Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 15.07.2021
Aprovado em: 26.07.2021

PERFILIZAÇÃO E COLETA DE DADOS COMPORTAMENTAIS: AS POLÍTICAS DE PRIVACIDADE DA GOOGLE PELA ÓTICA CONSUMERISTA NO CAPITALISMO DA VIGILÂNCIA

Naína Ariana Souza Tumelero[1]

Resumo
O presente artigo partiu do método indutivo e da técnica de pesquisa documental para analisar as técnicas de perfilização e a coleta de dados comportamentais por meio das políticas de privacidade da Google no contexto do capitalismo da vigilância. Esta nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado utilizando-se da perfilização, técnica ainda pouco explorada na bibliografia brasileira. Tal processo impacta diretamente a efetivação de direitos como a autodeterminação informativa, a informação e a livre iniciativa, aprofundando a vulnerabilidade do consumidor.

Palavras-chave: capitalismo da vigilância; dados comportamentais; proteção dos consumidores; perfilização; Google.

PROFILLING AND BEHAVIORAL DATA COLLECTION: GOOGLE'S PRIVACY POLICIES FROM A CONSUMER PERSPECTIVE IN SURVEILLANCE CAPITALISM

This paper aims to analyze profiling techniques and the collection of behavioral data through Google's privacy policies in the surveillance capitalism by the inductive method and the documentary research technique. This new form of information capitalism seeks to predict and modify human behavior as a mean of producing revenues and market control using profiling, a technique that is still not explored in the Brazilian bibliography so far. Such a process directly impacts the realization of rights such as informational self-determination, information, free enterprise and deepening consumer vulnerability.

Keywords: surveillance capitalism; behavioral data; consumer protection; profiling; Google

Introdução

Já vem se apontando a importância da leitura transversal e da articulação entre o tema da proteção de dados e o direito dos consumidores. O que se vê pela movimentação e atuação dos PROCONS e das entidades de defesa dos consumidores desde antes da vigência da Lei

[1] Mestra em Direito (UFSC). Especialista em Direito Civil e Processual Civil. Advogada. Doutoranda Interdisciplinar em Ciências Humanas (UFSC). Atualmente dedicada aos temas de proteção de dados, relação humana com a tecnologia e condição humana no capitalismo da vigilância. E-mail: naina.tumelero@gmail.com. http://lattes.cnpq.br/8147326214849577

Geral de Proteção de Dados (LGPD), o que culminou na assinatura, neste último dia 22 de março de 2021, do acordo de cooperação técnica entre a Secretária da Secretaria Nacional do Consumidor (SENACON) e a Autoridade Nacional de Proteção de dados (ANPD), destinado à proteção de dados dos consumidores, cujo principal objetivo é maior agilidade nas investigações de incidentes de segurança.

Neste contexto, o presente artigo tem por objetivo geral analisar as técnicas de perfilização e a coleta de dados comportamentais por meio das políticas de privacidade da Google no contexto do capitalismo da vigilância. A importância de tal análise ser feita de forma interdisciplinar é o reconhecimento da vulnerabilidade e da posição complexa de "titular consumidor".

O "profiling" ou "perfilização", é um registro sistemático, proposital e classificatório de dados relacionados aos consumidores que permite a um provedor de serviços atingir indivíduos por meio de anúncios ou posicionamento de produto/serviço específicos, restringindo, de certa forma, a liberdade de escolha dos consumidores.

Sem o objetivo de exaurir o tema, pelo contrário, de contribuir com essa questão todavia recente no cenário brasileiro, pelo método indutivo o artigo partirá do referencial teórico do capitalismo da vigilância, que tem como principal nome a autora estadunidense Shoshana Zuboff, seguido pela pesquisa documental com base nas políticas de privacidade dos serviços Google, avançando com a conceituação da perfilização com base em estudos estrangeiros e também na autora Ana Frazão para ao final, considerando todas essas questões, realizar apontamentos com base no CDC e na LGPD.

Em razão da atualidade e urgência do tema, preferiu-se partir da superação de algumas questões como: o histórico da defesa dos consumidores e da proteção de dados no Brasil, o reconhecimento da vulnerabilidade do consumidor na era digital e a direta relação da proteção de dados com os direitos da personalidade. Deste modo, foram utilizadas as legislações e as políticas de privacidade como fonte primária e principalmente artigos científicos publicados desde o ano de 2017, data intermediária entre a realização do Regulamento Geral sobre a Proteção de Dados Europeu (GPDR), datado de 14/04/2016 e a sua implementação em 25/05/2018, quando as discussões sobre proteção de dados e as produções científicas começaram a tomar corpo no Brasil.

1 Capitalismo da vigilância e os termos de privacidade do Google

Com alguns dados é possível descobrir informações sobre o futuro de uma pessoa. Em 2012, Adam Sadilek, pesquisador da Universidade de Rochester e John Krumm, engenheiro no laboratório de pesquisa da Microsoft, mostraram que poderiam prever a localização aproximada de uma pessoa até 80 semanas no futuro, com uma precisão acima de 80%. Para atingirem tal resultado, os pesquisadores extraíram o que eles descreveram como um "conjunto de dados maciços" coletando 32 mil dias de leituras de GPS tiradas de 307 pessoas e 396 veículos.

