social" (Ajana, 2010, p.237). Além dos riscos associados ao uso de biometria e citados anteriormente, devemos considerar que essa tecnologia tem em seu âmago o expurgo da dimensão narrativa que integra a identidade humana (Ajana, 2013, 2010). Afinal, quem a pessoa é ultrapassa os limites impostos pela linguagem: quando uma pessoa tenta dizer *quem é* ela, acaba dizendo *o que* ela é, o que aponta para a ambiguidade própria da identidade e a complexidade das experiências vividas (Ajana, 2010). Os sujeitos que inspiram o esforço filosófico de Ajana são os requerentes de asilo. Contudo, observando as discussões sobre os riscos das tecnologias biométricas e conjugando-os aos esforços teóricos de Mbembe e Ajana, percebemos que essas tecnologias usadas inclusive no bojo de estratégias de marketing são produtoras de vulnerabilidade para os consumidores, sendo capazes de universalizar os riscos associados a elas, dada a sua aspiração excessivamente zelosa à objetividade, exatidão e precisão.

Nos parece evidente que a posição majoritária, seguindo o mercado de bilhões e o posicionamento do Marketing Science Institute (MSI, 2020), é de que as tecnologias biométricas são incontornáveis. Preocupações com questões éticas acompanham essa posição, porém a discussão sobre privacidade do consumidor, que normalmente ocorre dentro do âmbito acadêmico de marketing (eg Bleier, Golfarb & Tucker, 2020) é limitada. O conceito de vulnerabilidade amplia essa discussão ao possibilitar que seja considerada a potencial vulnerabilidade a qual todos estamos sujeitos enquanto sociedade face à perfilização.

Discutimos neste artigo questões que envolvem aspectos legais da proteção de dados para mostrar que o debate no âmbito jurídico não está centrado exclusivamente em questões de privacidade e liberdades civis. A LGPD, assim como outras legislações internacionais de proteção de dados, sinaliza uma preocupação com o tratamento que os dados podem receber após sua coleta e, como sugere Zanatta (2019), isso está relacionado aos riscos da perfilização, ultrapassando a esfera individual e subjetiva, normalmente associada aos estudos que têm como foco o consumidor e as estratégias de marketing que visam experiências notáveis. Contra isso, tornar dados pessoais anônimos não surte efeitos para além da manutenção da privacidade. Perfis ainda serão produzidos e usados contra os consumidores cuja privacidade foi protegida.

Falar sobre marketing biopolítico não excluí o fato de que vivemos em uma sociedade de controle (Deleuze, 1992), na qual somos livres (ou acreditamos que somos) para vivermos nossas vidas sem estruturas que forneçam disciplina, principalmente física. Em uma sociedade de controle as estruturas são flexíveis, maleáveis e visam modular o

comportamento humano (Deleuze, 1992, p.4). Os computadores são emblemáticos desse tipo de sociedade (Deleuze, 1992, p.6) e os indivíduos se tornaram meros sujeitos incorporados, infinitamente divisíveis e redutíveis a dados pelas tecnologias de controle – "divíduos" (Deleuze, 1992, p.5). Cobbe (2021) argumenta que apesar de toda liberdade, não necessariamente estamos livres de disciplina: mesmo em sociedades de controle, somos disciplinados através da internalização da lógica social, o que significa que a disciplina assumiu uma forma que lhe permita se estender mais amplamente. Uma maneira de entender como vulnerabilidade e biopolítica e governança estão vinculadas é pensar sobre o porquê de precisarmos de dados biométricos quando já vivemos em tempos nos quais quantidades massivas de dados já são produzidas voluntariamente por consumidores, coletadas e tratadas. Outra pergunta que importante é o porquê da necessidade de predição, já que prever é, em si, uma forma de controle (Ajana, 2013).

São questões sem respostas fáceis e imediatas, mas existem indícios na literatura para aqueles dispostos a ver. Ceyhan (2002) trabalha com a ideia de gestão da incerteza e do risco ao explorar o uso da biometria nas políticas de segurança contemporâneas nos Estados Unidos e na França. A biometria guarda, segundo Ceyhan (2002, p.113), um objetivo de identificação, ou seja, "a atribuição de uma identidade reconhecível a uma pessoa por meio de um processo de distinção entre uma pessoa "perigosa" e "não perigosa" que vai além de um simples ato de autenticação". Mohan e Wall (2007) exploram o conceito de vigilância somática que envolve o monitoramento dos corpos através de dispositivos variados, transformando-os em nós dentro de redes que objetivam e extraem valor dos indivíduos ao mesmo tempo que ignora seu contexto social (p. 169). Os autores concordam que se trata de uma forma de exercer controle através da modulação das capacidades do corpo ou através do automonitoramento e modificação do comportamento. Crampton (2019) identifica e analisa o Microsoft Face, um dos principais sistemas biométricos faciais no mercado que promete analisar quais das sete emoções "universais" um sujeito está experimentando. Segundo o autor, o software representa uma maneira do capital neoliberal de se apropriar da experiência humana, sujeitando seus usuários à governança algorítmica, o que possibilitaria prever e alterar comportamentos.

