

# DISCRIMINAÇÃO ALGORÍTMICA, PROFILING E GEOLOCALIZAÇÃO: UMA ANÁLISE DOS IMPACTOS JURÍDICOS DO GEO-PRICING E GEO-BLOCKING

ALGORIMIC DISCRIMINATION, PROFILING  
AND GEOLOCATION: AN ANALYSIS OF THE LEGAL  
IMPACTS OF GEO-PRICING AND GEO-BLOCKING

JOSÉ LUIZ DE MOURA FALEIROS JÚNIOR<sup>1</sup>

ARTHUR PINHEIRO BASAN<sup>2</sup>

## RESUMO

O presente trabalho visa verificar os impactos jurídicos da utilização, por empresas que exploram atividades de comércio eletrônico, das práticas de *geo-pricing* e *geo-blocking*. A partir da geolocalização do usuário, essas práticas de mercado propiciam informações diversas para potenciais consumidores que estejam em localidades mais ou menos propensas à formalização da contratação. A partir do tratamento de dados, são criados perfis (*profiling*) e, efetivamente, pratica-se discriminação baseada em algoritmos, violando os direitos dos consumidores e o princípio da neutralidade da rede. No presente estudo, será analisado o caso concreto em que o Departamento de Proteção e Defesa do Consumidor (DPDC), órgão do Ministério da Justiça, condenou a empresa “Decolar.com” ao pagamento de multa por diferenciação de preço de acomodações e negativa de oferta de vagas, de acordo com a localização geográfica do consumidor que utilizava a plataforma para a busca desses serviços. A hipótese de pesquisa está fundamentada na violação ao artigo 9º da Lei nº 12.965/2014 e aos artigos 12, §2º, 20 e 46 da Lei nº 13.709/2018, sendo de rigor a adoção de parametrizações que permitam a adequada solução de práticas discriminatórias dessa estirpe, inclusive a partir da imposição de deveres de prevenção. A pesquisa utilizará o método de abordagem indutivo, revisitando o caso da empresa “Decolar.com” para evidenciar o contexto de incidência da hipótese. Além disso, o trabalho promoverá a análise bibliográfico-doutrinária para, logo em seguida, apresentar as considerações finais.

**Palavras-chave:** *geo-pricing*; *geo-blocking*; *profiling*; neutralidade da rede; dados pessoais.

- 1 Doutorando em Direito pela Universidade de São Paulo – USP. Doutorando em Direito pela Universidade Federal de Minas Gerais – UFMG. Mestre em Direito pela Universidade Federal de Uberlândia – UFU. Especialista em Direito Processual Civil, Direito Civil e Empresarial, Direito Digital e *Compliance* pela Faculdade de Direito Prof. Damásio de Jesus. Participou de curso de extensão em direito digital da University of Chicago. Professor de cursos preparatórios para a prática advocatícia. Pesquisador do Grupo de Estudos em Direito Digital da Universidade Federal de Uberlândia –UFU. Autor de obras e artigos dedicados ao estudo do direito e às suas interações com a tecnologia. Associado do Instituto Brasileiro de Estudos em Responsabilidade Civil – IBERC. Membro Fundador do Instituto Avançado de Proteção de Dados – IAPD. Advogado. Contato eletrônico: juniorfaleiros@outlook.com ORCID <https://orcid.org/0000-0002-0192-2336>
- 2 Doutor em Direito pela Universidade do Vale do Rio dos Sinos (UNISINOS). Mestre em Direito pela Universidade Federal de Uberlândia – UFU. Associado Titular do Instituto Brasileiro de Estudos em Responsabilidade Civil – IBERC. Professor adjunto na Universidade de Rio Verde – UniRV. E-mail: arthurbasan@hotmail.com ORCID <https://orcid.org/0000-0002-0359-2625>.

### Como citar esse artigo:/How to cite this article:

FALEIROS JÚNIOR, José Luiz de Moura; BASAN, Arthur Pinheiro. Discriminação algorítmica, *profiling* e geolocalização: uma análise dos impactos jurídicos do *geo-pricing* e *geo-blocking*. *Revista Meritum*, Belo Horizonte, v. 16, n. 3, p. 302-320, 2021. DOI: ???

## ABSTRACT

*This paper aims to verify the legal impacts of the use, by companies that explore electronic commerce activities, of geo-pricing and geo-blocking techniques. Based on the user's geolocation, these market practices provide diverse information for potential consumers who are in locations more or less prone to formalizing the contract. Profiles are created based on data processing and, in effect, discrimination based on algorithms is put forth, violating consumer rights and the principle of net neutrality. In this study, we will analyze the specific case in which the Department of Consumer Protection and Defense (DPDC), an organ of the Brazilian Ministry of Justice, ordered the company "Decolar.com" to pay a fine for differentiating the price of accommodation and denying offer of vacancies, according to the geographic location of the consumer who used the platform to search for these services. The research hypothesis is based on the violation of article 9 of Law No. 12,965/2014 and articles 12, §2, 20 and 46 of Law No. 13,709/2018, showcasing the need of rigorous parameters that allow for the adequate solution of discriminatory practices of this strain, including the imposition of prevention duties. The research will use the method of inductive approach, revisiting the case of the company "Decolar.com" to evidence the context of incidence of the hypothesis. In addition, the work will promote the bibliographic-doctrinal analysis to, soon after, present the final considerations.*

**Keywords.** *geo-pricing; geo-blocking; profiling; net neutrality; personal data.*

## 1. INTRODUÇÃO

Este trabalho visa analisar as práticas denominadas *geo-pricing* e *geo-blocking*, que consistem na coleta e no tratamento de dados que indiquem a geolocalização do usuário de modo a ofertar-lhe condições de contratação diversas das usuais, ou mesmo negar-lhe acesso ao produto ou serviço desejado.

No Brasil, o Departamento de Proteção e Defesa do Consumidor (DPDC), órgão do Ministério da Justiça, condenou a empresa "Decolar.com" ao pagamento de multa por diferenciação de preço de acomodações e negativa de oferta de vagas em serviços de hotelaria, baseando-se na localização geográfica do potencial consumidor. O caso trouxe à tona grande preocupação com os impactos jurídicos do *geo-pricing* e do *geo-blocking*, instigando reflexões sobre seus limites e a necessidade de regulação específica.

Essencialmente, o problema ora investigado decorre da inegável violação ao princípio da neutralidade da rede, constante do artigo 9º da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet) (BRASIL, 2014), e aos preceitos contidos nos artigos 12, §2º, e 20 (*profiling*) e 46 e seguintes (segurança de dados), da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais) (BRASIL, 2018c). Assim, o presente trabalho busca, inicialmente, demonstrar as nuances particulares do caso envolvendo a empresa "Decolar.com", para, em seguida, investigar se o ocorrido pode servir de parâmetro para a tutela dos direitos dos consumidores no comércio eletrônico em situações análogas. E, a partir disso, partindo para análise mais ampla, o trabalho também almeja aferir a suficiência dos parâmetros regulatórios existentes no ordenamento, tendo em vista o total repúdio a tais práticas discriminatórias.

No intuito de desenvolver raciocínio mais específico sobre a imperiosidade da proteção e do combate às práticas abusivas no meio virtual, trabalhar-se-á com a hipótese de que a incidência da Lei Geral de Proteção de Dados Pessoais, em vigência desde setembro de 2020, em especial com relação aos metaparâmetros dos arts 46 a 51, será ferramenta efetiva para a prevenção de ilícitos dessa natureza. (BRASIL, 2018c)

A pesquisa utilizará o método de abordagem indutivo, revisitando o caso da empresa “Decolar.com” para evidenciar o contexto de incidência da hipótese. Ao fim, partindo para considerações finais, apresentar-se-á uma síntese conclusiva do tema.

## 2. DISCRIMINAÇÃO ALGORÍTMICA A PARTIR DA GEOLOCALIZAÇÃO: AS PRÁTICAS DENOMINADAS *GEO-PRICING* E *GEO-BLOCKING*

O rastreamento georreferencial pode ser realizado de várias formas, tais como: (a) a primeira é através dos dados da rede móvel de equipamento diretamente conectado a um provedor de conexão (*Internet Service Provider*, ou ISP), sem acurácia suficiente (a precisão é de cinquenta metros ou mais) para que se tenha a certeza de que houve interação entre duas pessoas; (b) a segunda funciona através de aplicativos instalados no dispositivo, que acessam, de forma mais precisa, dados de localização e interação, via *Bluetooth* ou *Wi-Fi*, por exemplo, de modo que tais aplicativos possam, diretamente, ter a função de rastreamento e alerta sobre interações especificamente mapeadas, ou estar vinculados a outros aplicativos que o usuário já tenha no seu celular (ISRAVEL; SILAS; RAJSINGH, 2020, p. 6-13); (c) a partir da coleta do número IP (*Internet Protocol*) e de outros dados de navegação (*cookies*), que permitam o processamento algorítmico das interações recentes do usuário para viabilizar a estruturação de seu ‘perfil’<sup>3</sup>.

