ISSN 1982-0496

DIREITO À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS: ANÁLISE DAS PRÁTICAS OBSCURAS DE DIRECIONAMENTO DE PUBLICIDADE CONSOANTE A LEI N.º 13.709, DE 14 DE AGOSTO DE 2018

RIGHT TO PRIVACY AND DATA PROTECTION: AN ANALYSIS OF TARGETING PRACTICES ACCORDING TO LAW 13.709 OF AUGUST 14th 2018

Lia Carolina Vasconcelos Camurça

Mestra em Direito Constitucional pelo Programa de Pós-graduação em Direito pela UFC (2020). Bacharela em Direito com magna cum laude pela Universidade Federal do Ceará (UFC) em 2016. Ex-bolsista da Fundação Cearense de Apoio ao Desenvolvimento Científico e Tecnológico. Pesquisadora na área de Direito, focando seus estudos e trabalhos em Direito Civil e em Direito Comercial.

João Luís Nogueira Matias

Doutor em Direito Comercial pela Universidade de São Paulo - USP (2009). Doutor em Direito público pela Universidade Federal de Pernambuco (2003). Mestre em Direito e desenvolvimento pela Universidade Federal do Ceará (1999). MBA em gestão de empresas FGV/MARPE (2005). Professor Titular da Universidade Federal do Ceará e do Centro Universitário 7 de Setembro - UNI7.

Resumo

Este artigo tem como escopo apresentar estudos sobre o direito à privacidade relacionado com a proteção dos dados pessoais, destacando os desafios apresentados ao ambiente jurídico pela utilização de práticas obscuras de direcionamento de publicidade. Em 14 de agosto de 2018, foi promulgada a Lei n.º 13.709, também conhecida como Lei Geral de Proteção de Dados (LGPD). Realizou-se uma breve análise sobre as alterações sociais promovidas pela sociedade de informação, principalmente quanto às novas feições do direito à privacidade. Ademais, analisou-se as técnicas de monitoramento de usuários a partir de seus rastros digitais. Destacou-se, além disso, os casos mais marcantes sobre as consequências da criação de perfis comportamentais e a sua prejudicialidade aos consumidores. Dessa forma, este trabalho visa discutir tais problemáticas, aprofundando, ao final, sobre as principais inovações da nova legislação, apresentando possíveis alternativas e tecendo

DOI: 10.25192/issn.1982-0496.rdfd.v26i21590

críticas e sugestões sobre o modelo a ser estabelecido.
Palavras-chave: Direcionamento de publicidade. Privacidade. Tratamento de dados pessoais.

Abstract

This academic work brings an analysis on the function right to privacy linked to data protection laws, highlighting challenges of the legal environment by the use of obscure advertising practices. On August 14, 2018, was enacted Law No. 13,709, also known as the General Law on Data Protection. A brief analysis of the social changes was made, mainly concerning the new features of the right to privacy. In addition, were analyzed the techniques of monitoring users based on their digital traces. It was also highlighted the most striking cases about the consequences of creating behavioral profiles and their harmfulness to consumers. Thus, this essay aims to discuss such matters, deepening, at the end, the main innovations of the new legislation to present possible alternatives to the issue, weaving criticisms and suggestions about the currently used model.
Keywords: Privacy. Processing of personal data. Targeted advertising.

1. CONSIDERAÇÕES INICIAIS

A internet revolucionou a humanidade e a forma com que o homem enfrenta sua existência. Iniciou conectando pessoas, de forma a haver, na atualidade, uma economia digital que alterou profundamente as estruturas sociais. Os seres humanos estão vinte e quatro horas por dia conectados. O monitoramento digital vai desde o controle de eficácia do sono ao controle de rotas ao trabalho, incluindo nisto uma vasta quantidade de detalhes da vida privada de cada indivíduo inserido na rede.

A inteligência humana entra em convergência com a utilização das máquinas, de forma que elas correspondam às necessidades humanas, tornando a experiência cada vez mais intuitiva e a vida, cada vez mais conveniente. Foram abandonados os manuais de utilização, as coisas são quem ensinam como devem ser utilizadas. Elas, além de reagirem a comandos, também interagem com outros dispositivos, tornando a informação, em si, inteligente.

O homem e a máquina tendem, cada vez mais, a entrarem em constante simbiose. A conectividade saiu do meio digital e chegou à vida física, integrando ser humano e objeto. Em vez de homem *versus* máquina, a interação ocorre de forma homem-máquina. Com essa revolução tecnológica surgem alguns desafios principalmente quanto à privacidade e à segurança das informações.

A escolha pela privacidade máxima e restrita para si próprio pode encerrar o

indivíduo em ostracismo, eis que, para se conectar minimamente, deverá abrir mão de informações pessoais mínimas, tais como nome, documentos pessoais e endereço. Eis o preço de incluir-se na sociedade digital.

A evolução de ferramentas de publicidade também é marcante. A personalização de anúncios implica em acompanhamento dos rastros digitais dos usuários e direcionamento de publicidades mais adequadas a cada perfil de consumo. O anúncio deve ser útil e relevante, havendo um impacto sobre a forma de fazer negócios. O investimento nos serviços *on demand* faz em que conveniência se torne a palavra-chave.