Acreditamos que são necessários mais trabalhos dedicados à vulnerabilidade dos consumidores na era do marketing digital, levando em consideração os resultados não desejados da perfilização e outros problemas, como o racismo algorítmico (eg Silva & Araújo, 2020).

6. Considerações Conclusivas

Nas pesquisas sobre vulnerabilidade o contexto é o foco do estudo e pode ser um fator impulsionador para a transformação ou impacto, bem como contribuição teórica (Dunnett et al., 2018, p.367). O contexto descrito inicialmente e aprofundado aqui parece apontar até agora para a necessidade de maior cautela com o uso das tecnologias biométricas nas estratégias de marketing, para que assim não sejam aprofundadas, nem produzidas vulnerabilidades para consumidores e sociedade em geral. Essas tecnologias são usadas sob o pretexto de contribuir para a segurança, eliminar riscos e oferecer experiências de consumo cada vez melhores. Ainda que sejam utilizadas de boa fé, ao contrário do que aconteceu no caso Raia-Drogasil, devemos questionar a necessidade de predição e controle associada às biometrias, pois essas estão diretamente relacionadas à produção de vulnerabilidade para a sociedade.

Buscar formas de promover a educação dos consumidores sobre seus direitos e principalmente sobre os riscos das TIC é urgente. Existem coletivos que atuam nesse sentido, como o Coding Rights, que promove cursos virtuais de proteção no ambiente digital que são abertos ao grande público e gratuitos. Material similar poderia ser produzido por

pesquisadores de marketing em parceria com pesquisadores de direito, usando linguagem acessível e com distribuição gratuita através de download e impressos, alertando consumidores sobre os direitos previstos na LGPD e riscos das tecnologias biométricas, além de como se prevenir e a quem recorrer em casos como o da Raia-Drogasil. Essa interface com a sociedade e com os consumidores fortalece o propósito das pesquisas de consumo, principalmente daquelas cujo foco é a vulnerabilidade do consumidor.

Nota da RIMAR

Uma versão preliminar desse artigo foi apresentada no XLVI *Encontro da ANPAD – EnANPAD*, em 2022.

Referências

Ajana, B. (2010). Recombinant Identities: Biometrics and Narrative Bioethics. *Journal of Bioethical Inquiry,* 7, 237–258

Ajana, B. (2013). *Governing through Biometrics: The Biopolitics of Identity*. London: Palgrave Macmillan

Andronikou, V., Yannopoulos, A., & Varvarigou, T. (2008). Biometric Profiling: Opportunities and Risks. In: Hildebrandt, M. & Gutwirth, S. (eds.) *Profiling the European Citizen – Cross-Disciplinary Perspectives*, Springer, Dordrecht, 131-145.

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. *Journal of Macromarketing*, *25*(2), 128-139.

Baker, S. M., & Mason, M. (2012). Toward a process theory of consumer vulnerability and resilience: Illuminating its transformative potential. In D. G. Mick (Ed.), *Transformative consumer research for personal and collective well-being* (pp. 571-592). New York, NY: Routledge.

Beer, D. (2014). The Biopolitics of Biometrics: An Interview with Btihaj Ajana. *Theory, Culture & Society*, 31(7/8), 329–336

Bioni, B. (2019). *Autodeterminação informacional: qual o papel e os limites do consentimento na proteção dos dados pessoais.* São Paulo: Grupo Gen.

Bleier, A., Goldfarb, A., & Tucker, C. (2020). Consumer privacy and the future of data-based innovation and marketing. *International Journal of Research in Marketing*, 37(3), 466-480

Bruno, F. G., Bentes, A. C. F., & Faltay, P. (2019). Economia Psíquica dos Algoritmos e Laboratório de Plataforma: Mercado, Ciencia e Modulação do Comportamento. *Revista Famecos*, 26(3), e33095-e33095.