A utilização de redes móveis para o rastreamento georreferencial não permite, isoladamente, saber se duas pessoas apontadas como estando no mesmo prédio, de fato, estão numa mesma sala ou não, pois podem estar em andares diferentes. Em simples termos, a localização via *app* possibilita uma análise muito mais realista e eficiente, apontando se duas pessoas realmente estiveram no mesmo ambiente de um edifício e por quanto tempo, com exatidão. Por esse motivo, o rastreamento que usualmente se faz é baseado em grandes acervos de dados coletados do usuário<sup>4</sup>, no modelo tradicionalmente descrito pela doutrina como *profiling* (ou perfilização, em tradução para o português). (ZANATTA, 2019)

Na Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, dispositivo bastante tímido, inserido em um único parágrafo do artigo que cuida da anonimização de dados (artigo 12, §2º), conceitua a referida prática: “Poderão ser igualmente considerados como dados

3 Conferir, sobre o tema, a análise de Steven Englehardt e Arvind Narayanan de cerca de 1 milhão de sítios virtuais e suas práticas relacionadas à coleta de *cookies* de navegação dos usuários: ENGLEHARDT; NARAYANAN, 2016.

4 A tecnologia HTML5 propicia vantagens específicas para o atingimento desse tipo de mapeamento, como informa Anthony Holdener III (2011, p. 79): “There is no doubt that geolocation will continue to grow for years to come—just look at the ever-increasing trends among the popular location-based services for mobile phones to see why. While Foursquare, Gowalla, Twitter, Glympe, and all the rest continue impressive growth (and will continue to do so for quite some time), the W3C Geolocation API will also continue to open ever more doors for native browser applications in this market. Consider some of the following: • Geolocation applications have gone from niche and novelty pieces of software to cultural and trendy “must-haves” in today’s mobile world. • Phones are becoming increasingly “smart,” with more and more people switching from basic cell phones to smart devices, and the smartphone market is growing around the world and tapping into new markets. • More smartphones equals more GPS-enabled devices to utilize geolocation technology. • Companies now recognize the huge earnings potential with advertising on the popular location-based services, particularly as advertisements can be directed to individuals and specific locals. • HTML5 and the W3C Geolocation API will allow for websites to add geolocation to their functionality, removing the native application-only nature geolocation software shared in the past.”

peçoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.” (BRASIL, 2018c) Trata-se, basicamente, da coleta do maior número possível de informações que possam ser processadas para a produção de uma decisão automatizada que categorize as preferências do usuário<sup>5</sup>.

O artigo 20 da LGPD prevê o direito à revisão das decisões automatizadas. Na redação original da lei, essa revisão deveria ser realizada por um humano (pessoa natural), mas veto presidencial culminou em reforma posterior, levada a efeito pela Medida Provisória nº 869/2018, posteriormente convertida na Lei nº 13.853/2019, que retirou essa exigência específica. (BRASIL, 2019) Basicamente, pode-se dizer que decisões automatizadas são aquelas realizadas exclusivamente por algoritmos.

Já se caminha, entretanto, para um ambiente no qual a ruptura das limitações técnicas de máquinas, que trabalham com base puramente nas estruturas matemáticas da predição estatística e da análise combinatória, permitirá avanços formidáveis.

Em tempos nos quais tanto se questiona a discriminação algorítmica tão bem suscitada por O’Neil (2016), sempre pareceu uma realidade distante e distópica imaginar que abusos poderiam ser cometidos com absoluta precisão, maculando a proteção almejada às relações de consumo.

Entretanto, em junho de 2018, divulgou-se a condeção da empresa “Decolar.com” por violação a direitos de seus consumidores. O caso teve início com a instauração de inquérito civil, pela 5ª Promotoria de Justiça de Tutela Coletiva de Defesa do Consumidor e do Contribuinte da Capital, do Ministério Público do Estado do Rio de Janeiro. (RIBEIRO, 2018)<sup>6</sup>

Logo que o caso veio a público, em decisão inédita no Brasil, o Departamento de Proteção e Defesa do Consumidor (DPDC) condenou a fornecedora supracitada, na esfera administrativa, ao pagamento de multa no valor de R\$ 7.500.000,00 (sete milhões e quinhentos mil reais) por diferenciação de preço de acomodações e negativa de oferta de vagas em hotéis, quando existentes, de acordo com a localização geográfica do consumidor.<sup>7</sup> O caso envolvia a utilização das técnicas conhecidas como *geo-pricing* e *geo-blocking*, respectivamente.

Desse modo, logo após a supracitada condenação, a notícia foi amplamente divulgada pelos meios de comunicação, forçando a empresa a se pronunciar publicamente. Em nota, defendeu-se alegando que opera em cada país por meio de *sites* locais e que estes não fazem

5 Comenta a doutrina: “Algorithmic predictions about health risks, based on information that individuals share with mobile apps about their caloric intake, may soon result in higher insurance premiums.’ Sites soliciting feedback on ‘bad drivers’ may aggregate the information, and could possibly share it with insurance companies who score the risk potential of insured individuals. The scoring trend is often touted as good news. Advocates applaud the removal of human beings and their flaws from the assessment process. Automated systems are claimed to rate all individuals in the same way, thus averting discrimination. But this account is misleading.” (CITRON; PASQUALE, 2014, p. 4)

6 Nos dizeres de Pedro Fortes e Guilherme Martins, “o algoritmo estrutura as informações do problema a ser resolvido com base em instruções (aspecto estático) e possíveis execuções (aspecto dinâmico). Ao longo das últimas décadas, a revolução da tecnologia da informação tem sido pautada pelo desenvolvimento de inúmeros modelos de algoritmos – simbolistas, conectados, evolucionários, bayesianos e analógicos – e de variados desenhos adaptados para diferentes funcionalidades – interrupção ótima (*optimal stopping*), explorar/aproveitar (*explore/exploit*) e classificação (*sorting*), dentre outras. Todavia, nem só de progresso é feita a experiência do desenvolvimento tecnológico e do comércio eletrônico, existindo um lado obscuro que reduz a própria autonomia individual, a liberdade do consumidor e a igualdade de condições de compra em uma experiência de consumo.” (FORTES; MARTINS, 2019, p. 237)

7 Consta da decisão o seguinte: “[A empresa foi] sancionada por conta da prática aqui apontada, qual seja, a diferenciação de preço de acomodações e negativa de oferta de vagas, quando existentes, de acordo com a localização geográfica do consumidor, sendo considerada uma prática abusiva e discriminatória, a empresa deve cessar imediatamente a prática, sob pena de suspensão da atividade, bem como a retirada do site do ar [...]” (BRASIL, 2018b)

nenhuma discriminação de preços com relação a consumidores nacionais ou estrangeiros. (VENTURA, 2018; MIOZZO, 2018)

Em relação aos preços desiguais evidenciados por usuários distintos, a empresa alegou que foram comparados mercados diferentes (no caso, da Argentina e do Brasil), sujeitos a legislações e regulamentos também diversos. (RIBEIRO, 2018) A fornecedora ainda alegou que atua como mera intermediadora entre os fornecedores e consumidores no que diz respeito à hospedagem, sendo esses fornecedores os reais responsáveis pela inclusão dos preços e disponibilidade de acomodações, insistindo, portanto, que não pratica o denominado *geo-pricing*.

No relatório que acompanha a decisão que impôs sanção administrativa à “Decolar.com”, o Departamento de Proteção e Defesa do Consumidor (DPDC) considerou que, ao precificar (ou mesmo permitir que se precifique) o serviço de acomodação de acordo com a localização geográfica do consumidor, a fornecedora viola as práticas legais do mercado.