A problemática se inicia mediante a existência do consentimento do usuário para a utilização dos seus rastros. Quando inexistente a transparência na coleta e na posterior utilização de dados — observado em práticas obscuras de rastreamento de usuários ou na venda dos dados coletados sem o consentimento —, um direito mínimo à privacidade resta seriamente prejudicado. Com o advento da Lei n.º 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera o Marco Civil da Internet (Lei n.º 12.965, de 23 de abril de 2014), buscou-se verificar a eficácia dos dispositivos legais ante tais práticas anteriormente mencionadas.

Na segunda seção do trabalho, imediatamente após a introdução, busca-se pautar as novas feições do direito à privacidade, relacionadas ao eixo constitucional da proteção da pessoa e os desdobramentos de seu consentimento no ambiente digital. Na terceira seção analisam-se as práticas mais comuns, e por vezes obscuras, para obtenção de dados para direcionamento de publicidade nos novos modelos de comércio eletrônico. Na quarta seção destacam-se os casos mais marcantes em que a criação de perfis comportamentais de usuários culminou em massivo prejuízo aos consumidores. Na quinta e última seção estudam-se as principais inovações da nova legislação, na perspectiva de proteção de dados pessoais dos consumidores nos direcionamentos de publicidade.

A metodologia utilizada é, principalmente, a pesquisa bibliográfica. Foi realizada a exploração de fontes bibliográficas tais como livros, teses, dissertações, monografias, artigos científicos, sites governamentais e institucionais, entre outros. As bibliotecas da Universidade Federal do Ceará foram, juntamente com pesquisas em sítios na internet, os principais acervos do trabalho.

2. NOVAS FEIÇÕES DO DIREITO À PRIVACIDADE NO AMBIENTE

DIGITAL: O PSEUDOCONSENTIMENTO PARA O TRATAMENTO DE DADOS PESSOAIS

O uso da internet se espalhou pelo mundo no final do século XX e causou grande impacto na sociedade moderna por promover, por meio de uma plataforma eletrônica, revolução na forma com que as pessoas se comunicam, trabalham, estudam, deslocam-se etc. Coisas que apenas se sonhavam possíveis vários séculos adiante, tornaram-se reais em poucas décadas e, hoje, é difícil imaginar a vida sem estar conectado. Comunicar-se só era possível através de cartas. Comprar, apenas pessoalmente. Aprender era caro. Atualmente, estas são tarefas simples, mas um tanto efêmeras. Vive-se em uma obsolescência programada: o novo se torna velho em questão de segundos.

Mark Weiser (1999, p. 01) já ditava, em 1999, que as tecnologias mais profundas eram aquelas que desapareciam no dia a dia, até se tornarem indistinguíveis da rotina. O uso de tais tecnologias indistinguíveis, no entanto, está gerando uma perda possivelmente irreparável ao ser humano: sua privacidade. A facilidade de utilização dos mais diversos aplicativos e redes sociais mediante simples cadastro pode revelar a máxima de que se o produto é de graça, você é o produto. Mais precisamente, o produto seria as preferências e as informações de cada um.

Partindo-se do eixo constitucional existente, não se trata de proteger os dados pessoais em si, mas a pessoa que está por trás deles, em seu verdadeiro direito de personalidade. O reconhecimento à privacidade trata-se de um direito fundamental, garantido pela Constituição Brasileira no art. 5º, inciso X, com consequentes deveres negativos e, sobretudo, deveres positivos por parte do Estado.

A privacidade, aspecto mais amplo que a intimidade, é um conjunto das facetas da vida de uma pessoa, possibilitando que se tenha um retrato de sua vida íntima e sua personalidade pessoal, familiar e social. O Código Civil, em seu artigo 21, estabeleceu também que “[...] a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2002) A estratificação do perfil comportamental de usuários a partir do tratamento de dados pode, ainda, ser analisada a partir de parâmetros do direito consumerista.

Analisando esses preceitos, indica-se que o conceito de dados pessoais está incluso na noção de privacidade. Há de se falar, neste contexto, no direito à

autodeterminação informativa, nascido de uma construção jurisprudencial da Corte Constitucional Alemã. Nas palavras de Ana Francisca Sanden,

> [...] O direito à autodeterminação informativa se apresenta como uma fórmula jurídica que parece não só encarnar os principais dilemas envolvendo o processamento automático da informação, como, ao mesmo tempo, foi a solução mais adequada e equilibrada que se encontrou até o momento para resolvê-los. Com efeito, ela atende, de um lado, à necessidade de fortalecer a posição do indivíduo, atribuindo-lhe o direito de ter controle sobre as informações relativas a ele. Por outro lado, ela não fecha as portas ao processamento automático da informação relativa à pessoa, permitindo, sob determinadas condições, que medre a liberdade de informação. (SANDEN, 2014, p. 90).

A autodeterminação informativa foi apresentada ao direito brasileiro em 14 de agosto de 2018, com a promulgação da Lei n.º 13.709, Lei Geral de Proteção de Dados, doravante chamada pela sigla LGPD. O art. 2º da presente legislação determina como fundamentos da disciplina da disciplina da proteção de dados pessoais, no inciso II, a autodeterminação informativa, significando que, ao se abrir mão parcialmente de sua privacidade para se inserir na era digital, deve ser resguardado o direito ao ser humano de um controle — mesmo que mínimo — de suas informações, bem como das conclusões que se retiram delas.