O capitalismo da vigilância, conceituado por Zuboff (2018. 18) se formou gradualmente durante a última década, incorporando novas políticas e relações sociais que ainda não haviam sido bem delineadas ou teorizadas. A autora aponta o fenômeno da "transformação da cotidianidade em estratégia de comercialização" (ZUBOFF, 2018, p. 19), isto é, o cotidiano, a rotina, os influencers, o "comum" transformado ou cooptado por estratégicas de marketing.

O capitalismo da vigilância e a cultura da vigilância são categoriais complementares, e conforme Lyon (2018, p. 153), a cultura da vigilância pode ser compreendida como um produto das condições contemporâneas da modernidade tardia ou da "modernidade digital".

Uma questão fundamental da cultura da vigilância é a densidade dos rastros digitais deixados, tendo em vista que ao longo do tempo o sucesso do capitalismo dependeu da emergência de novas formas de mercado com novas lógicas de acumulação (ZUBOFF, 2018, p. 23). Como aponta a autora (ZUBOFF, 2018 p. 18), esta nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado, "o big data é, acima de tudo, o componente fundamental de uma nova lógica de acumulação, profundamente intencional e com importantes consequências, que eu chamo de capitalismo da vigilância" (ZUBOFF, 2018 p. 18). Nas palavras da autora: "o capitalismo de vigilância, portanto, se qualifica como uma nova lógica de acumulação, com uma nova política e relações sociais que substituem os contratos", o "Big Other existe na ausência de uma autoridade legítima e é em grande parte livre de detecção ou de sanções. Neste sentido, o Big Other pode ser descrito como um golpe automatizado de cima, não um golpe de Estado, mas um golpe entre as pessoas" (ZUBOFF, 2018, p. 49).

Zuboff (2018, p. 18) afirma que o big data não é uma tecnologia ou um efeito tecnológico inevitável, tendo origem no social, é ali que devemos encontrá-lo e estudá-lo.

Ideia que corrobora Lyon (2018, p. 173) ao afirmar que as práticas que emergiram nas mídias sociais são práticas sociais, cujos imaginários que elas formam e que as moldam são igualmente sociais.

Importante notar que o big data é constituído pela captura de *small data*, das ações e discursos, mediados por computador, de indivíduos no desenrolar da vida prática. Nada é trivial ou efêmero, desde as curtidas do Facebook, as buscas no google, e-mails, localizações, até palavras com erros ortográficos (ZUBOFF, 2018, p. 31). Esses fluxos de dados foram rotulados pelos tecnólogos de "*data exhaust*" (ZUBOFF, 2018, p. 32). Ou seja, mais usuários produzem mais *data exhausts*, que por sua vez, melhoram o valor preditivo das análises e resultam em leilões mais lucrativos, ou seja, o que importa é a quantidade e não a qualidade dos dados (ZUBOFF, 2018, p. 33).

Conforme Lyon (2018, p. 166), deve-se ter em mente o caráter multifacetado das situações em que a vigilância é experimentada, portanto, reconhecer a variedade e a sutileza das reações nos ajuda a compreender as realidades vividas pelos sujeitos da vigilância. Ou seja, o social.

Na tecnologia da informação, conforme aponta Zuboff (2018. p. 20), a automação gera informações que proporcionam um nível mais profundo de transparência a atividades que pareciam parcial ou totalmente opacas. Neste sentido, a cultura da vigilância é formada por meio de dependência organizacional, poder político econômico, conexões de segurança e envolvimento em mídias sociais (LYON, 2018, p. 154).

Todos esses blocos conceituais podem facilitar a compreensão sobre o big data tendo em mente que, pelo menos 3 bilhões dos 7 bilhões de pessoas do mundo têm uma ampla gama de atividades diárias mediadas, muito além das fronteiras tradicionais do local de trabalho (ZUBOFF, 2018, p. 23).

Na relação entre a utilização de dados na modulação do comportamento dos consumidores, Zuboff (2018, p. 34) afirma que "os processos extrativos que tornam a big data possível normalmente ocorrem na ausência de diálogo ou de consentimento", ainda que se utilizem não apenas de fatos objetivos, mas especialmente de questões subjetivas. "É propriamente o status de tais dados como sinais de subjetividade que os tornam mais valiosos para os anunciantes" (ZUBOFF, 2018, p. 34).

De acordo com Varian, economista da Google, as pessoas concordam com essa invasão de privacidade caso recebam algo em troca, como uma hipoteca, um conselho médico, um

conselho legal, ou mesmo sugestões do seu assistente pessoal digital (ZUBOFF, 2018, p. 46). Isso o que pode ser chamado de "vigilância suave" de acordo com Lyon (2018, p. 167), tornou-se hoje lugar-comum.

Zuboff (2018, p. 41) citou entrevista concedida por Varian, que afirmou que "como as transações são agora mediadas pelo computador, podemos observar comportamentos que anteriormente não eram observáveis e redigir contratos sobre esses comportamentos [...] as transações mediadas pelo computador permitiram novos modelos de negócios" (ZUBOFF, 2018, p. 41)

Sobre tais novos negócios, afirma a autora (ZUBOFF, 2018, p. 51):

> As ferramentas oferecidas pela Google e outras empresas capitalistas de vigilância respondem às necessidades dos indivíduos sitiados da segunda modernidade – e, assim como o fruto proibido, uma vez que são experimentadas, tona-se impossível viver sem elas. Quando o Facebook ficou fora do ar em cidades dos Estados Unidos durante algumas horas no verão de 2014, muitos estadunidenses chamaram seus serviços de emergência locais no 911.