Noutros termos, de acordo com o relatório, nada justificaria a apresentação de preços diferentes para serviços que são prestados no mesmo local e nas mesmas condições. Em verdade, nesta situação, qualquer consumidor que esteja disposto a pagar por esses serviços deveria ser cobrado na mesma quantia. Embora o Código de Defesa do Consumidor não tenha regras específicas relacionadas às práticas de *geo-pricing* e *geo-blocking*, é constituído de cláusulas gerais e princípios abrangentes que possibilitam a averiguação da ilicitude de tais condutas. (MORASSUTTI, 2019, p. 216-219)

Ainda assim, no que se refere à não exibição da disponibilidade total de acomodações, a infração à ordem jurídica, conforme destacado na decisão administrativa, é ainda mais evidente. (MARTINS, 2019, p. 635-647) Segundo consta, a empresa não ofertava o serviço que não queria vender a determinado consumidor – no caso, um consumidor brasileiro –, enquanto o oferecia a outro – um consumidor argentino. Concluiu-se que o favorecimento (ou desfavorecimento), bem como a discriminação em razão da localização geográfica, ou devido a qualquer outra característica extrínseca ao ato comercial, causa desequilíbrio no mercado e nas relações de consumo, violando o sistema jurídico pátrio. (BRASIL, 2018a) O caso da “Decolar.com” representa um dos maiores temores no que se refere à utilização indevida de dados pessoais, especialmente para fins de discriminação de consumidores a partir de implementos algorítmicos desprovidos do devido consentimento esclarecido e prévio.

E mais: é violação que fere frontalmente o princípio da neutralidade da rede, pois, a partir de algoritmos sofisticados, o usuário-internauta é exposto a estruturas informacionais que podem adaptar os termos contratuais para melhorar ou piorar as condições apresentadas, maculando a transparência da transação. (ABERNATHY, 2017)

O que ocorre é verdadeira reconfiguração dos elementos que conduzem à formalização do contrato, pois ocorre verdadeira manipulação na apresentação do contrato eletrônico de consumo. Ocorre a ‘quebra’ do dever de informação, corolário do princípio da transparência<sup>8</sup> e da boa-fé objetiva. Pratica-se, ao fim e ao cabo, violação fatal ao princípio da neutralidade da rede (art. 9º do Marco Civil da Internet<sup>9</sup>), que impõe justamente a não-discriminação. (PAREN-

8 Sobre o tema, confira-se: BARROS, 2017, v. 5, p. 509-512.

9 “Art. 9º. O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.”

TONI, 2017, p. 195-243; BELLI, 2016, p. 11-12) A partir desse importantíssimo princípio, tem-se por completamente abusiva e descabida qualquer iniciativa voltada ao desvirtuamento da relação de lisura que deve preponderar entre as partes.

### 3. O CÓDIGO DE DEFESA DO CONSUMIDOR E A VEDAÇÃO ÀS PRÁTICAS DISCRIMINATÓRIAS

Não há dúvidas de que, “se o fenômeno informático é recente, a problemática dos direitos fundamentais é pensada há muito tempo” (LIMBERGER, 2007, p. 197) e, com o advento da Constituição da República de 1988, todo o sistema jurídico brasileiro foi submetido a uma verdadeira reformulação, visando à atribuição de coerência ao modelo de Estado democrático estabelecido. Adotou-se a defesa do consumidor como princípio fundamental, consagrando passo essencial para a consolidação do chamado “direito privado solidário”. (BENJAMIN; MARQUES; BESSA, 2016, p. 27)

Um universo de dados, *Big Data*<sup>10</sup>, tem sido a motivação da pujante busca por algoritmos sofisticados, cada vez mais detalhistas e capazes de processar grandes volumes informacionais.<sup>11</sup> Em verdade, analisando a lógica do mercado, que opera pela busca de lucro, a proteção do consumidor se apresenta como forma de superar as falhas estruturais que expõem pessoas a potenciais danos. (SANDEL, 2012, p. 11) Dito de outro modo, é a lei que exerce a função de ordenar o mercado visando à proteção das pessoas das práticas comerciais abusivas, garantindo o cumprimento efetivo do fundamento de tutela da pessoa humana, expresso na carta constitucional, e que gera efeitos sobre as relações privadas em razão de sua eficácia horizontal. (DUQUE, 2013, p. 50)

O Código de Defesa do Consumidor ocupa o vértice desse ecossistema. Não por outra razão, logo em seu artigo inaugural, estebelece que sua finalidade é a proteção e defesa do consumidor, matéria de ordem pública e interesse social, ressaltada em razão do que prevê o artigo 170, inciso V, da Constituição da República.

Tal dispositivo impõe ao legislador infraconstitucional a defesa do consumidor como princípio geral da atividade econômica, mas que também cumpre função promocional dos direitos humanos. (SARLET, 2010, p. 79) Noutras palavras, no sistema jurídico brasileiro, só se admite a prática comercial e financeira que, além de outros princípios, respeite a dignidade da pessoa humana. Esta, em seu sentido mais amplo, congloba os direitos dos consumidores.

Significa dizer que a norma constitucional procura compatibilizar a livre iniciativa com a tutela das pessoas vulneráveis expostas às práticas do mercado, utilizando, dentre outras fontes, o CDC para a instrumentalização dessa tutela. (GARCIA, 2019, p. 25) Nesse sentido, conforme exposto, o artigo 1º do CDC prevê o interesse social de suas disposições, ou seja,

10 Em simples termos, eis o conceito: “Big Data is all about seeing and understanding the relations within and among pieces of information that, until very recently, we struggled to fully grasp.” (MAYER-SCHÖNBERGER; CUKIER, 2014, p. 19)

11 Comentando essa tendência: “Today, we can still think of information as the intangible enabler of communications, media, and software. But as technology advances in this century, our present intuition about the nature of information will be remembered as narrow and shortsighted. We can think of information narrowly only because sectors like manufacturing, energy, health care, and transportation aren’t yet particularly automated or ‘net-centric.’” (LANIER, 2013, p. 22)

trata-se de legislação que ultrapassa a relação entre as partes (consumidor/fornecedor), pois também deve ser interpretado no interesse de toda a sociedade, de modo que o fornecedor que age contrariando suas disposições não apenas viola o direito do consumidor diretamente envolvido no caso, como também prejudica a livre concorrência e, em última análise, pode colocar terceiros em situação de vilipêndio.<sup>12</sup>

Como ‘coluna vertebral’ da Política Nacional das Relações de Consumo, o artigo 4º do CDC prevê os princípios de regência das relações consumeristas no intuito de cumprir essa função social supracitada. (GRAU, 1993, p. 166) O inciso I expressamente reconhece a vulnerabilidade do consumidor no mercado de consumo, razão pela qual se tem um microsistema norteado por um ‘código’, ao invés de simplesmente ‘lei’ (DE LUCCA, 1995, p. 35-36), que exerce função protetiva, buscando, por meio de seus instrumentos, promover o equilíbrio contratual a partir de soluções justas e harmônicas.

Diante do exposto, para os fins do presente trabalho, é importante destacar a previsão do artigo 6º, inciso II, no qual consta como direito básico do consumidor a divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações.<sup>13</sup> Significa dizer que, se determinado produto ou serviço é oferecido ao mercado, deve sê-lo a todo consumidor potencialmente interessado em adquiri-lo, sem discriminações de qualquer tipo, desde que esteja disposto a pagar o preço.

A própria norma consumerista somente permite a recusa nos casos excepcionais<sup>14</sup> de intermediação regulados em leis especiais, como no caso de uma farmácia que nega a venda de um medicamento sem a apresentação da necessária prescrição médica. E tal proibição de discriminação é de tamanha importância jurídica que a recusa de venda de bens e produtos oferecidos no mercado configura crime contra as relações de consumo (art. 7º, I e IV, da Lei 8.137/90) (BRASIL, 1990b)

Privilegia-se a liberdade de escolha e a igualdade nas contratações, que devem ser respeitadas nas relações jurídicas de consumo, visando, evidentemente, consagrar uma sociedade plural e igualitária no que se refere ao exercício de direitos no mercado de consumo, com amplo respeito à transparência. (KREZMANN, 2019) E, no que diz respeito à Internet, tem-se um novo ambiente, no qual novas modalidades de proteção normativa impõem o reconhecimento de proteção adequada às contratações que, nesse novo ambiente, são levadas a efeito.

12 Para ilustrar, destaca-se o consumidor por equiparação, vítima do evento, previsto no art. 17 do CDC. Neste caso, a pessoa protegida pelo código sequer possui relação jurídica com o fornecedor, sendo, mesmo assim, protegida pela lei. É o exemplo do celular defeituoso que explode e atinge pessoas que estavam próximas ao aparelho.