A partir disso, é necessária a identificação do que seriam, afinal, os dados pessoais que devem ser resguardados. Após anos de inquietações doutrinárias sobre a definição de dados pessoais no Brasil, o art. 5º da LGPD, em seus incisos I e II, define dado pessoal e dado pessoal sensível respectivamente como:

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018).

Neste contexto, por vezes, consentimos uma análise de dados pessoais sem, necessariamente, ler e concordar com os termos de uso de utilização das mais diversas plataformas digitais. Isso decorre já que não é socialmente exigível que um usuário realmente leia as infindáveis páginas destes termos, que sequer poderiam ser adequados e modificados a cada um.

Pode-se fazer um paralelo ao contrato de adesão, cujas cláusulas foram

estabelecidas unilateralmente, sem que o usuário possa discutir ou modificar substancialmente seu conteúdo. Isto é uma prática comercial abusiva, como uma condição *take it or leave it*, principalmente ao se pautar no âmbito das relações de consumo.

O tratamento de dados pessoais para a composição de um perfil comportamental de consumidores não esbarraria no direito à privacidade, desde que houvesse a utilização de alguma das bases legais estabelecidas na legislação protetiva, como é o caso da figura do consentimento do usuário. Este é definido como "[...] manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", consoante próprio art. 5º, inciso XII, da LGPD.

Além disso, como regra da legislação consumerista, há o exemplo do art. 46 do CDC, que dispõe sobre o conhecimento prévio do consumidor e a compreensão de sentido e alcance, com exceção de serviços continuados. É minimamente leal, ético e legal que se haja uma compreensão prévia, e não mero conhecimento, sobre o que se está concordando.

Com isso, não se está mais a tolerar o tratamento de dados pessoais a partir de um pseudoconsentimento do usuário, sem a sua real compreensão das implicações da análise de suas informações e sua estratificação em perfis de consumo.

3. TRATAMENTO DE DADOS PESSOAIS PARA FINS DE DIRECIONAMENTO DE PUBLICIDADE: UTILIZAÇÃO DE PRÁTICAS OCULTAS

Os dados dos mais variados indivíduos, agrupados em imenso volume de conhecimento, são conhecidos como *big data*. Este é um termo geral que abrange um grande número de operações de tratamento de dados pessoais, algumas já identificadas e outras ainda por se desenvolver (MAÑAS *et al*., 2017, p. 75). Há uma grande discussão sobre a quantificação das características do *big data*, mas em destaque geral estão os oito "vv": Volume, Valor, Veracidade, Visualização, Variedade, Velocidade, Viscosidade[1] e Viralidade.

O tratamento, portanto, é a palavra-chave. Sem este, uma imensidão de dados sem estratificação torna-se inútil para os motivos de sua coleta, principalmente se este

[1] Possibilidade de estar aderente à diversas realidades.

for o direcionamento de publicidade. A partir do tratamento, a publicidade se torna útil e totalmente relevante, com grande impacto sobre a forma de fazer negócios.

As informações se tornaram o carro-chefe da atividade empresarial. O estudo do público-alvo é imprescindível para a obtenção de sucesso nos negócios digitais. De grande relevância é a passagem de Fernando Pessoa ao citar o caso do insucesso de exportação das fábricas inglesas de taças para ovos na Índia. A forma inglesa de comer ovos em taças, estas em que o ovo entra até a metade, rapidamente chegou à Índia, à época colônia britânica. Vários ingleses que lá viviam manteriam seus modos de comer o ovo e, para isso, havia um mercado para adquirir tais taças. Supreendentemente, as exportações das casas inglesas foram batidas pelas casas exportadoras alemãs, que vendiam o mesmo produto por igual preço. Havia nisto um grande diferencial: o estudo dos clientes locais. Acontece que os ovos das galinhas indianas eram ligeiramente maiores que os das galinhas da Europa, não servindo ao seu propósito na Índia as taças produzidas para os clientes ingleses pelas casas exportadoras inglesas e, sim, as taças alemãs, ligeiramente maiores, próprias para os ovos dos consumidores locais. (PESSOA, 2006, p. 80-81).

Com vistas na atualidade, tal caso é forte exemplo de coleta e de tratamento de dados para análise da necessidade dos consumidores. No entanto, para se chegar a estas conclusões, não houve uma massiva invasão da privacidade dos clientes, como possivelmente ocorreria nos dias de hoje.

De forma a descobrir exatamente o que cada perfil consumerista quer e precisa, sem dúvida é necessário um estudo do usuário. Essas análises, por vezes, servem para melhorar a experiência de consumo, com produtos adaptados às suas necessidades. Apesar das vantagens que os anúncios se tornem cada vez mais pessoais e personalizados, as novas práticas para um melhor direcionamento de publicidade podem ser bastante obscuras.

Como exemplo está a prática do *profiling*, em que, a partir de técnicas preestabelecidas, criam-se modelos ou perfis de caráter geral por sistemas de rastreamento implementados pela indústria de publicidade online, com o fim último de direcionamento da opinião do consumidor para compra do produto A ou B.

Os sistemas de rastreamento estão espalhados por toda a *web*, coletando intermitentemente informações sobre as atividades on-line dos usuários. Em janeiro de 2016, a Universidade de Princeton realizou medição de mais de um milhão de sites

para verificar o número de terceiras partes[2] que rastreavam os usuários para coleta e categorização de seus dados.