A autora pontua que "essa dependência social está no cerne do projeto de vigilância", da forma que o sentimento de que esses serviços são essenciais a uma vida mais eficaz é o contrário da resistência ao projeto de vigilância, conflito que produz uma espécie de entorpecimento psíquico (grifo meu) que habitua as pessoas à serem rastreadas, analisadas, mineradas e modificadas ao mesmo tempo que elimina os antigos emaranhados de reciprocidade e confiança em favor do ressentimento desconfiado, da frustração, da defesa ativa e/ou da dessensibilização (ZUBOFF , 2018, p. 51).

Daí a importância de enfocar igualmente em uma cultura da vigilância, conforme Lyon, "o senso de como a vigilância institucional pode ser enfrentada, tecnológica, política, jurídica e, acima de tudo, eticamente, deve ser revisto. Culturas de vigilância, sejam elas críticas ou complacentes, são socialmente construídas e, portanto, podem ser desafiadas e reconstruídas" (LYON, 2018, p. 172).

2 Políticas de privacidade da Google: onde o capitalismo da vigilância encontra o consumidor

O estudo de caso, por meio da análise documental nos auxilia a visualizar de que forma a perfilização por meio da coleta de cookies é feita e está atrelada ao comportamento na internet. A coleta de dados foi feita na data de 28/03/21 na página oficial do Google Privacidade e Termos[2]. A google é considerada por muitos como a pioneira do big data e da lógica de acumulação mais ampla, dominada por Shoshana Zuboff (2018, p. 25) por capitalismo de vigilância, da qual o big data é tanto uma condição quanto uma expressão. "No Google, nós buscamos ideias e produtos que frequentemente desafiam os limites da tecnologia existente" sessão de tecnologia.

As questões que orientam essa coleta de dados são: Como está a linguagem e apresentação da política? Para quem se aplicam os temos? Para que servem os cookies? Como e de onde são coletados? Quais são os dados utilizados?

Todos os dados coletados se referem a todos os serviços Google listados na sessão "Guia de privacidade", quais sejam: a ferramenta de pesquisa, gmail, youtube, *hangouts*, google maps, google chrome, google+, dispositivos Android Nexus, google agenda, google play, anúncios, blogger, google drive, google fotos, documentos google (incluindo documentos, planilhas, apresentações, formulários e desenhos), google notícias, pesquisa de livros do google, google *keep*, google *payments*, google *analytics*, grupos do google, google *nest*.

A Google fornece serviços, processa informações e atende às leis de privacidade aplicáveis em duas afiliadas, a "Google *Ireland Limited*", para contas do Espaço Econômico Europeu (países da União Europeia, Islândia, Liechtenstein e Noruega) ou na Suíça, regida, portanto, pelo GDPR; e a "Google LLC", com sede nos Estados Unidos, que atende o restante do mundo, sendo que a versão da política que rege a relação entre usuário e Google pode variar a depender de leis locais[3], mas **os Serviços do Google são essencialmente os mesmos**, independentemente de qual afiliada os oferece ou do país associado à sua conta.

No que tange à apresentação das políticas de privacidade, pode-se dizer que a linguagem está acessível, constando, inclusive, imagens que facilitam a leitura. No entanto, toda a redação da política está apresentada em um sentido de bem-estar do consumidor, ocultando em grande medida a finalidade econômica da extração dos dados. É o que se vê

[2] https://policies.google.com/technologies/cookies?hl=pt-BR
[3] https://policies.google.com/faq?hl=pt-BR

neste trecho da parte "como o google usa informações de sites ou apps que utilizam nossos serviços":

Constam nos termos informativos: "Muitos sites e apps usam serviços do Google para melhorar o próprio conteúdo e mantê-lo gratuito". Quando integram nossos serviços, esses sites e apps compartilham informações com o Google:

> O Google usa as informações compartilhadas por sites e apps para entregar nossos serviços, mantê-los e melhorá-los, além de desenvolver novos serviços, medir a eficácia da publicidade, proteger contra fraude e abuso e personalizar o conteúdo e os anúncios que você vê no Google e nos sites e apps de nossos parceiros (GOOGLE, 2021, página da web).

A respeito da perfilização, o Google informa utilizando um exemplo:

> [...] quando você acessa um site que usa serviços de publicidade, como o Google AdSense, incluindo ferramentas de análise, como o Google Analytics, ou um site com conteúdo de vídeo incorporado do YouTube, seu navegador da Web envia automaticamente certas informações ao Google. Isso inclui o URL da página que você está acessando e seu endereço IP. Também podemos configurar cookies no seu navegador ou ler os cookies que já estão lá. Os apps que usam serviços de publicidade do Google também compartilham informações com o Google, como o nome do app e um identificador exclusivo para publicidade.

Em relação às bases legais utilizadas, o Google expõe que "o processamento pode acontecer com seu **consentimento** ou em nome de **interesses legítimos"**, exemplificando como interesses legítimos o fornecimento, manutenção e melhoria dos serviços para atender às necessidades dos usuários (GOOGLE, 2021, página da web) (grifo meu).

A Google destinou um trecho nas suas políticas para a questão da perfilização em si, denominada "personalização de anúncios", onde a empresa afirma que, no caso de a personalização estar ativada o Google usará as informações para "tornar os anúncios **mais úteis**" (grifo meu) (GOOGLE, 2021, página da web).