13 Como se nota, visando evitar qualquer tipo de discriminação e como cumprimento dos objetivos fundamentais da Constituição, em especial o de promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação, o CDC consagrou como direitos básicos do consumidor a liberdade de escolha e a igualdade na aquisição de bens e serviços. Nesse sentido, vale lembrar, inclusive, o artigo 2º da Declaração Universal de Direitos Humanos: “Não será também feita nenhuma distinção fundada na condição política, jurídica ou internacional do país ou território a que pertença uma pessoa, quer se trate de um território independente, sob tutela, sem governo próprio, quer sujeito a qualquer outra limitação de soberania. (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948)

14 Em razão disso, a lei proíbe que o fornecedor faça distinção de valores ou que realize ofertas contendo qualquer forma de discriminação, conforme expressamente prevê o CDC: “Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: (...) II - recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes; (...) IX - recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais.”

(MARQUES, 2004, p. 94) Os consumidores são praticamente ‘de vidro’/‘transparentes’, como sugere Susanne Lacey<sup>15</sup>, tamanha a exposição a que estão submetidos no e-commerce.

Em que pese o CDC não tenha regras específicas para a tutela de práticas como as mal-fadadas discriminações georreferenciais (*geo-pricing* e *geo-blocking*), seu arcabouço principiológico é constituído por cláusulas gerais e princípios abrangentes que possibilitam a averiguação da ilicitude de tais condutas no mundo fático. Com efeito, tais fenômenos exigem maior atenção e cuidado do sistema jurídico visando à concretização dos direitos dos ciberconsumidores<sup>16</sup>, que se tornaram mais frágeis ao serem expostos à sociedade informatizada.

#### 4. O PROFILING COMPREENDIDO A PARTIR DO DIÁLOGO DE FONTES ENTRE O CDC, O MCI E A LGPD

A utilização indiscriminada de algoritmos de Inteligência Artificial faz surgir uma necessidade premente de revisitação dos valores que norteiam o desenvolvimento tecnológico no século XXI. A doutrina sinaliza a necessidade de atuação proativa quanto ao estabelecimento de parâmetros éticos para algoritmos.<sup>17</sup> Como arrematam Eduardo Tomasevicius Filho e Angelo Viglianisi Ferraro (2020, p. 412), “chegou o momento de o problema da Inteligência Artificial ser seriamente abordado no nível político-regulatório”<sup>18</sup>. E, de fato, os impactos sobre direitos atinentes à privacidade, à liberdade e à autonomia, por exemplo, foram relativizados diante do poder de comunicação, de coleta e de processamento de dados proporcionado pelas tecnologias virtuais.

Nesse contexto, segundo Jorge Pereira da Silva (2015, p. 354):

O desiderato a se atingir é o de que o poder de intervenção estatal e a liberdade dos cidadãos se equilibrem de modo a garantir ao indivíduo tanta protecção quanto a necessária, mas também tanta liberdade pessoal quanto seja possível. Por isso, segundo a denominada concepção pessoal do bem jurídico, tem-se entendido que integram este conceito aquelas “realidades ou fins que são necessários para uma vida social livre e segura, que garantam os direitos humanos e fundamentais do indivíduo, assim como para o funcionamento do sistema estatal erigido para a consecução de tal objectivo. Não que, com esta referência, se pretenda induzir à importação acrítica para o

15 A autora apresenta os principais riscos disso: “The following five points summarize risks discussed throughout this book: *Injustice* – this includes using inaccurate or out-of-date information, making unjust inferences, function creep (when information is used for a different purpose from that for which it was collected) and the reversal of the presumption of innocence. *Lack of control of information* – such as the inability to find out what is held or where data are collected from, unjustified surveillance and data collected without consent. *Loss of dignity and autonomy* – this may result from the absence of transparency, the absence of anonymity or unjustified disclosure. *Inconvenience* – such as making a substantial effort to find out what information has been collected, how it has been used or to secure the correction of data. *Risks to life chances* – as the private sector concentrates on people and areas that present the best risks.” (LACE, 2005, p. 211)

16 A despeito da multiplicidade de nomenclaturas, é fato que grande parte dos usuários da Internet está exposta à publicidade irrefreável, que dá origem à figura do ‘turboconsumidor’ descrito por Gilles Lipovetsky e Jean Serroy, na exata medida em que “o universo do consumo vê dissolver-se as antigas culturas de classe que enquadravam os comportamentos dos diferentes meios sociais por pressões e outras intimidações”. (LIPOVETSKY; SERROY, 2011, p. 57)

17 Com efeito: “Perhaps unsurprisingly, AI ethics policy faces numerous challenges. We have seen that some policy proposals endorse a vision of AI ethics that is *proactive*: we need to take ethics into account at the early stage of development of AI technology.” (COECKELBERGH, 2020, p. 167)

18 No original: “Sono maturi i tempi perché il problema dell’Intelligenza artificiale venga affrontato seriamente a livello politico-normativo.”

direito constitucional dos resultados (nem sempre pacíficos) atingidos pela doutrina penalista sobre a teoria do bem jurídico – até porque a protecção penal é apenas uma modalidade, entre várias outras, de protecção de direitos fundamentais –, mas é importante reconhecer que a multifuncionalidade dos direitos fundamentais implica uma atenção redobrada ao conceito de bem jusfundamental e a sua colocação no centro do processo construtivo dos *conglomerados jurídicos* usualmente designados por direitos fundamentais.

A Inteligência Artificial afeta exatamente esse contexto, pois distorce os tradicionais *standards* de protecção historicamente construídos. (GREENE; PARK; COLARESI, 2019) Altera-se, essencialmente, a própria acepção que se tem do que é considerado “humano”. (COLEMAN, 2019) Tudo se reduz à matemática, à heurística, à predição e ao mapeamento dos interesses como condicionantes funcionais de estruturas de mercado, pois não se atingiu a já descrita singularidade tecnológica. As máquinas não são capazes de agir ou tomar decisões imbuídas de concepções morais.

Em verdade, o uso da tecnologia (cada vez mais consideradas em perspectiva nanotecnológica<sup>19</sup>) abre novas dimensões para a exploração de práticas abusivas; porém, os dispositivos do Código de Defesa do Consumidor já são capazes de tutelá-las, ainda que se trate de uma lei datada de 1990. (BRASIL, 1990a) Significa que “a Internet configura um novo meio, permitindo a conexão de pessoas nas mais diversas situações, com os mais diversos propósitos.

A inter-relação é de tal modo facilitada que se costuma falar em desterritorialização das relações celebradas por meio eletrônico. (KLEE, 2014, p. 227) Noutros dizeres, a protecção do consumidor poderá ser dividida em “antes/depois” da aparição do comércio eletrônico, tornando necessárias novas soluções para esses novos problemas que surgem. (LORENZETTI, 2004, p. 354; RODOTÀ, 2008, p. 59)

No Brasil, o que guiou a promulgação da Lei Geral de Protecção de Dados Pessoais foi justamente esse “núcleo duro” de parâmetros extraídos de uma compreensão mais ampla do direito à privacidade<sup>20</sup>, previstos no texto legal como fundamentos, em seu artigo 2º, e que atuam como vetores axiológicos para os direitos (e deveres) descritos noutras passagens da lei e, também, para a atuação posterior do Estado, no exercício de seu poder regulatório. Destaca-se a redação do inciso VII do artigo 2º da LGPD: “A disciplina da protecção de dados pessoais tem como fundamentos: (...) VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.” (BRASIL, 2018c)

Embora a vigência da LGPD seja recente (desde setembro de 2020), é possível afirmar que já existe, no Brasil, um arcabouço principiológico reconhecido e aprovado pelo legislador e que está em plena harmonia com outros textos legais vigentes, que formam um microsistema de protecção ao titular de dados. Nesse âmbito, podem ser citados, dentre outros, o Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei de Acesso à Informação, além da Constituição da República.<sup>21</sup> Além disso, em maio de 2020, o Supremo Tribunal Federal reconheceu o direito fundamental à autodeterminação informativa (e a corolária protecção

19 Sobre o tema, ver, por todos, Borges e Martins (2017, p. 417-438).

20 Sobre o tema, anota a doutrina: “The right to privacy functions as a ‘window’ to the constitutional rights, which protects the private and personal sphere of an individual, e.g., dignity, free development of personality, religious freedom, privacy and data protection.” (TRSTENJAK, 2016, p. 48)

21 Bruno Miragem (2019, p 174) aponta que há na LGPD a “adoção expressa da interpretação sistemática segundo a técnica do diálogo das fontes, ademais desenvolvida no próprio direito do consumidor”.

de dados pessoais) ao suspender a Medida Provisória n.º 954, que determinava o compartilhamento dos dados pessoais dos usuários de telefonia pelas empresas telefônicas ao IBGE.<sup>22</sup>

O tema é de tamanha relevância que, além desta sinalização da Excelsa Corte, também a doutrina já sinaliza a consagração da proteção de dados pessoais como direito fundamental. (DONEDA, 2020) Ainda que reconhecido como direito implícito, o tema já provocou movimentações no Legislativo, uma vez que tramita perante o Congresso Nacional a Proposta de Emenda à Constituição 17/2019, que visa incluí-lo entre os direitos e garantias fundamentais do cidadão, inserindo o inciso XII-A ao rol do artigo 5º da Constituição.