O objetivo de grande parte desses terceiros, que funcionam como intermediadores — ou seja, não necessariamente veiculam o anúncio —, é o repasse das informações dos usuários às empresas que criarão e veicularão os anúncios. Essa é a ferramenta do *retargeting*, técnica que permite que anúncios de produtos vistos anteriormente sigam as pessoas pelos *websites*.

A forma mais conhecida para o rastreamento são os *cookies*, um pequeno pedaço de código que armazena informações úteis do usuário (idioma, carrinhos de compra, busca de produtos realizados etc.) ao seguir sua navegação, para posterior repasse. Por serem os mais conhecidos, uma grande parte dos usuários de internet sabem da possibilidade de bloqueá-los, de limitar seu uso ou de deletá-los.

Existem, ainda os *supercookies*, que não se confundem com os *cookies*. Aqueles, diferentemente destes, continuam o rastreamento mesmo após o usuário bloquear ou deletar todos os seus *cookies* (MAYER, 2011). Ou seja, eles conseguem reativar todo o conteúdo dos *cookies* deletados pelo usuário e enviar suas informações às terceiras partes. Como agravante, a consciência da maioria dos usuários sobre a sua existência é baixa.

Além desses *supercookies*, existe uma técnica ainda mais perigosa: o *fingerprinting*. Como destaca Peter Eckersley:

> Nesse meio tempo, um usuário buscando evitar ser seguido pela Web deve passar por três testes. O primeiro é complicado: deve-se encontrar configurações apropriadas que permitam que os sites utilizem os cookies para os recursos necessários da interface do usuário, mas previnam também outros tipos de rastreamento menos bem-vindos. O segundo é mais difícil: aprender sobre todos os tipos de supercookies, talvez incluindo alguns tipos bem obscuros, encontrando maneiras de desativá-los. Apenas uma pequena minoria de pessoas passará nos dois primeiros testes, mas quem fizer isto será confrontado por um terceiro desafio: a impressão digital [fingerprinting]. Como um mecanismo de rastreio para uso contra pessoas que limitam cookies, a impressão digital também tem a propriedade insidiosa de que pode ser muito mais difícil para os investigadores detectarem do que os métodos supercookie, já que ela não deixa evidência persistente de marcação no computador do usuário. (ECKERSLEY, 2010, p. 03, tradução nossa).[3]

[2] Primeiras partes são os sites que o usuário visita diretamente, enquanto as terceiras partes são rastreadores escondidos, tais como provedores de anúncios, ligados às páginas. (ENGLEHARDT; NARAYANAN, 2016, p. 02.)

[3] Texto original: "*In the mean time, a user seeking to avoid being followed around the Web must pass three tests. The first is tricky: find appropriate settings that allow sites to use cookies for necessary user interface features, but prevent other less welcome kinds of tracking. The second is harder: learn about all the kinds of supercookies, perhaps including some quite obscure types, and find ways to*

Com isso, a técnica do *fingerprinting* é em grande parte maliciosa, posto que realizada para rastrear diretamente as pessoas que, no exercício do seu direito à privacidade, limitam a ação dos *cookies*. Sem o controle e conhecimento do usuário, essas práticas parecem ser mais assustadoras do que úteis. Em verdade, demonstra-se que o *fingerprinting* não oferece nenhuma funcionalidade ao usuário, criando-se, inclusive, um potencial identificador global, em que se pode acompanhar a navegação dos usuários, para, em seguida, realizar o direcionamento de publicidade a partir dos perfis criados. (ECKERSLEY, 2010, p. 03) É uma forma de *machine learning* que pode chegar a conclusões sobre o usuário e que não necessariamente se relacionam com os dados diretamente fornecidos por ele.

Dos sete fundamentos sobre a disciplina da proteção dos dados pessoais no Brasil, dispostos na LGPD, a técnica da impressão digital viola diretamente o respeito à privacidade, à autodeterminação informativa e à inviolabilidade da intimidade, da honra e da imagem. Além disso, vai em direto encontro ao art. 7º da referida lei, que dispõe que o tratamento de dados pessoais só poderá ser realizado mediante fornecimento de consentimento do titular.

A publicidade on-line e a personalização de anúncios, em si, não são um problema. A questão está na falta transparência e nas práticas obscuras que por vezes as permeiam, indo de encontro à vida privada do usuário. É indispensável a valorização da obtenção de dados lícitos diretamente fornecidos pelo consumidor, sabendo estes das possibilidades de direcionamento de publicidade. A coleta de dados diretamente é um diferencial a se estimular, desde que esteja de acordo com o ordenamento jurídico brasileiro.