E explica com um exemplo "um site que vende mountain bikes pode usar os serviços de anúncios do Google. Depois de visitar esse site, você poderá ver um anúncio para mountain bikes em um site diferente que mostra anúncios veiculados pelo Google" (GOOGLE, 2021, página da web). No caso de personalização de anúncios desativada, o Google informa que "não coletará nem usará [...] informações para criar um perfil de anúncios

ou personalizar os anúncios", o consumidor, no caso, ainda verá anúncios, mas "talvez eles não sejam tão úteis" (GOOGLE, 2021, página da web). E mesmo com a personalização de anúncios desativadas:

> [...] os anúncios ainda podem se basear no assunto do site ou app sendo visualizado, nos seus termos de pesquisa atuais ou na sua localização geral, mas **não nos seus interesses, histórico de pesquisa ou histórico de navegação**. Suas informações ainda podem ser utilizadas para as outras finalidades mencionadas acima, como medição da eficácia da publicidade e proteção contra fraude e abuso (GOOGLE, 2021, página da web).

Ao optar pela desativação o usuário receberá a mensagem "Se você desativar a personalização de anúncios eles continuarão sendo exibidos, mas poderão ser menos úteis para você; não será mais possível definir preferências para anúncios ou anunciantes [...]".

A perfilização é realizada por meio de cookies, e nas suas políticas de privacidade a Google (2021, página da web) expõe que: "um cookie é um pequeno texto enviado ao navegador pelo site que você visita. Com ele, o site lembrar das informações sobre a visita, o que facilita seu próximo acesso e deixa o site mais útil para você". Ainda, com a intenção de traduzir a perfilização como benéfica ao consumidor, opta por exemplificar da seguinte forma: "usamos cookies para lembrar seu idioma preferido, mostrar anúncios mais relevantes para você, contar quantos visitantes recebemos em uma página, ajudar você a se inscrever nos nossos serviços, proteger seus dados e lembrar suas Configurações de anúncios" (GOOGLE, 2021, página da web).

São utilizadas 5 classificações de cookies: funcionalidade, segurança, análise, publicidade e personalização, além de outras informações que não tratam especificamente dos cookies, mas de dados comportamentais são o reconhecimento de padrões, a localização e a utilização da voz.

1. Cookies de funcionalidade	Os cookies de f**uncionalidade** permitem a interação dos usuários com um serviço ou site para acessar recursos considerados fundamentais. Esses recursos incluem preferências de idioma, otimizações de produto para manter e melhorar um serviço e a manutenção de informações relacionadas à sessão do usuário, como o conteúdo de um carrinho de compras. O termo de privacidade traz uma série de cookies, cada qual com o tempo de validade, que é o tempo em que a informação fica registrada. O termo também apresenta aos cookies utilizados pelo Youtube. Segundo a Google, alguns cookies são usados para manter e melhorar a experiência do usuário durante uma determinada sessão de navegação, e somente será usado enquanto o navegador do usuário estiver aberto. Outros cookies melhoram o desempenho dos Serviços do Google, por exemplo, o "CGIC" que preenche automaticamente as consultas de pesquisa com base na entrada inicial do usuário para melhorar a exibição de resultados, sendo este com validade de seis meses.
2. Cookies de segurança	São cookies usados para questões de segurança que evitam fraudes, autenticam usuários e os protegem quando eles interagem com um serviço. Também autenticam usuários com o objetivo de garantir que apenas o proprietário de uma conta possa acessá-la. Por exemplo, cookies chamados "SID" e "HSID" contêm dados criptografados e assinados digitalmente do ID da Conta do Google de um usuário, além do horário de login mais recente. Alguns cookies são usados para evitar spam, fraude ou abusos. Por exemplo, os cookies "pm_sess" e "YSC" asseguram que as solicitações feitas em uma sessão de navegação realmente são do usuário, e não de outros sites. Esses dois cookies impedem sites maliciosos de agir sem o conhecimento do usuário e de se passarem por ele.

3. Análise	São cookies que coletam dados para entender como os usuários interagem com um determinado serviço. Com essas informações, é possível ajustar o conteúdo e os recursos dos serviços e oferecer uma **melhor experiência do usuário**. Alguns cookies ajudam os proprietários de sites a entenderem o engajamento dos usuários, como é o caso do Google Analytics, que "usa um conjunto de cookies para coletar informações e relatar estatísticas de uso do site". Alguns cookies também permitem que um serviço diferencie um usuário de outro e tem validade de dois anos.
4. Publicidade	Para a publicidade os cookies incluem a personalização de anúncios, veiculação e renderização, limitação de vezes que um anúncio é exibido para um usuário, desativação de anúncios que o usuário escolheu deixar de ver e a medição da eficácia dos anúncios. Nesta sessão da política a Google traz alguns termos técnicos como "NID", "IDE" e "ANID" e não os traduzem, entretanto explicam para que cada um funciona. Também explica que outros Serviços do Google, como o YouTube, também podem usar esses cookies e outros para exibir anúncios mais relevantes. Alguns cookies usados para publicidade são destinados a usuários que fazem login para usar os Serviços do Google. As empresas podem anunciar nos Serviços do Google usando nossa própria plataforma de publicidade. Com ela, também é possível anunciar em sites de terceiros que sejam empresas parceiras. Alguns cookies são compatíveis com a exibição de anúncios pelo Google em sites de terceiros. Por exemplo, permitem que sites mostrem anúncios do Google e que meçam a atividade do usuário, o desempenho das campanhas publicitárias e as taxas de conversão de anúncios do Google nos sites acessados. Essa ativação é válida por 13 meses no Espaço Econômico Europeu (EEE), na Suíça e no Reino Unido e por 24 meses em outros lugares.