A PEC ainda define como de competência exclusiva da União o poder para legislar sobre o assunto. Entretanto, por todo o exposto, é de fácil constatação que esse mencionado direito já existe, ainda que implicitamente, e é protegido pelo ordenamento.

É importante deixar claro que os dados de localização geográfica da população podem ser considerados dados sensíveis<sup>23</sup> se, analisados em conjunto com outros dados, for possível identificar outros elementos. (KONDER, 2019, p. 455)

É neste contexto que se enquadram as práticas abusivas exercidas no mercado, como aquelas denominadas de *geo-blocking* e *geo-pricing*. A primeira é evidenciada pela manipulação da disponibilidade das ofertas. Em simples termos, a empresa promove o bloqueio de uma oferta a determinado grupo de consumidores, enquanto a disponibiliza para outros em razão da sua localização de conexão. Tal prática é viabilizada pelo uso da tecnologia na coleta (muitas vezes realizada por singles *clicks*) e interpretação dos dados, os quais permitem, por sua vez, a identificação da posição geográfica do consumidor/usuário.

Na segunda prática, denominada *geo-pricing*, o fornecedor, levando em consideração novamente a posição geográfica do consumidor, permitida também pela interpretação dos dados coletados, promove a diferenciação de preços. Dito de outro modo, por meio do *geo-pricing* a empresa pode apresentar, para o mesmo produto ou serviço, diversos preços, condicionando o valor à localização em que se encontra o usuário.

Desse modo, através do *geo-blocking* e do *geo-pricing*, os fornecedores podem praticar total ou parcialmente a recusa à venda de bens ou à prestação de serviços, indicando tal discriminação a determinado grupo de consumidores geograficamente posicionados. Isto coloca em perspectiva o real valor da proteção de dados (WINEGAR; SUNSTEIN, 2019, p. 3-5), propiciando uma nova compreensão dos impactos que um mercado rico em dados (*data-rich market*)<sup>24</sup> pode vir a ter sobre a própria estrutura econômica de um país. Tais medidas, naturalmente, configuram práticas abusivas, vedadas pelo CDC na esteira da dicção do artigo 39 do diploma.<sup>25</sup>

22 STF. ADIs n.º 6.387, 6.388, 6.389, 6.390 e 6.393. Relatora: Min. Rosa Weber. Julgado em 7 de maio de 2020.

23 “Art. 5º Para os fins desta Lei, considera-se: 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.”

24 Segundo a doutrina, “[t]he key difference between conventional markets and data-rich ones is the role of information flowing through them, and how it gets translated into decisions. In data-rich markets we no longer have to condense our preferences into price and can abandon the oversimplification that was necessary because of communicative and cognitive limits. This makes it possible to pair decentralized decision-making, with its valuable qualities of robustness and resilience, with much-improved transactional efficiency.” (MAYER-SCHÖNBERGER; RAMGE, 2018, p. 7)

25 No contexto do citado dispositivo do CDC, prevalece o entendimento de que “essas práticas abusivas levadas a efeito por fornecedores de produtos e serviços ao redor do mundo partem da discriminação entre consumidores em razão de sua

Como já se anotou, o consumidor é exposto a um algoritmo complexo, que é capaz de adaptar os termos contratuais para melhorar ou piorar as condições apresentadas, maculando a transparência da transação. (VAN OOIJEN; VRABEC) O potencial de discriminação de preços, nesses casos, depende de variáveis dinâmicas e dos substratos valorados (com maior ou menor ‘peso’) nos algoritmos que operacionalizam a mineração de *cookies* e o processamento de dados do consumidor. Antes mesmo da ocorrência da discriminação, outra grande ilicitude dessas práticas consiste no tramento oculto, porquanto não informado, não consentido e não lastreado noutra base legal, dos dados do consumidor para a prática do *geo-pricing* ou do *geo-blocking*. (DIAS; NOGUEIRA; QUIRINO, 2019, p. 76) Em observância ao direito básico do consumidor à informação, a empresa precisaria informar qual(is) tipo(s) de dado(s) estaria(m) sendo tratado(s) durante a navegação, visando ao cumprimento do dever de transparência.

Por meio do *profiling*, leciona Danilo Doneda, empresas que possuem muitos dados os tratam com técnicas que se dedicam a obter “uma ‘metainformação’, que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa”, sendo que “o resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo”. (DONEDA, 2019, p. 151)

O §2º do artigo 12 da LGPD trata dessa prática, estabelecendo que “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”. Trata-se de dispositivo tímido, mas especificamente dedicado à regulação de um tema ainda peculiar e muito desafiador no que concerne à vigilância de dados (*dataveillance*<sup>26</sup>).

Apesar de o dispositivo acima se referir à pessoa natural “se identificada”, Bruno Bioni está correto ao defender que o foco da Lei está nas consequências que determinado tratamento de dados pode ter sobre uma pessoa, e, por tal razão, dados anonimizados podem ser considerados como dados pessoais quando formam perfis comportamentais. (BIONI, 2020, p. 78-81)

A doutrina destaca que o processo de perfilização envolve, pelo menos, as etapas de (a) registro dos dados, (b) agregação e monitoramento de dados, (c) identificação de padrões nos dados, (d) interpretação de resultados, (e) monitoramento dos dados para checar resultados e (f) aplicação de perfis. (ZANATTA, 2019, p. 6) Desse modo, é certo que o cerne da discussão quanto ao uso da localização geográfica pelos fornecedores está baseado em uma aferição da razoabilidade da diferenciação. Com efeito, destaca-se a possibilidade de os dados pessoais localizadores justificarem o tratamento distinto, de maneira legalmente tolerada. Se a diferenciação dos valores ocorrer, por exemplo, em razão do frete, não há que se falar em geodiscriminação e, conseqüentemente, não se configura nenhuma prática abusiva. Todavia, quando a geodiscriminação é utilizada no intuito de maximizar lucros, sem a devida ‘justa

---

origem (geodiscriminação), e acabam por gerar limitação ao livre trânsito de pessoas, com repercussão em outros direitos e garantias fundamentais, como o direito ao lazer e à cultura, sem falar do fortalecimento de preconceitos como resultado indireto, já que o convívio com diferentes indivíduos, grupos e culturas ainda se mostra a sua melhor forma de combate.” (BARBOSA, 2019, p. 213)

26 Trata-se de um acrônimo para “*data surveillance*” (vigilância de dados), a indicar uma nova espécie ou técnica de vigilância em razão do surgimento de novos métodos de monitoramento, como a vigilância de dados pessoais e a vigilância de dados em massa, que exigem salvaguardas mais eficazes e uma estrutura política formal. Sobre o tema, cf. CLARKE, 1988.

causa', permitida pelo CDC, configurar-se-á evidente prática abusiva repudiável, que deve ser combatida pelo sistema jurídico.