4. CONSEQUÊNCIAS DANOSAS DA UTILIZAÇÃO DE PERFIS COMPORTAMENTAIS NO DIRECIONAMENTO DE PUBLICIDADE

Apesar das inúmeras situações de vazamento de dados de usuários e sua utilização indevida, passa-se a destacar os principais casos em que, com base nos perfis comportamentais, prejudicaram seriamente os consumidores, tanto socialmente

disable them. Only a tiny minority of people will pass the first two tests, but those who do will be confronted by a third challenge: fingerprinting. As a tracking mechanism for use against people who limit cookies, fingerprinting also has the insidious property that it may be much harder for investigators to detect than supercookie methods, since it leaves no persistent evidence of tagging on the user's computer". (ECKERSLEY, 2010, p. 03).

quanto monetariamente. A criação desses perfis incide em um grande risco de discriminação de usuários em compras, como diferenciação de preços e até mesmo o vazamento de informações privadas aos familiares, entre outras situações. Passa-se, então, a analisar casos, comparando-os, ao final, com as disposições da Lei Geral de Proteção de Dados Brasileira a entrar em vigência em agosto de 2020.

Um dos casos de grande destaque foi o da a rede de varejo Target, que informou ao pai de uma adolescente que ela estava grávida antes que ele mesmo tivesse conhecimento da gravidez. O caso iniciou em uma coleta de dados de anos da empresa, que catalogava todas as compras de seus clientes por um *Guest ID* — número que identifica cada cliente, informado ao caixa no momento da compra. Com isso, eles saberiam que deveriam enviar cupons de protetor solar em julho (verão americano) para os clientes que compraram roupas de banho em abril. Além disso, saberiam que mulheres grávidas comprariam mais cremes inodoros no começo do segundo trimestre de gravidez e que mulheres de até vinte semanas comprariam muitos suplementos de cálcio, magnésio e zinco, utilizando essas informações para atraí-las paras suas lojas (DUHIGGFEB, 2012).

O problema, no caso, deu-se porque a jovem mãe ainda era adolescente, com a correspondência controlada pelo pai. Enviaram cupons de descontos de roupas de bebês e de berços, deixando o pai da moça ensandecido, culpando a companhia de estimular jovens adolescentes a engravidarem.

A empresa, tentando desculpar-se com a família, algumas semanas após o ocorrido realizou uma ligação, momento em que, na verdade, o pai da jovem se desculpou, pois a gravidez de sua filha era uma realidade.

No caso, a vida privada da jovem foi descoberta com grave violação à sua intimidade e privacidade perante a sua família, por conta de cruzamento de dados e direcionamento de publicidade. No tratamento dado pela lei brasileira, em sua seção III, o tratamento de dados pessoais de crianças e de adolescentes só poderá ser realizado com consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal, sendo explicitado que o controlador dos dados deve esforçar-se para verificar que o consentimento dado realmente partiu de seu responsável legal. O acesso de menores ao meio digital está cada vez maior e o controle dessas danosas publicidades, cada vez mais difícil.

Passando para casos brasileiros, também existem situações emblemáticas. Em 18 de abril de 2018, a ViaQuatro, concessionária da Linha 4 Amarela do metrô de

São Paulo, instalou um recurso de reconhecimento facial nas portas dos vagões. A tecnologia permitiria contabilizar quantos usuários do metrô viram as propagandas, bem como suas reações a elas (CRISTINA, 2018). O Instituto de Defesa do Consumidor (IDEC) moveu uma Ação Civil Pública contra a concessionária visando impedir a coleta massiva de dados com as portas digitais. Nos termos da petição inicial proposta:

> A conduta ilegal da Ré: (i) viola o direito básico do usuário de serviços públicos a 'proteção de suas informações pessoais, nos termos da Lei nº 12.527, de 18 de novembro de 2011' (art. 6º, IV, do Código de Defesa dos Direitos do Usuário dos Serviços Públicos); (ii) descumpre os parâmetros definidos pelo art. 10 da Lei 13.709/2018; (iii) descumpre o direito básico do consumidor de proteção contra práticas abusivas nos termos do art. 6º, IV, do CDC; (iv) consiste em prática abusiva, nos termos do art. 39, V do CDC, pois exige do consumidor vantagem manifestamente excessiva; (v) desobedece a obrigação dos fornecedores de informar aos consumidores de forma clara sobre os preços de produtos e serviços ofertados (artigos 6º e 31, do CDC); e (vi) a proibição de imposição de cumprimento de obrigações excessivamente onerosas pelos consumidores que ensejem vantagens manifestamente excessivas para os fornecedores (arts. 6º, V, 39, V, e 51, §1º, I a III); (vii) descumpre o direito constitucional de proteção de imagem (art. 5º, CF) e viola o artigo 20 do Código Civil; (viii) infringe o direito de crianças e adolescentes pela coleta de dados pessoais.

No caso, foi deferida a tutela de urgência, em 14 de setembro de 2018, objetivando o desligamento dos recursos de reconhecimento facial e a cobertura das câmeras com adesivos. Nisto, vislumbra-se a falta do dever de informação ao consumidor, que tinha seus dados biométricos captados para o estudo do desempenho do anúncio.

De acordo com a LGPD, em seu art. 5º, o reconhecimento biométrico está categorizado como dado pessoal sensível e, de acordo com seu art. 11, seu tratamento só poderá ocorrer quando houver específico consentimento, ou, na ausência de consentimento, em caso de tratamento de dados pela administração pública, realização de estudos por órgãos de pesquisa, proteção da vida do titular, entre outras situações elencadas.