Charitsis, V. (2019). Survival of the (Data) Fit: Self-Surveillance, Corporate Wellness, and the Platformization of Healthcare. *Surveillance & Society*, 17(1/2), 139-144.

Ceyhan, A. (2002). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. *Surveillance & Society*, 5(2), 102-123.

Cobbe, J. (2021). Algorithmic Censorship by Social Platforms: Power and Resistance. *Philosophy & Technology*, 34(4), 739-766.

CONJUR (2021a). Disponível em https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis . Acesso em 26 de março de 2022.

CONJUR (2021b). Disponível em https://www.conjur.com.br/2021-set-30/drogasil-nao-esclarece-finalidade-biometria-procon-sp . Acesso em 26 de março de 2022.

Costanza-Chock, S. (2018). Design Justice, A.I., and Escape from the Matrix of Domination. *Journal of Design and Science*, http://dx.doi.org/10.21428/96c8d426

Crampton, J. W. (2019). Platform Biometrics*. Surveillance and Society, 17(1/2): 54-62.*

Darmody, A., & Zwick, D. (2020). Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. *Big Data & Society*, 7(1), 2053951720904112.

Daunt, K. L., & Greer, D. A. (2017). The dark side of marketing: Introduction to the special issue. *Journal of Marketing Management*, 33 (15-16), 1231-1235.

Dean, J. Communicative Capitalism: Circulation and the Foreclosure of Politics. In: Boler, M. (Ed.) *Digital Media and Democracy: Tatics in Hard Times*, 101-121.Cambridge, Massachusetts: The MIT Press, 2008.

Deleuze, G. (1992). Postscript on the Societies of Control. October, 59, 3–7. http://www.jstor.org/stable/778828

Doneda, D. (2006). *Da Privacidade à Proteção de Dados Pessoais.* Rio de Janeiro: Renovar.

Du, R. Y., Netzer, O., Schweidel, D. A., & Mitra, D. (2021). Capturing Marketing Information to Fuel Growth. *Journal of Marketing*, *85*(1), 163–183.

Dunnett, S., Hamilton, K., & Piacentini, M. (2018). Consumer vulnerability: critical insights from stories, action research and visual culture. In *The Routledge Companion to Critical Marketing* (pp. 366-382). Routledge.

Haggerty, K. D. & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology, 51*(4): 605-622.

IDEC (2021). https://idec.org.br/idec-na-imprensa/idec-notifica-raia-drogasil-dono-da-droga-raia-sobre-biometria-digital

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1), 4-20.

Jones, J. L, & Middleton, K. L. (2007). Ethical decision-making by consumers: the roles of product harm and consumer vulnerability. *Journal of Business Ethics*, *70*(3), 247-264.

Kanashiro, M. M., Bruno, F. G., Evangelista, R. de A., Firmino, R. J. (2013) Maquinaria da privacidade. RUA [online] 19(2), 22-41

Kotler, P. (1972). A generic concept of marketing. *Journal of marketing*, 36(2), 46-54.

Lupton, D. (2016). *The Quantified Self* (ePub). Cambridge, UK: Polity Press.

Marketing Science Institute (MSI) (2020). Research Priorities 2020-2022. Disponível em https://www.msi.org/wp-content/uploads/2020/06/MSI_RP20-22.pdf. Acesso em 27 de março de 2022.

Mendes, L. S. (2016). O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor, 105*, 1-30.

Monahan, T., & Wall, T. (2007). Somatic surveillance: Corporeal control through information networks. *Surveillance & Society*, 4(3), 154-173.

Moutinho, L. (2021). Further future in marketing research techniques. In Wright, L. T., Moutinho, L., Stone, M, & Bagozzi, R. P. (eds.) *The Routledge Companion to Marketing Research*, 540-551. London/New York: Routledge

Nason, R. W. (1989). The social consequences of marketing: macromarketing and public policy. *Journal of Public Policy & Marketing*, 8(1), 242-251.

Oliveira, R. C. de A. de. (2021). Plataformização da pele? Tatuagens biométricas, dataísmo e a datificação do consumidor. *Cadernos EBAPE. BR,* 20*, 207-217.*

Patterson, M., O'Malley, L., & Evans, M. (1997). Database marketing: investigating privacy concerns. *Journal of Marketing Communications*, 3(3), 151-174.

Plassmann, H., Venkatraman, V., Huettel, S., & Yoon, C. (2015). Consumer Neuroscience: Applications, Challenges, and Possible Solutions. *Journal of Marketing Research*, 52 (4), 427–435.