Vale lembrar que, "para que uma pessoa seja obrigada a reparar um dano injusto, é fundamental que ela tenha a autonomia de atuação, isto é, tenha a capacidade de reconhecer a licitude ou ilicitude de sua conduta e, ao mesmo tempo, a habitualidade de identificar e prever a potencialidade danosa desta." (MULHOLLAND, 2019, p. 332)

A LGPD consagrou um dever geral em seu artigo 46, que trata do imperativo da segurança da informação. Em simples termos, o referido dispositivo estabeleceu a tutela da responsabilidade civil em razão de danos decorrentes da violação aos deveres de proteção da segurança dos dados, delimitando um critério geral de imputação lastreado na verificação e demonstração do defeito na prestação de serviços por parte dos provedores, com emanação lastreada na ruptura de uma expectativa legítima quanto à segurança dos processos de coleta, tratamento e armazenagem de dados. Segundo Rafael de Freitas Valle Dresch (2009, p. 138), "a responsabilidade civil pelo fato do produto e do serviço no Código de Defesa do Consumidor é especial, fundada no defeito, o que, tecnicamente, determina a análise da culpa levíssima presumida".

Trata-se de previsão com equivalência ao que dispõe o Regulamento Geral de Proteção de Dados europeu (CASTRO, 2005, p. 229) em seu artigo 2.º, que elenca como fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o direito ao livre desenvolvimento da personalidade, o desenvolvimento econômico e tecnológico, a livre iniciativa, a livre concorrência e a defesa do consumidor.

Na lei brasileira, quando se transcende a própria legislação para impor parâmetros preventivos (ou exigências de *compliance*), vê-se surgir vasto rol de novas nuances que somente quem está diretamente atrelado ao tratamento de dados poderá antever e evitar, o que atribui previsibilidade a certos riscos e demanda atuação 'em conformidade' para o controle da responsabilização erigida pelo novo marco regulatório.<sup>27</sup>

Ao se considerar a privacidade e todos os seus contornos e características, inúmeras ações podem (e devem) ser implementadas por quem detém o poder sobre os sistemas, a fim de se salvaguardar os riscos relacionados à proteção de dados dos usuários que se valem de um serviço específico para que haja lisura nas operações de tratamento.<sup>28</sup> Práticas como a minimização do volume de processamento de dados pessoais (*privacy by design*) (NARAYANAN; SHMATIKOV, 2010, p. 24), a anonimização (CAVOUKIAN; CASTRO, 2014, p. 1), a permissibilidade ao monitoramento do tratamento pelo titular dos dados e até mesmo a

27 A doutrina destaca que "[h]á grande semelhança quando se compara os direitos europeu e brasileiro sob esse ponto de vista. Afinal, a grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida exatamente na instituição de um modelo *ex-ante* de proteção de dados. Fundamenta-se esse conceito no fato de que não existem mais dados irrelevantes diante do processamento eletrônico e ubíquo de dados na sociedade da informação. Considerando que os dados pessoais são projeções diretas da personalidade, qualquer tratamento de dados acaba por influenciar a representação da pessoa na sociedade, podendo afetar sua personalidade e, portanto, tem o potencial de violar os seus direitos fundamentais." (BIONI; MENDES, 2019, p. 810-811)

28 Com efeito: "We have a right to privacy, but it is neither a right to control personal information nor a right to have access to this information restricted. Instead, it is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones. This is the right I have called contextual integrity, achieved through the harmonious balance of social rules, or norms, with both local and general values, ends, and purposes. This is never a static harmony, however, because over time, conditions change and contexts and norms evolve along with them." (NISSENBAUM, 2010, p. 231)

realização de treinamentos regulares com as equipes são exemplos de ações que fomentam uma cultura de prevenção.

Nessa linha, é fundamental que se tenha em conta que toda política ou boa prática de governança de dados envolverá a articulação de algum objetivo independente e igualmente desejável por controladores e operadores de dados. Como consequência disso, a responsabilização por tratamento inadequado de dados pressuporá o equacionamento do enfrentamento das ações cabíveis e regularmente esperadas do respectivo agente para que seja possível promover o reequilíbrio das tensões causadas durante tais operações e que culminem na perda da autodeterminação informativa (ou, noutros dizeres, em verdadeira manipulação do controle exercido pelo consumidor sobre sua decisão). Segundo Jorge Werthein, “a perda do sentimento de controle sobre a própria vida e a perda da identidade são temas que continuam preocupantes e que estão ainda por merecer estratégias eficientes de intervenção.” (WERTHEIN, 2000, p. 76)

Na esfera pré-contratual, a lisura e a transparência são esperadas como desdobramentos da boa-fé objetiva que rege as relações de consumo e pela qual se permite integrar a norma jurídica para a junção do dever de proteção de dados emanado da LGPD aos deveres de respeito à boa-fé objetiva e à proteção das relações de consumo já delimitados como *standards* normativo-comportamentais no Código de Defesa do Consumidor. (MARQUES, 2007, p. 176-200) Isso porque “os fornecedores que conduzem negócios por meio eletrônico na Internet devem esclarecer como coletam e usam os dados dos consumidores, em face do direito de informação por estes titularizado (art. 6º, III, da Lei 8.078/1990)”. (MARTINS, 2014, p. 334)

Considerando-se que a proteção da privacidade demanda a implementação de vasto rol de boas práticas que se traduzem, ao fim e ao cabo, no imperativo da prevenção, impositivo às corporações que exploram atividades voltadas aos mercados ricos em dados e que, tradicionalmente, por serem detentoras do controle de arquitetura e programação das plataformas onde se operam tais transações, acabam por se sobrepujar ao *animus* regulatório e fiscalizatório de um Estado, o resguardo à não discriminação<sup>29</sup> – e à efetivação do princípio da neutralidade da rede – passam a demandar investigação sobre os próprios limites da liberdade econômica.

Trata-se de debate complexo e sem respostas definitivas sobre um contexto “no qual a sedução exercida pela publicidade e pelo *marketing* agressivo ultrapassa os limites do inverossímil (...)”. (DE LUCCA, 2014, p. 97) E, para combater essa situação, não se pode admitir a adoção abusiva de práticas discriminatórias na Internet, que impedem até mesmo a concretização de direitos humanos já consolidados. (MOYN, 2018, p. 220)

Os potenciais e limites da concretização de deveres de prevenção para a tutela das relações jurídicas de consumo na Internet perpassa, enfim, por virtuoso diálogo de fontes, que

29 É o que salienta Mandana Zarrehparvar (2006, p. 233): “No other human rights can be claimed if the nondiscrimination principle is not applied. Nondiscrimination is the principle that makes the other rights operational and, in a sense, makes human rights universal, not only in judicial discourse but also, to a great degree, in political and moral discourse. The WSIS Declaration of Principles and the Action Plan for the development of a global information society, although only political documents that state parties have committed themselves to, serve as platforms from which the development of the global information society should occur. The documents signal the importance of the information society, and such a society cannot exist as a democratic one if the principle of nondiscrimination is not applied. The documents ought to remind the states of their obligations to combat discrimination and to recommend implementation and mainstreaming of the non-discrimination principle in national legislation and policies to protect individuals from violations of human rights and secure their rights to access ICT. The information society can become a reality only when all human beings can claim their rights without prejudice and discrimination.”

seja capaz de conectar os diversos marcos normativos que consolidam o microssistema de proteção ao titular de dados que consome na *web* – o ciberconsumidor –, impondo-se a governança como resposta às dificuldades de tutela dessa nova realidade (PÉREZ LUÑO, 1996, p. 10), que ultrapassa a ideia de segurança da informação como mera utilização de bloqueios que evitem a invasão e o vazamento de dados, pois o que se almeja é chegar a um contexto de completa e verdadeira delimitação de métodos preventivos capazes de propagar uma cultura de integridade (*compliance*), transparência (*disclosure*) e responsabilidade (*accountability*).

## 5. CONCLUSÃO

Por todo o mencionado, a conclusão inexorável a que se chega é a de que existe agudo descompasso entre inovação e regulação, vetores antagônicos, o que conduz à formação de espaços desregulados nos quais a atuação fervorosa de agentes de tratamento dados que disputam os melhores e mais eficazes algoritmos e buscam, a todo custo, ocupar mercados, podendo praticar, ainda que inadvertidamente, a malfadada discriminação algorítmica.

Mesmo considerando que muitas questões relevantes sobre o tema ultrapassam o contexto do presente trabalho, certamente a decisão envolvendo a “Decolar.com” serve como um alerta de que a ocorrência de práticas abusivas no comércio eletrônico brasileiro não configura um universo de impunidade inacessível e intutelável pelo labor estatal, uma vez que se encaixa como um importante referencial para a ampliação dos debates sobre práticas como *geo-pricing* e *geo-blocking*. Nesse contexto, a investigação deflagrada pelo Ministério Público do Estado do Rio de Janeiro desencadeou apurações que já resultaram em sanção administrativa e, eventualmente, podem resultar em responsabilização civil da empresa em questão.