Outras práticas comuns são as de *geoblocking* e de *geopricing*. Em relação ao primeiro, a partir do perfil consumerista predeterminado do usuário, ele pode ser impedido de contratar alguns serviços por estar em certa região — por exemplo, uma pessoa residente de certa cidade não encontra vagas em hotéis em sua própria localização em sites de busca, pois o consumo de tais serviços por turistas é mais lucrativo. Quanto ao segundo, analisados os perfis de compras do consumidor, os

itens anunciados podem ser mais caros ou mais baratos. Nesta situação, houve condenação pelo Departamento de Proteção e Defesa do Consumidor (DPDC) à empresa a Decolar.com ao pagamento de multa de R$ 7.500.000,00 (sete milhões e quinhentos mil reais) por diferenciação de preço de acomodações (*geopricing*) e negativa de oferta de vagas, quando existentes (*geoblocking*), de acordo com a localização geográfica do consumidor.

Também está em trâmite uma Ação Civil Pública proposta pelo Ministério Público do Estado do Rio De Janeiro, diante de inquérito civil instaurado a partir de representação da empresa Booking.com, que afirmou que sua concorrente estaria discriminando consumidores brasileiros e argentinos, sendo a prática provada por oficiais notariais de diferentes países que fizeram buscas no site da empresa Decolar.com. Quanto ao tratamento trazido na legislação brasileira, a LGPD, em seu art. 6º, inciso IX, dispõe que as atividades de tratamento de dados pessoais deverão observar a boa-fé, elencando princípios a serem seguidos, estando entre eles o da impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

O último caso a se listar, longe da exaustividade das diversas situações de abuso ocorridas, trata-se de uma investigação em andamento pelo Ministério Público do Distrito Federal e Territórios, em que a *startup* de anúncios In Loco Tecnologia da Informação teria obtido dados de geolocalização de 60 milhões de brasileiros que clicavam em seus anúncios, sem especificar qual o tratamento específico seria dado a esses dados. Entre os aplicativos que contrataram a referida empresa estão Buscapé e Turma da Galinha Pintadinha. No caso, a lei brasileira especifica, em seu art. 9º, que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva.

Cada vez mais, decisões são tomadas sobre os usuários com base em inferências e perfis comportamentais realizados por máquinas, à revelia dos dados diretamente fornecidos pelos consumidores.

5. ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS COMO FORMA DE PROTEÇÃO DOS USUÁRIOS-CONSUMIDORES DE PRÁTICAS OCULTAS DE DIRECIONAMENTO DE PUBLICIDADE

A tomada de consciência de um monitoramento intermitente dos cidadãos por

empresas ou por órgãos governamentais por meio de seus rastros digitais, a exemplo dos casos citados no tópico anterior, revela que as alterações constantes da era digital apresenta obstáculos à regulação destas pelo Direito. Ainda mais porque o problema de monitoramento pode ir além do direcionamento de publicidade, utilizando-se de mecanismos de percepção de preferências que modulariam, inclusive, o jogo político.

Já aduziu Norberto Bobbio que o direito não é um sistema de regras já postas e transmitidas, mas um conjunto de regras em movimento a serem postas e repropostas de forma contínua. O objeto da ciência jurídica deve ser não tanto as regras, ou seja, as valorações dos fatos sociais que elas consistem, e sim os próprios fatos sociais de que as regras jurídicas são valorações. (BOBBIO, 2007, p. 40).

Nisso, a ausência de uma proteção específica aos dados pessoais, a partir da transformação dos fatos sociais, reclamou a importância da promulgação da LGPD.

Há a regulação pelo Marco Civil da Internet, Lei n.º 12.965, de 23 de abril de 2014, que traz disposições gerais sobre os direitos do usuário, e pelo Decreto n.º 8.771, de 11 de maio de 2016, que regulamentou o Marco Civil em hipóteses de discriminação de pacotes de dados na internet e proteção de dados por provedores de conexão e de aplicações, entre outras medidas. Contudo, anteriormente à promulgação da Lei n.º 13.709, de 14 de agosto de 2018, o País carecia de um diploma jurídico se sistematizasse as questões relacionadas aos dados pessoais e sua utilização por terceiros.

A LGPD inspira-se na Diretiva Europeia 95/46/CE que vigorou de 1995 a 2018. A diretiva europeia foi substituída pelo Regulamento Geral sobre a Proteção de Dados 2016/679, mais conhecido no Brasil por *General Data Protection Regulation* - GDPR. Por sua vez, o modelo americano é baseado em disposições esparsas e fontes jurisprudenciais, fundando-se, principalmente, na ideia de liberdade. (ZANON, 2013, p. 75)

O conceito de consentimento é citado apenas quatro vezes nos 32 artigos do Marco Civil e nenhuma vez no decreto regulamentador. Com base nisso, a LGPD trouxe breves alterações no Marco Civil da Internet não para aperfeiçoar nele a proteção aos dados pessoais, e sim com menções à sua legislação própria.

A LGPD adotou o consentimento como uma de suas bases legais em seu art. 7º, não sendo a única base sobre a qual o tratamento de dados pode ser realizado. Apesar de não existir hierarquia entre estas, na referida lei, o consentimento é superdimensionado em relação às outras bases legais, sendo citado 35 (trinta e cinco)

vezes nos seus mais de 65 (sessenta e cinco) artigos.