5. **Personalização**	Os cookies usados para personalização são utilizados com a justificativa de **melhorar a experiência do usuário** fornecendo conteúdo e recursos personalizados, que seria a própria definição da perfilização estudada no tópico anterior. São cookies que permitem recomendações melhores em um serviço. Neste sentido, a Google exemplifica com a ativação de recomendações personalizadas no YouTube baseadas nos vídeos assistidos e nas pesquisas anteriores. Além do cookie que ativa recursos de preenchimento automático personalizado na Pesquisa enquanto os usuários digitam termos de pesquisa.

Fonte: Guia de privacidade Google

Neste sentido, é importante entender também a utilização de outros dados comportamentais, que são o reconhecimento de padrões, a localização e a voz, que constam separadamente, na sessão "como a Google usa o reconhecimento de padrões para dar sentido a imagens". A google explica que os computadores podem ser treinados para reconhecer certos padrões de cores e formas, sendo que, por meio dessa tecnologia o Google fotos pode, por exemplo, organizar fotos e permitir que os usuários as encontrem com uma pesquisa simples. A mesma tecnologia pode ser utilizada para reconhecer os padrões comuns de formas e cores que compõem uma imagem digital de um rosto. Esse processo é conhecido como detecção facial e é utilizado também no *Street View*, em que os computadores tentam detectar e desfocar os rostos de todas as pessoas que estavam na rua quando o carro do *Street View* passou.

Essa mesma tecnologia de reconhecimento de padrões da detecção facial permite que um computador entenda as características do rosto detectado. Por exemplo, pode haver certos padrões que sugerem que um rosto está sorrindo ou que os olhos estão fechados. Uma tecnologia semelhante também disponibiliza o recurso de agrupamento por reconhecimento facial do Google Fotos em determinados países. Importante notar que os exemplos utilizados pela Google são apenas relacionados às fotos e pequenas praticidades, embora o reconhecimento facial já esteja sendo questionado nos termos da proteção dos dados e da personalidade[4].

[4] Neste sentido, verificar DE ÁVILA NEGRI, Sergio Marcos Carvalho; DE OLIVEIRA, Samuel Rodrigues; COSTA, Ramon Silva. O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL BASEADAS EM INTELIGÊNCIA ARTIFICIAL E O DIREITO À PROTEÇÃO DE DADOS. Direito Público, v. 17, n. 93, 2020.

Já, em relação à utilização da voz, os temos apresentam duas sessões diferentes, a primeira trata da pesquisa por voz e o segundo do Google Voice.

A Pesquisa por voz permite a consulta a um aplicativo cliente da Pesquisa do Google em vez de digitar essa consulta em um dispositivo. A Pesquisa por voz usa o reconhecimento de padrões para transcrever palavras faladas em texto escrito. Em cada consulta feita são armazenados o idioma, o país e o palpite do sistema para o que foi dito. As falas são mantidas para melhorar os serviços e treinar o sistema a reconhecer melhor a consulta de pesquisa correta. As falas serão enviadas para o Google na hipótese de se ter indicado a intenção de usar a função Pesquisa por voz (por exemplo, pressionando o ícone do microfone na barra de pesquisa rápida ou no teclado virtual ou dizendo "Google" quando a barra de pesquisa rápida indica que a função Pesquisa por voz está disponível).

Já o Google Voice armazena, processa e mantém o histórico de chamadas do usuário (incluindo o número de telefone do autor e do recebedor da chamada, a data, a hora e a duração da chamada), as saudações e mensagens de correio de voz, mensagens SMS, conversas gravadas e outros dados relacionados à conta do usuário para que ele receba o serviço.

Mesmo excluindo o histórico de chamadas, saudações e mensagens do correio de voz, (áudio e/ou transcrições), mensagens SMS e conversas gravadas, o histórico de chamadas de ligações sujeitas a cobrança poderá permanecer visível na conta.

Por fim, na sessão "Como a localização é usada para mostrar anúncios?", a Google explica que anúncios podem ser veiculados com base na localização geral, incluindo a localização derivada do endereço IP do dispositivo. E ainda, a depender das configurações de personalização, é possível receber anúncios baseados na atividade da Conta do Google.

Isso inclui o que está armazenado na Atividade na Web e de apps, que pode ser usado para anúncios. O exemplo utilizado é o seguinte:

> Se [...] frequenta regularmente algum local, como estações de esqui, é possível que você veja um anúncio de equipamentos de esqui ao assistir um vídeo no YouTube. O Google também usa o Histórico de localização de maneira anônima e agregada para os usuários que ativaram a opção, a fim de ajudar os anunciantes a mensurar com que frequência uma campanha de anúncios on-line ajuda a direcionar tráfego para lojas ou propriedades físicas.

1. Perfilizações e os riscos da utilização de dados comportamentais

Tendo em vista a leitura focada da política de privacidade da Google é possível inferir que a economia movida a dados e o capitalismo de vigilância são as duas faces da mesma moeda porque quanto maior é a importância dos dados, mais incentivo haverá para o aumento da vigilância e, por conseguinte, maior será a coleta de dados (FRAZÃO, 2019, Local: 968).

Desta forma, se torna relevante a compreensão do "*profiling*" ou, como estamos denominando aqui, a perfilização. Buchi et al (2020), por meio do artigo "*The chilling effects of algorithmic profling: Mapping the issues*" apresentaram resultados interdisciplinares nas áreas de direito, comunicação e tecnologia da informação.