Para além disso, obtempera-se a existência de um conjunto de normas aplicável a esses casos e a outros assemelhados, mesmo antes da vigência da Lei Geral de Proteção de Dados Pessoais. Tem-se, no Brasil, verdadeiro microssistema de proteção do titular de dados na Internet, que é composto por normas como o Marco Civil da Internet e o Código de Defesa do Consumidor, e todas devem ser aplicadas transversalmente, em festejável diálogo de fontes.

Merece realce o papel do Código de Defesa do Consumidor como eixo desse microssistema que ultrapassa as lindes das tradicionais relações de consumo e irradia seus efeitos sobre as relações virtuais. Impõe-se, nesse contexto, a distinção conceitual entre os perigos e os riscos para que se possa lançar propostas regulatórias baseadas na identificação de parâmetros extranormativos para o preenchimento de verdadeiras ‘zonas cinzentas’, pois a predição comportamental a partir de algoritmos desafia o *jus imperii* estatal, uma vez que o controle sobre as plataformas resta, ao fim e ao cabo, sob o poder das corporações que delas se valem para impor métricas dedicadas à otimização de seus resultados comerciais.

Nessa linha, a proliferação de uma cultura de *compliance*, baseada em função revigorante da responsabilidade civil catalisada por instrumentais *ex ante*, aparece como saudável novo filtro para a imposição de deveres que fazem ressurgir a teoria do risco, sob viés aprimorado e adequado à sociedade da informação.

Confirma-se a hipótese dessumida na introdução, na medida em que o papel da conceitualização atribuída aos dados pessoais sensíveis pela legislação de regência propicia manancial exemplificativo de direitos que ostentam essa característica e que devem receber maior proteção do ordenamento, não se esgotando, portanto, no rol do artigo 5º, II, da LGPD. Ademais, a própria instituição da proteção aos direitos humanos como fundamento da referida lei (art. 2º, VII) denota a preocupação do legislador com a construção de uma estrutura de postulados que ultrapassa a lei individualmente considerada e inspira todo o ordenamento, conectando fontes e definindo freios ao desenvolvimento desregulado.

## REFERÊNCIAS

- ABERNATHY, David Ray. *Using geodata and geolocation in the social sciences: mapping our connected world*. Londres: Sage Publications, 2017.
- BARBOSA, Fernanda Nunes. O dano informativo do consumidor na era digital: uma abordagem a partir do reconhecimento do direito do consumidor como direito humano. *Revista de Direito do Consumidor*, São Paulo, v. 122, p. 203-232, mar./abr. 2019.
- BARROS, João Pedro Leite. Os contratos de consumo celebrados pela Internet. Um estudo de direito comparado luso-brasileiro. In: ATAÍDE, Rui Paulo Coutinho de Mascarenhas; BARATA, Carlos Lacerda (Coord.). *Estudos de direito do consumo*. Lisboa: AAFDL, 2017. v. 5.
- BELLI, Luca; DE FILIPPI, Primavera. General introduction: towards a multistakeholder approach to network neutrality. In: BELLI, Luca; DE FILIPPI, Primavera (Ed.). *Net neutrality compendium: human rights, free competition and the future of the Internet*. Cham: Springer, 2016.
- BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. *Manual de direito do consumidor*. 7. ed. São Paulo: Revista dos Tribunais, 2016.
- BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019.
- BIONI, Bruno Ricardo; MENDES, Laura Schertel. Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral brasileira de Proteção de Dados: mapeando convergências na direção de um nível de equivalência. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. São Paulo: Revista dos Tribunais, 2019.
- BORGES, Gustavo Silveira; MARTINS, Patricia Santos. As nanotecnologias, os riscos incertos e a hipervulnerabilidade do nanoconsumidor. *Revista de Direito do Consumidor*, São Paulo, v. 113, ano 26, p. 417-438, set./out. 2017.
- BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*, 12 set. 1990a. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8078compilado.htm](http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm). Acesso em: 2 set. 2021.
- BRASIL. Lei nº 8.137, de 27 de dezembro de 1990. Define crimes contra a ordem tributária, econômica e contra as relações de consumo, e dá outras providências. *Diário Oficial da União*, 28 dez. 1990b. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8137.htm](http://www.planalto.gov.br/ccivil_03/leis/l8137.htm). Acesso em: 2 set. 2021.
- BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União*, 24 abr. 2014. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 2 set. 2021.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais – LGPD. *Diário Oficial da União*, 15 ago. 2018c. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm). Acesso em: 2 set. 2021.

- BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. *Diário Oficial da União*, 15 ago. 2019. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/l13853.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm) Acesso em: 2 set. 2021.
- BRASIL. Ministério da Justiça e Segurança Pública. *Decolar.com é multada por prática de geo pricing e geo blocking*. 2018a. Disponível em: <https://www.justica.gov.br/news/collective-nitf-content-51>. Acesso em: 11 nov. 2020.
- BRASIL. Secretaria Nacional do Consumidor. Departamento Nacional de Proteção e Defesa do Consumidor. Despacho nº 299/2018. Decisão de Aplicação de Sanção Administrativa. Processo nº 08012.002116/2016-21. Representada: Decolar.com Ltda. *Diário Oficial da União*, 18 jun. 2018b.
- CASTRO, Catarina Sarmiento e. *Direito da informática, privacidade e dados pessoais*. Coimbra: Almedina, 2005.
- CAVOUKIAN, Ann; CASTRO, Daniel. Big Data and innovation, setting the record straight: de-identification does work. *The Information Technology & Innovation Foundation*, Ontario, p. 1-18, jun. 2014.
- CITRON, Danielle Keats; PASQUALE, Frank. The scored society: due process for automated predictions. *Washington Law Review*, Seattle, v. 89, p. 1-33, 2014.
- CLARKE, Roger A. Information technology and dataveillance. *Communications of the ACM*, Nova York, v. 31, n. 5, p. 498-512, maio 1988.
- COECKELBERGH, Mark. *AI Ethics*. Cambridge: The MIT Press, 2020.
- COLEMAN, Flynn. *A human algorithm: how Artificial Intelligence is redefining who we are*. Berkeley: Counterpoint, 2019.
- DE LUCCA, Newton. A proteção dos consumidores no âmbito da internet. In: LIMA, Cíntia Rosa Pereira de; NUNES, Lydia Neves Bastos Telles (Coord.). *Estudos avançados de direito digital*. Rio de Janeiro: Elsevier, 2014.
- DE LUCCA, Newton. *Direito do consumidor: aspectos práticos – perguntas e respostas*. São Paulo: Revista dos Tribunais, 1995.
- DIAS, Daniel; NOGUEIRA, Rafaela; QUIRINO, Carina de Castro. Vedação à discriminação de preços sem justa causa: uma interpretação constitucional e útil do art. 39, X, do CDC. *Revista de Direito do Consumidor*, São Paulo, v. 121, p. 51-97, jan./fev. 2019.
- DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.
- DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito digital: direito privado e Internet*. 3. ed. Indaiatuba: Foco, 2020.
- DRESCH, Rafael de Freitas Valle. *Fundamentos da responsabilidade civil pelo fato do produto e do serviço: um debate jurídico-filosófico entre o formalismo e o funcionalismo no direito privado*. Porto Alegre: Livraria do Advogado, 2009.
- DUQUE, Marcelo Schenk. *Direito privado e constituição: drittwirkung dos direitos fundamentais, construção de um modelo de convergência à luz dos contratos de consumo*. São Paulo: Revista dos Tribunais, 2013.
- ENGLEHARDT, Steven; NARAYANAN, Arvind. Online tracking: a 1-million-site measurement and analysis. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications*, Nova York, p. 1388-1401, out. 2016. Disponível em: <https://doi.org/10.1145/2976749.2978313>. Acesso em: 30 nov. 2020.
- FORTES, Pedro Rubim Borges; MARTINS, Guilherme Magalhães. O consumidor contemporâneo no Show de Truman: a geodiscriminação como prática ilícita no direito brasileiro. *Revista de Direito do Consumidor*, São Paulo, v. 124, p. 235-260, jul./ago. 2019.
- GARCIA, Leonardo de Medeiros. *Código de Defesa do Consumidor comentado artigo por artigo*. Salvador: Juspodivm, 2019.
- GRAU, Eros Roberto. Interpretando o Código de Defesa do Consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 5, jan./mar. 1993.