Em um estudo realizado pela Universidade Carnegie Mellon, com base em usuários americanos, descobriu-se que, se todos lessem anualmente as políticas de cada site que visitam, a nação americana gastaria por volta de 54 bilhões de horas lendo políticas de privacidade. Em perspectiva, uma pessoa necessitaria de 244 horas por ano para ler as políticas, ou seja, seria exigido de cada um por volta de 40 minutos por dia. (MCDONALD; CRANOR, 2008, p. 563).

Quiçá, já que para a leitura adequada dos termos de uso demandam-se incontáveis horas, poderia haver um redimensionamento do texto para alternativas mais sintéticas, ou, até mesmo, que uma síntese das questões sensíveis à privacidade fosse destacada ao usuário, concordando ele com cada questão separadamente.

Outro ponto de destaque é sobre a possibilidade da anonimização dos dados na nova legislação, deixando de torná-los pessoais. Partindo disso, é relevante a disposição do art. 12, em que "[...] os dados anonimizados não serão considerados dados pessoais para os fins desta Lei" (BRASIL, 2018). Com isso, houve permissão legal para que os dados coletados continuem sendo utilizados de forma anônima, totalmente destacados do seu titular. Inclusive, consoante o art. 16, inciso IV, uma das possibilidades de conservação de dados após o término do tratamento é que haja uso exclusivo do controlador, desde que anonimizados os dados.

Em não sendo dados pessoais, a comercialização de dados anônimos resta autorizada em quem neles obtiver interesse. No entanto, as atuais práticas de vendas de blocos cadastros com dados pessoais ficam praticamente inviabilizadas, mas para que ocorram deve-se haver o consentimento inequívoco de todos os titulares dos dados.

O vazamento de dados pessoais ou a sua coleta por práticas ocultas foi seriamente repelido. No art. 52 estão dispostas as sanções administrativas àqueles que infringirem as normas da LGPD, variando o alcance desde uma advertência, publicização da infração, bloqueio e eliminação dos dados a que se refere a infração até, em casos extremos, multa de até R$ 50.000.000,00 (cinquenta milhões de reais). Havia sanções administrativas mais graves, como suspensão ou proibição do exercício de tratamento de dados pessoais, nos incisos VII, VIII e IX, mas foram vetadas por "[...] gerar insegurança aos responsáveis por essas informações, [...] podendo acarretar prejuízo à estabilidade do sistema financeiro nacional". (BRASIL, 2018). Ainda, a Lei n.º 13.853/2019 vetou os incisos X, XI e XII.

Quanto à responsabilidade, deve-se destacar ainda o art. 6º da legislação: “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]”. (BRASIL, 2018). Nesse caso, poderia se entender a boa-fé citada como a objetiva, já que a necessidade por uma interpretação dessa boa-fé como subjetiva pode deixar o dispositivo inócuo. Ademais, quanto à responsabilidade e ao ressarcimento de danos, traz a LGPD normas específicas em seu art. 42:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei. (BRASIL, 2018).

Uma Lei Geral de Proteção de Dados era uma necessidade de anos para o País. A presente lei possui aspectos positivos e outros aspectos que, consoante discutido nesse tópico, deverão ser esclarecidos em sua vigência.

6. CONSIDERAÇÕES FINAIS

A discussão sobre a proteção dos dados pessoais é relativamente recente no Brasil, mesmo ante algumas décadas da ocorrência da revolução informática. A partir do surgimento da sociedade de informação, “[...] tudo pode ser encontrado e cruzado nessa imensa mina de dados pessoais”. (ZANON, 2013, p. 71).

Com a sociedade confessional e exibicionista em que se vive, a privacidade está diretamente ligada à publicidade que a pessoa faz da própria vida privada nas redes sociais. Isso não significa a ausência de proteção do eixo constitucional da intimidade, da vida privada, da honra e da imagem das pessoas. Na maioria das vezes, apenas se releva a magnitude da proteção da privacidade quando esta resta violada. Ainda, por vezes, quando ocorre a sua violação, ela se dá de forma irreversível.

Nisso surge a autodeterminação informativa, regulada na nova lei como fundamento da proteção dos dados pessoais. Vincula-se à “[...] necessidade de

fortalecer a posição do indivíduo, atribuindo-lhe o direito de ter controle sobre as informações relativas a ele" (SANDEN, 2014, p. 90). A autodeterminação também se efetiva na figura do consentimento do usuário, que não mais se trata de um pseudoconsentimento do "Li e concordo". Deve haver uma compreensão inequívoca do que se está compartilhando e se haverá, ou como será, o tratamento de seus dados.

Nos novos modelos de negócios digitais, a publicidade útil e direcionada se faz essencial para o aumento de consumo de produtos e de serviços. Tornou-se necessário captar as ânsias de uma geração e convertê-las em verdadeiros objetos de desejo. As informações pessoais, assim, tornaram-se altamente relevantes para personalização da experiência. Essa personalização, contudo, resta maculada quando realizada por práticas ocultas de rastreamento do usuário, como os *supercookies* e o *fingerprinting*. Elas violam frontalmente os sete fundamentos estabelecidos sobre a disciplina da proteção dos dados pessoais no Brasil, tais como o respeito à privacidade, à autodeterminação informativa e à inviolabilidade da intimidade, da honra e da imagem.