A perfilização é definida pelos autores como um registro sistemático, proposital e classificatório de dados relacionados aos indivíduos. Um perfil é a compilação de dados pessoais, sendo que, na mudança para a era digital a criação de perfil passou a ser algorítmica e automatizada, culminando no *big data* e na criação de perfis a partir de fontes de dados muito mais extensas (BUSHI, et al, 2020, p. 02).

É possível se ter uma dimensão do risco para os consumidores considerando que Martin Hilbert, especialista em *Big Data*, afirma que, apenas com 150 "curtidas", determinados algoritmos podem saber mais sobre uma pessoa do que o seu companheiro e que, com 250 "curtidas", os algoritmos podem saber mais sobre uma pessoa do que ela própria (FRAZÃO, 2019, local: 934). Os algoritmos buscam padrões de correlações nos dados, de forma indutiva, produzindo novos conhecimentos a partir do conhecimento existente e analisando correlações (BUSHI, et al, 2020, p. 02).

O setor privado está particularmente interessado na classificação de determinados dados que se relacionam a um usuário específico ou à uma categoria de usuários. Segundo Buchi, et al (2020, p. 03) "os exemplos incluem dados relacionados a compras online e off-line, registros de censo, comportamentos e interesses de navegação online, dados de localização e assim por diante" (tradução minha). Como afirma Frazão (2019, local:920), dados importam na medida em que podem ser convertidos em informações necessárias ou úteis para a atividade econômica. Assim, a perfilização permite a um provedor de serviços atingir indivíduos por meio de anúncios ou posicionamento de produtos e serviços específicos (BUSHI, et al, 2020, p. 03), visando, evidentemente, a atividade econômica.

Os algoritmos estão programados para a extração de padrões e inferências que possibilitam a tomada de decisão de forma automatizada tanto sobre questões objetivas,

atreladas diretamente a dados sensíveis, além de decisões sobre questões subjetivas que envolveriam complexo juízo de valor, como:

> (i) avaliar as características, a personalidade, as inclinações e as propensões de uma pessoa, inclusive no que diz respeito à sua orientação sexual; (ii) analisar o estado de ânimo ou de atenção de uma pessoa; (iii) identificar estados emocionais, pensamentos, intenções e mesmo mentiras; (iv) detectar a capacidade e a habilidade para determinados empregos ou funções; (v) analisar a propensão à criminalidade; (vi) antever sinais de doenças, inclusive depressão, episódios de mania e outros distúrbios, mesmo antes da manifestação de qualquer sintoma (FRAZÃO, 2020, local 1051).

As inferências abrangem previsões sobre ações ou omissões futuras, características gerais e preferências específicas. Essas categorias de dados podem pintar um quadro detalhado de um indivíduo combinando informações "banais", como a versão do navegador usada, com atributos previstos, como o valor da casa. As inferências podem ser comunicadas abertamente ao usuário (por exemplo, recomendações para um show de música específico ou restaurante), podem ser meramente assumidas pelo usuário (por exemplo, anúncio que não está obviamente relacionado a uma pesquisa anterior), ou podem ser totalmente ocultadas (por exemplo, dados sendo reunidos e vendidos por corretores de dados, como a Acxiom, ou por terceiros, como foi o caso no escândalo Cambridge Analytica (BUSHI, et al, 2020, p. 03).

A perfilização costuma ser formada por dados pessoais fornecidos pelos próprios usuários, ou de inferências automatizadas extraídas de informações existentes, "não confidenciais" ou divulgadas voluntariamente, entretanto, a forma como os dados são utilizados desvia substancialmente de qualquer compreensão que os usuários poderiam fazer diretamente acerca do fornecimento (BUSHI, et al, 2020, p. 03). Analisando a política de privacidade da Google vê-se o que pontua Frazão (2019, local 927) que os cidadãos muitas vezes não conseguem saber quais dados foram coletados, e a dificuldade é ainda maior no que se refere à compreensão das inúmeras destinações que a eles pode ser dada e a extensão do impacto destas em suas vidas.

No setor privado, a vantagem competitiva da datificação da vida íntima e social das pessoas, na era do *big data*, tem causado um aumento nas capacidades e avanços das técnicas de vigilância de dados (BUSHI, et al, 2020, 03), o que leva a questionar inclusive as práticas concorrenciais atreladas.

No aspecto da responsabilidade civil, sem aprofundamentos por ora, essa prática também se apresenta como um desafio, tendo em vista que os autores (BUSHI, et al, 2020, p.

07) pontuam que os seus efeitos nem sempre são aparentes, diretos ou diretamente ligados às consequências da criação de perfis, sendo frequentemente intangíveis e difíceis de identificar ou quantificar. No entanto, a literatura existente forneceu evidências de diferentes modificações comportamentais, tanto online, por meio de autocensura e customização de comportamento, quanto off-line, por meio de gerenciamento de impressão (BUSHI, et al, 2020, p. 06), o que demonstra séria violação aos direitos da personalidade.

É importante pensar sobre potenciais externalidades da perfilização, evidenciando que essa prática vai além da privacidade e proteção de dados, mas é uma ameaça potencial à autonomia individual (BUSHI, et al, 2020, p. 12). No mesmo sentido, a autora Frazão (2019, local, 10101) afirma que a consequência disso é uma perda, não um ganho, de liberdade, já que essas práticas procuram moldar e predizer o comportamento dos indivíduos de acordo com trajetórias de oportunidades e desejos que são determinadas externamente, aumentando sobremaneira a vulnerabilidade do consumidor.