GREENE, Kevin T.; PARK, Baekwan; COLARESI, Michael. Machine learning human rights and wrongs: how the successes and failures of supervised learning algorithms can inform the debate about information effects. *Political Analysis*, Cambridge, v. 27, n. 2, p. 223-230, abr. 2019.

HOLDENER III, Anthony. *HTML5 Geolocation*. Sebastopol: O'Reilly, 2011.

ISRAVEL, Deva Priya; SILAS, Salaja; RAJSINGH, Elijah. Reliable surveillance tracking system based on software defined Internet of Things. In: PETER, J. Dinesh; ALAVI, Amir H.; JAVADI, Bahman; FERNANDES, Steven L. *The cognitive approach in Cloud Computing and Internet of Things technologies for surveillance tracking systems*. Londres: Academic Press/Elsevier, 2020.

KLEE, Antonia Espíndola Longoni. *Comércio eletrônico*. São Paulo: Revista dos Tribunais, 2014.

KRETZMANN, Renata Pozzi. *Informação nas relações de consumo: o dever de informar do fornecedor e suas repercussões jurídicas*. Belo Horizonte: Casa do Direito, 2019.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei nº 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro*. São Paulo: Thomson Reuters Brasil, 2019.

LACE, Susanne. The new personal information agenda. In: LACE, Susanne (Ed.). *The glass consumer: life in a surveillance society*. Bristol: The Policy Press, 2005.

LANIER, Jaron. *Who owns the future?* Nova York: Simon & Schuster, 2013.

LIMBERGER, Têmis. Direito e informática: o desafio de proteger os direitos do cidadão. In: SARLET, Ingo Wolfgang (Org.). *Direitos fundamentais, informática e comunicação: algumas aproximações*. Porto Alegre: Livraria do Advogado, 2007.

LIPOVETSKY, Gilles; SERROY, Jean. *A cultura-mundo: resposta a uma sociedade desorientada*. Tradução de Maria Lúcia Machado. São Paulo: Cia. das Letras, 2011.

LORENZETTI, Ricardo Luís. *Comércio eletrônico*. Tradução de Fabiano Menke. São Paulo: Revista dos Tribunais, 2004.

MARQUES, Claudia Lima (Org.). *A nova crise do contrato*. São Paulo: Revista dos Tribunais, 2007.

MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Revista dos Tribunais, 2004.

MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor*. 8. ed. São Paulo: Revista dos Tribunais, 2016.

MARTINS, Guilherme Magalhães. O geopricing e geoblocking e seus efeitos nas relações de consumo. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). *Inteligência artificial e direito: ética, regulação e responsabilidade*. São Paulo: Thomson Reuters Brasil, 2019.

MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na Internet*. 2. ed. São Paulo: Revista dos Tribunais, 2014.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data: a revolution that will transform how we live, work, and think*. Nova York: Houghton Mifflin Harcourt, 2014.

MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. *Reinventing capitalism in the age of Big Data*. Nova York: Basic Books, 2018.

MIOZZO, Júlia. Decolar é multada em R\$ 7,5 milhões por práticas abusivas contra consumidor. *InfoMoney*, 18 jun. 2018. Disponível em: <https://www.infomoney.com.br/minhas-financas/turismo/noticia/7479979/decolar-multada-milhoes-por-praticas-abusivas-contra-consumidor>. Acesso em: 12 nov. 2020.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. *Revista dos Tribunais*, São Paulo, v. 1009, p. 173-222, nov. 2019.

MIRAGEM, Bruno. Função social do contrato, boa-fé e bons costumes: nova crise dos contratos e a reconstrução da autonomia negocial pela concretização das cláusulas gerais. In:

- MORASSUTTI, Bruno Schimitt. Responsabilidade civil, discriminação ilícita e algoritmos computacionais: breve estudo sobre as práticas de geoblocking e geoprizing. *Revista de Direito do Consumidor*, São Paulo, v. 124, p. 213-234, jul./ago. 2019.
- MOYN, Samuel. *Not enough: human rights in an unequal world*. Cambridge: Harvard University Press, 2018.
- MULHOLLAND, Caitlin. Responsabilidade civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA): autonomia, imputabilidade e responsabilidade. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coord.). *Inteligência Artificial e Direito: ética, regulação e responsabilidade*. São Paulo: Thomson Reuters Brasil, 2019.
- NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and fallacies of personally identifiable information. *Communications of the ACM*, Austin, v. 53, n. 6, p. 24-26, jun. 2010.
- NISSENBAUM, Helen. *Privacy in context: technology, policy, and the integrity of social life*. Stanford: Stanford University Press, 2010.
- O'NEIL, Cathy. *Weapons of math destruction: how Big Data increases inequality and threatens democracy*. Nova York: Crown, 2016.
- ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Assembleia Geral das Nações Unidas. *Declaração Universal dos Direitos Humanos*. Paris. 10 dez. 1948. Disponível em: <https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf>. Acesso em: 15 nov. 2020.
- PARENTONI, Leonardo. Network neutrality: what is internet made of, how is it changing and how does it affect your life? *Revista da Faculdade de Direito da UFMG*, Belo Horizonte, nº Especial, p. 195-243, 2017.
- PÉREZ LUÑO, Antonio Enrique. *Manual de informática e derecho*. Barcelona: Ariel, 1996.
- RIBEIRO, Luci. Decolar é multada em R\$ 7,5 milhões por práticas abusivas. *Estadão*. 18 jun. 2018. Disponível em: <https://economia.estadao.com.br/noticias/negocios,decolar-e-multada-em-r-7-5-milhoes-por-praticas-abusivas,70002354803>. Acesso em: 20 nov. 2020.
- RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
- SANDEL, Michael J. *O que o dinheiro não compra: os limites morais do mercado*. Tradução de Clóvis Marques. Rio de Janeiro: Civilização Brasileira, 2012.
- SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional*. 10. ed. Porto Alegre: Livraria do Advogado, 2010.
- SILVA, Jorge Pereira da. *Deveres do Estado de protecção de direitos fundamentais: fundamentação e estrutura das relações jusfundamentais triangulares*. 3. ed. Lisboa: Universidade Católica Editora, 2015.
- TOMASEVICIUS FILHO, Eduardo; FERRARO, Angelo Viglianisi. Le nuove sfide dell'umanità e del diritto nell'era dell'Intelligenza Artificiale. *Revista Direitos Culturais*, Santo Ângelo, v. 15, n. 37, p. 401-413, 2020.
- TRSTENJAK, Verica. General report: The influence of human rights and basic rights in private law. In: TRSTENJAK, Verica; WEINGERL, Petra (Eds.). *The influence of human rights in private law*. Cham: Springer, 2016.
- VAN OOIJEN, Iris; VRABEC, Helena U. Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of Consumer Policy*, Berlin/Heidelberg: Springer-Verlag, v. 42, p. 91-107, 2019.
- VENTURA, Ivan. Decolar.com é multada em R\$ 7,5 milhões por desrespeito ao consumidor. *Consumidor Moderno*, 18 jun. 2018. Disponível em: <https://www.consumidormoderno.com.br/2018/06/18/decolar-multada-milhoes-desrespeito-consumidor/>. Acesso em: 11 nov. 2020.
- WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ciência da Informação*, Brasília, v. 29, n. 2, p. 71-77, mai./ago. 2000.
- WINEGAR, Angela G.; SUNSTEIN, Cass R. How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, [S. l.], v. 42, p. 1-16, 2019.
- ZANATTA, Rafael. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Protecção de Dados. *ResearchGate*, fev. 2019. Disponível em: <https://bit.ly/3hQe5wM>. Acesso em: 1 dez. 2020.

ZARREHPARVAR, Mandana. A nondiscriminatory information society. In: JØRGENSEN, Rikke Frank (Ed.). *Human rights in the global information society*. Cambridge: The MIT Press, 2006.

#### **Dados do processo editorial**

- Recebido em: 22/05/2020
- Controle preliminar e verificação de plágio: 22/05/2020
- Avaliação 1: 31/10/2020
- Avaliação 2: 04/11/2020
- Decisão editorial preliminar: 09/11/2020
- Retorno rodada de correções: 07/08/2021
- Decisão editorial/aprovado: 03/09/2021

#### **Equipe editorial envolvida**

- Editor-chefe: 1 (SHZF)
- Editor-assistente: 1 (ASR)
- Revisores: 2