Pridmore, J. & Zwick, D. (2011). Editorial: Marketing and the Rise of Commercial Consumer Surveillance. *Surveillance & Society*, 8(3), 269-277.

Puntoni, S., Reczek, R. W., Giesler, M., & Botti, S. (2021). Consumers and artificial intelligence: An experiential perspective. *Journal of Marketing*, *85*(1), 131-151.

Saúde Business (2019). Disponível em https://www.saudebusiness.com/ti-e-inovao/healthbit-como-o-uso-de-dados-e-tecnologias-pode-melhorar-o-sistema-de-sade . Acesso em 26 de março de 2022.

Shugan, S. M. (2004). The Impact of Advancing Technology on Marketing and Academic Research. *Marketing Science* 23(4), 469-475.

Shultz II, C. J., & Holbrook, M. B. (2009). The paradoxical relationships between marketing and vulnerability. *Journal of Public Policy & Marketing*, *28*(1), 124-127.

Silva, M. L., & Araújo, W. F. (2020). Biopolítica, racismo estrutural-algorítmico e subjetividade. *Educação Unisinos*, 24, 1-20.

Silva, R. O., Barros, D. F., Gouveia, T. M. A., & Merabet, D. O. B. (2021). Uma discussão necessária sobre a vulnerabilidade do consumidor: avanços, lacunas e novas perspectivas. *Cadernos EBAPE.BR*, 19, 83-95.

Smith, N. C, & Cooper-Martin, E. (1997). Ethics and target marketing: the role of product harm and consumer vulnerability. *Journal of Marketing*, *61*(3), 1-20.

Tadajewski, M., Denegri-Knott, J., Varman, R. (2018). Introducing and Advancing Critical Marketing Studies. In: Tadajewski, M., Higgins, M., Denegri-Knott, J. and Varman, R. (2018) *The Routledge Companion to Critical Marketing*. New York, NY: Routledge.

The Intercept (2021). Disponível em https://theintercept.com/2021/07/05/nao-cadastre-biometria-na-droga-raia/. Acesso em 10 de julho de 2021.

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2), 197-208.

Verhulst, N., De Keyser, A., Gustafsson, A., Shams, P., & Van Vaerenbergh, Y. (2019). Neuroscience in Service Research: An Overview and Discussion of its Possibilities. *Journal of Service Management, 30*(5), 621–649.

Wästlund, E., Otterbring, T., Gustafsson, A., & Shams, P. (2015). Heuristics and resource depletion: Eye-tracking customers in situ gaze behavior in the field. *Journal of Business Research, 68*(1), 95–101.

Zanata, R. A. F. (2017). Proteção de Dados Pessoais como Regulação de Risco: uma nova moldura teórica? *Artigos Selecionados REDE 2017*, *I Encontro da Rede de Pesquisa em Governança da Internet*, Rio de Janeiro, 14 de novembro de 2017, 176-193.

Zanatta, R. A. F. (2019). Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados. In: *ResearchGate* [S. l.] Disponível em https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais. Acesso em 26 de março de 2022.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology,* 30 (1), 75-89.

Zwick, D., & Denegri-Knott, J. (2009). Manufacturing Customers: the database as new means of production. *Journal of Consumer Culture*, 9(2), 221-247.

Zwick, D., & Bradshaw, A. (2018). Biopolitical marketing and the commodification of social contexts. In: Tadajewski, M., Higgins, M., Denegri-Knott, J. and Varman, R. (2018) *The Routledge Companion to Critical Marketing*. New York, NY: Routledge.

Autora

1. Renata Oliveira, Doutora em Administração pela UNIGRANRIO. Professora do Programa de Pós-Graduação em Administração da UNIGRANRIO.

Contribuição da autora

Contribuição	Renata Oliveira
1. Definição do problema de pesquisa	✓
2. Desenvolvimento de hipóteses ou questão de pesquisa (no caso de trabalho empírico)	
3. Desenvolvimento de proposição teóricas (no caso de trabalho teórico)	✓
4. Referencial/fundamentos teórico(s) / revisão de literatura	✓
5. Definição de procedimentos metodológicos	
6. Coleta de dados / trabalho de campo	
7. Análise e interpretação de dados (quando existentes)	
8. Revisão do texto	✓
9. Redação do texto	✓

[i] Modelo que presume a ampla cognição dos termos de uso e políticas de privacidade online para livre contratação entre as partes (Zanatta, 2017, p.178)

[ii] https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/