3 A posição do consumidor no capitalismo da vigilância entre o CDC e a LGPD

Mateus de Oliveira Fornasier e Norberto Milton Paiva Knebel publicaram, em 2020 o artigo intitulado "O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados", apontando que ainda que a regulação em torno da proteção de dados reconheça o problema do extrativismo de dados, ela também fornece a segurança jurídica da liberdade contratual sob a disponibilidade desses dados.

A LGPD criou a figura do "titular de dados pessoais", que, ao mesmo tempo em que é vulnerável, também é considerado capaz de fornecer seus dados pessoais comportamentais por meio de um processo de consentimento com base no princípio da autodeterminação informativa, o que se apresenta como uma contradição digna de aprofundamentos.

Nesta análise o titular de dados vai ser sempre um consumidor, mas o controlador de dados continua sendo controlador, e não fornecedor. Porque o "fornecimento" em troca dos dados não é um serviço ou produto autônomo, mas a simples "experiência do consumidor", como se visualizou nos dados coletados. O que soa mais como uma limitação da informação e da livre iniciativa e se encaixa no que aponta Zuboff (2018, p. 19) como "a transformação da cotidianidade em estratégia de comercialização". Ademais, o termo "titular de dados"

subentende a possibilidade de mercantilização por meio da renúncia ou transmissão, que devem ser lidos pela lente dos direitos da personalidade.

Analisando os objetivos de ambas as legislações. O CDC, por lógico, visa estabelecer "normas de proteção e defesa do consumidor" (art. 1º CDC), já evidenciando que o objeto de proteção é o sujeito, o consumidor. A LGPD, por sua vez, "dispõe sobre o tratamento de dados pessoais [...] com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (art. 1º LGPD). Destaco que a simples leitura nos informa o seguinte: é uma lei que estabelece regras de tratamento de dados, ou seja, regulamenta esse mercado no Brasil, que até então não tinha regulamentação específica, e visa proteger a liberdade, privacidade e desenvolvimento da personalidade da pessoa natural, ou seja, o foco não é a proteção o usuário/consumidor/titular de dados.

Ao confrontar os artigos que tratam dos "sujeitos" em proteção nas leis, o Art. 2° do CDC que estabelece quem é o **consumidor** "toda pessoa física ou jurídica **que adquire ou utiliza produto ou serviço como destinatário final"**, equiparando-se a coletividade, e Art. 5º, inciso V da LGPD que estabelece como "**titular**: pessoa natural a quem se referem **os dados pessoais que são objeto de tratamento"** (grifos meus). Importante recordar que, no CDC a relação de consumo como um todo é bastante destacada. A legislação se ocupa muito de estabelecer os limites fáticos dos fornecedores em nome do princípio da vulnerabilidade, que nos permite considerar, por natureza, uma relação de desigualdade formal entre consumidor e fornecedor, o que não acontece na LGPD.

A LGPD traz em apenas um artigo com uma série de incisos estabelecendo os agentes da cadeia, não iniciando pela definição do titular, mas pela definição do que é "dado", desde o início o objeto da lei, e não a proteção do usuário. Confronta-se em um mesmo sujeito, o usuário/consumidor/titular, e em uma mesma relação, de consumo, duas perspectivas distintas: a primeira de cunho protetivo e a segunda de cunho liberal, que permite certa flexibilização.

Importante notar que, tanto a defesa do consumidor é um dos fundamentos da lei (art. 2º), junto com a livre iniciativa e a livre concorrência, como também, o art. 45 prevê que "as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente", neste sentido, pelo

princípio da especialidade é que a análise da política de privacidade da Google prioriza a ótica consumerista.

É na comparação entre os agentes de fornecimento que é possível visualizar a complexificação da relação jurídica em questão. O CDC traz a sua definição de fornecedor (art. 3º CDC), mas a LGPD (art. 5º) define uma série de outros atores dessa cadeia, quais sejam: o controlador, o operador e o encarregado. Com base nisso e no estudo do capitalismo da vigilância, é possível inferir que as relações jurídicas que envolvem dados perpassam questões mais complexas e técnicas. Entretanto, não há o reconhecimento concreto da desigualdade ou da vulnerabilidade do consumidor, interpretação que fica a cargo da análise transversal entre a LGPD e o CDC.

No que concerne aos produtos e serviços, o CDC parte de uma definição mais genérica e ampla de produtos e serviços, enquanto a LGPD estabelece de forma mais limitadas tudo aquilo que pode ser objeto de uma relação entre titulares e controladores, não havendo, a previsão expressa de um "dado comportamental", categoria privilegiada nesta análise, se não o que prevê o art. 12, § 2º "Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para **formação do perfil comportamental** de determinada pessoa natural, se identificada".

Para a presente análise o princípio consumerista da informação se relaciona diretamente ao princípio da autodeterminação informativa (art. 2º, II, LGPD), uma vez que o consumidor só poderá escolher quais dados e de que forma disponibilizar com base em informação transparente. Neste sentido, estabelece o CDC, em seu art. 6º do CDC:

> são direitos básicos do consumidor: II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; [...] III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; [...] IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços;

Sendo que a informação tem por requisitos: que seja correta, clara, precisa, ostensiva e em língua portuguesa sobre as características, quantidade, prazo de validade entre outros, bem como sobre os **riscos que apresentam** à saúde e segurança dos consumidores (art. 31 CDC). Igualmente, o art. 37 proíbe toda publicidade enganosa ou abusiva, definindo como publicidade enganosa "§ 1° [...] qualquer modalidade de informação [...] por qualquer outro

modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços".