A partir da necessidade de uma publicidade direcionada, ocorreram casos emblemáticos de violação de direitos dos consumidores, tais como o que a empresa Target informou à família de uma adolescente que ela estava grávida; o da Linha 4 Amarela do metrô de São Paulo, que captou dados sensíveis como a biometria facial de seus usuários para verificação de desempenho de anúncios; o da empresa Decolar.com, ao praticar discriminações como *geopricing*, diferença de preço com base no perfil ou localização do usuário, e *geoblocking*, ausência de ofertas de contratação de serviços para brasileiros com favorecimento de pessoas de outras nacionalidades; e o da *startup* que teria obtido dados de geolocalização de 60 milhões de brasileiros que clicavam em seus anúncios, sem especificar qual o tratamento específico que seria dado a esses dados.

A criação de uma Lei Geral de Proteção de Dados foi discutida por mais de dez anos,[4] com ampla participação social, culminando em uma legislação sistematizadora de uma matéria que, até o momento, era infimamente protegida no direito pátrio. A verificação sobre sua viabilidade para a proteção dos dados pessoais

[4] O Ministério de Justiça, em parceria com o Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas do Rio de Janeiro, discute o texto preliminar desde 2005, sendo exposto à consulta pública em 2011, tornando-se Projeto de Lei em 2016. (ZANON, 2013, p. 174)

se dará apenas com sua vigência, mas desde já se destacaram suas contribuições positivas, como a definição de dados pessoais e dados pessoais sensíveis e a responsabilização daqueles que causarem aos usuários dano patrimonial, moral, individual ou coletivo, em violação à legislação.

REFERÊNCIAS

BOBBIO, Norberto. **Da estrutura à função: novos estudos de teoria do direito**. Barueri: Manole, 2007.

BRASIL. **Código Civil, Lei 10.406, de 10 de janeiro de 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 04 dez. 2018.

BRASIL. **Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 06 dez. 2018.

BRASIL. **Constituição da República Federativa do Brasil, de 5 de outubro de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 dez. 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 dez. 2018.

BRASIL. **Mensagem nº 451, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm. Acesso em: 04 dez. 2018.

CRISTINA, Ane. Novas portas da Linha 4 Amarela contam com reconhecimento facial. **Jornal da USP**. 2018. Disponível em: <https://jornal.usp.br/atualidades/novas-portas-da-linha-4-amarela-contam-com-reconhecimento-facial/> Acesso em: 02 dez. 2018.

DUHIGGFEB, Charles. How Companies Learn Your Secrets. **The New York Times Magazin***e*, 2012. Disponível em: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp. Acesso em: 01 dez. 2018.

ECKERSLEY, Peter. How unique is your web browser?. *In*: ATALLAH, Mikhail J., HOPPER, Nicholas J. (Orgs.) **Proceedings of the 10th international conference on Privacy enhancing technologies (PETS'10).** Berlin: Springer-Verlag, 2010. Disponível em: https://panopticlick.eff.org/static/browser-uniqueness.pdf Acesso em: 24 nov. 2018.

ENGLEHARDT, Steven, NARAYANAN, Arvind. Online tracking: A 1-million-site measurement and analysis. *In*: **Proceedings of the 2016 ACM SIGSAC**

Conference on Computer and Communications Security, October 24-28, 2016, Vienna, Áustria, Doi: 10.1145/2976749.2978313. Disponível em: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf. Acesso em: 29 nov. 2018.

MAÑAS, José Luis Piñar. Derecho, tecnica e innovación em las llamadas ciudades inteligentes. Privacidad y gobierno aberto. *In*: RUARO, Regina Linden; MAÑAS, José Luis Piñar, MOLINARO, Carlos Alberto (Orgs.). **Privacidade e proteção de dados pessoais na sociedade digital.** Porto Alegre: Editora Fi, 2017. Disponível em: https://www.editorafi.org/193reginaruaro Acesso em: 27 nov. 2018.

MAYER, Jonathan. Tracking the trackers: Microsoft advertising. **CIS – The Center for Internet and Society**, 18 ago. 2011. Disponível em: https://cyberlaw.stanford.edu/comment/613 Acesso em 30 nov. 2018.

MCDONALD, A. M., CRANOR, L. F. The Cost of Reading Privacy Policies. **I/S: A Journal of Law and Policy for the Information Society**, vol. 4, no. 3 (2008), 543-568. Disponível em: http://hdl.handle.net/1811/72839 Acesso em: 03 dez. 2018.

MINISTÉRIO DA JUSTIÇA. **Despacho Nº 299/2018.** Disponível em: https://bit.ly/2Pmuvy1. Acesso em: 02 dez. 2018.

PESSOA, Fernando. **A economia em Pessoa**: verbetes contemporâneos. FRANCO, Gustavo (Org.). Rio de Janeiro: Reler, 2006.

SANDEN. Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado**. São Paulo: LTr, 2014.

WEISER, Mark. The Computer for the 21st Century. **SIGMOBILE Mob**. Rev. 3, July, 1999, p. 3-11. Doi: http://dx.doi.org/10.1145/329124.329126. Disponível em: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf Acesso em 25 nov. 2018.

ZANON, João Carlos. **Direito à proteção dos dados pessoais**. São Paulo: Editora Revista dos Tribunais, 2013.

Recebido em 20/05/2019
Aprovado em 11/11/2019
Received in 05/20/2019
Approved in 11/11/2019