Também pode-se somar à análise o que preleciona o artigo 43 do CDC acerca dos bancos de consumidores: "O consumidor [...] terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes".

Considerações finais

Utilizando-se do método indutivo a presenta pesquisa objetivou o estudo do "profiling", a criação de perfis comportamentais com base nas preferências e ações dos titulares consumidores na internet. Para tanto foi realizada pesquisa documental por meio das políticas de privacidade da Google, considerando que a empresa é pioneira do *big data* e da lógica de acumulação de dados, compreendido como capitalismo da vigilância.

O capitalismo da vigilância foi teorizado pela autora estadunidense Shoshana Zuboff e é compreendido como uma nova política de relações sociais que substituem os contratos. Esta nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado por meio das técnicas de perfilização.

Na análise legislativa, compreendeu-se que a LGPD criou a figura do "titular de dados pessoais", que, ao mesmo tempo em que é vulnerável, também é considerado capaz de fornecer seus dados pessoais comportamentais por meio de um processo de consentimento com base no princípio da autodeterminação informativa. Na presente análise o titular de dados vai ser sempre um consumidor, mas o controlador de dados continua sendo controlador, e não fornecedor. Porque o "fornecimento" em troca dos dados não é um serviço ou produto autônomo, mas a simples "experiência do consumidor", como se visualizou nos dados coletados, o que soa mais como uma limitação da informação, da livre iniciativa e da autodeterminação informativa, além do aprofundamento da vulnerabilidade do consumidor.

Por meio do estudo apresentado pode-se identificar que, no que tange à apresentação das políticas de privacidade, a linguagem das políticas da Google está acessível, constando,

inclusive, imagens que facilitam a leitura. No entanto, toda a redação da política está apresentada neste sentido de bem-estar do consumidor, ocultando em grande medida a finalidade econômica da extração dos dados. Outro ponto observado é que, mesmo com a personalização de anúncios desativadas, a Google informa que os anúncios ainda podem se basear no assunto do site ou app sendo visualizado, nos termos de pesquisa atuais ou na localização geral, ou seja, não há forma de desativar totalmente a coleta desses dados.

A forma como a informação está disposta pode sim induzir o consumidor a erro por desconsiderar os impactos apresentados da perfilização e a vulnerabilidade do consumidor, cuja compreensão dos impactos da utilização dos seus dados é naturalmente limitada.

A LGPD estabeleceu os dados "utilizados para a formação de perfil comportamental" e não o termo "dados comportais" em si, entretanto, a nomeação específica, junto à compreensão sobre os riscos da perfilização faz parte do início de um processo de maior conscientização e informação sobre a categoria específica, tendo em vista que, ao pensar em "dados" o imaginário social ainda relaciona mais fortemente ao perigo de vazamentos e golpes, e não é sobre o que a proteção de tais dados, em seu complexo nível de subjetividade, trata.

Como orientação para pesquisas futuras pode-se pensar em aprofundamentos no campo da responsabilidade civil, com o aprontamento da possível dificuldade de comprovação do nexo de causalidade nas técnicas de perfilização, além do aprofundamento na questão concorrencial e na própria percepção dos consumidores acerca das políticas de privacidade.

Referências

BRASIL, LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

BRASIL, LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências.

BÜCHI, Moritz et al. The chilling effects of algorithmic profiling: Mapping the issues. Computer Law & Security Review, v. 36, p. 105367, 2020. https://doi.org/10.1016/j.clsr.2019.105367

DE ALMEIDA, Valério Catarin. PRECIFICAÇÃO BASEADA EM COOKIES E GEOLOCALIZAÇÃO: DIREITO DO CONSUMIDOR. Revista Juris UniToledo, v. 5, n. 04, 2020.

DE ÁVILA NEGRI, Sergio Marcos Carvalho; DE OLIVEIRA, Samuel Rodrigues; COSTA, Ramon Silva. O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL BASEADAS EM INTELIGÊNCIA ARTIFICIAL E O DIREITO À PROTEÇÃO DE DADOS. Direito Público, v. 17, n. 93, 2020.

DONEDA, Danilo. A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL. Espaço Jurídico. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. p. 91-108.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 1 ed. São Paulo: Thomson Reuters Brasil, 2019. Kindle ebook.

LYON, David. Cultura da vigilância: envolvimento, exposição e ética na modernidade digital. In BRUNO, Fernanda (org.). Tecnopolíticas da vigilância: perspectivas da margem. 1 ed. São Paulo: Boitempo, 2018. p. 151-180.

NETO, Mário Furlaneto; DO CARMO, Júlio César Lourenço. COOKIES: VULNERABILIDADE DO DIREITO À PRIVACIDADE NOS MEIOS DIGITAIS NO ÂMBITO DA LEGISLAÇÃO BRASILEIRA.

POLÍTICA DE PRIVACIDADE GOOGLE. Página da Web. Disponível em: https://policies.google.com/technologies?hl=pt-BR. Acesso em 28 mar. 2021.
TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. Manual de direito do consumidor: direito material e processual. Volume único. 9 ed. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2020.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. Trad. Antonio Holzmeister Oswaldo Cruz e Bruno Cardoso. In BRUNO, Fernanda (org.). Tecnopolíticas da vigilância: perspectivas da margem. 1 ed. São Paulo: Boitempo, 2018. p. 151-180.