FURB
Revista Jurídica

PPGD
Programa de Pós-Graduação
Stricto Sensu em Direito

O CONSUMIDOR DIGITAL: DA VULNERABILIDADE ALGORÍTMICA AO EMPODERAMENTO

THE DIGITAL CONSUMER: FROM ALGORITHMIC VULNERABILITY TO EMPOWERMENT

Dennis Verbicaro[1]
Vanessa Maria Dias Montão[2]

RESUMO: O presente trabalho objetiva analisar a coleta, o tratamento e a destinação dos dados pessoais nas relações de consumo realizadas na internet. Os dados se tornaram um instrumento valioso aos empresários, podendo potencializar riscos à intimidade e privacidade do consumidor, sobretudo sob a perspectiva do capitalismo de vigilância pensado por Shoshana Zuboff. Nessa perspectiva, a tutela normativa dos dados pessoais será analisada nos planos nacional e internacional, tomando-se como referência as informações coletadas pelos aplicativos de delivery. Discute-se, também, como o empoderamento virtual do consumidor corporifica o ideal de solidariedade, na medida em que exerce força contra majoritária em relação aos abusos do poder econômico nesse ambiente dominado pelas plataformas eletrônicas. Utilizou-se o método dedutivo, através de pesquisa teórico-bibliográfica e da análise crítica do discurso, visando desvelar o que há por meio da linguagem virtual nas relações de poder entre esse novo perfil de fornecedor e a vulnerabilidade algorítmica do consumidor. Conclui-se que, diante da vulnerabilidade agravada do consumidor digital, a sofisticação do assédio de consumo e o controle insuficiente da política de dados das plataformas eletrônicas, a articulação conjunta por meio da insurgência qualificada nas redes sociais e sites de compartilhamento de experiências são medidas eficazes para preservar a liberdade de escolha dos consumidores e mitigar os efeitos das práticas abusivas.

PALAVRAS-CHAVE: Direito do Consumidor; Dados Pessoais; Privacidade Virtual; Empoderamento do Consumidor; Vulnerabilidade algorítmica.

ABSTRACT: The main focus of this study is to bring up the consumerist issue in a virtual environment, therefore, it aims to analyze the collection and use of personal data in consumer relations carried out on the internet under a social, political and legal context, given that such data currently they represent power and move the economy. Data has become a valuable tool businesspeople, being able to potentiate the sphere of damage to be applied ahead of the knowledge of the most banal acts to the most intimate of each individual. The practices of using consumer data are addressed, also the surveillance capitalism thought by Zuboff, but also the national and international regulatory tutelage around such discussion. In addition, the information requested by the delivery applications, such as the virtual consumer empowerment, that is, it aims to demonstrate how civil society, through the ideal of solidarity, exerts expressive strength in the face of the

[1] Doutor em Direito pela Universidade de Salamanca (ES). Mestre em Direito pela Universidade Federal do Pará – UFPA. Professor da Graduação e dos Programas de Pós-Graduação Stricto Sensu da Universidade Federal do Pará-UFPA e do Centro Universitário do Pará – CESUPA. Procurador do Estado do Pará. Advogado e Diretor do Brasilcon. Líder dos Grupos de Pesquisa (CNPq) "Consumo e Cidadania" e "Consumo sustentável e globalização econômica". E-mail: dennis@verbicaro.adv.br.
[2] Bolsista de iniciação científica (CNPq) e Graduanda em Direito da UFPA. Membro do Grupo de Pesquisa "Consumo e cidadania" (CNPq/UFPA).

arbitrations of the digital environment, building alternatives aimed at protecting personal data to, consequently, overcome the impacts positive in the process of forming a new paradigm in the behavior of the business segment in relation to their ethical duties towards the consumer. It should be noted that in such a study, the method of critical discourse analysis was used, since it aimed to unveil what exists through language, that is, power relations, situations of vulnerability and interpretation constructions. The results of the research can be fundamental to better understand what generates the need for effective consumer empowerment in digital media, as well as how this force can be exercised. It is concluded that, in view of the aggravated vulnerability of the digital consumer, the sophistication of consumer harassment and the insufficient control of the data policy of electronic platforms, the joint articulation through the qualified insurgency on social networks and experience sharing sites are measures effective measures to preserve consumers' freedom of choice and mitigate the effects of abusive practices.

KEYWORDS: Consumer Law; Personal data; Virtual Privacy; Consumer's Empowerment; Algoritmic Vulnerability.

1. INTRODUÇÃO

A atual discussão sobre os desafios da tutela do consumidor foi, inevitavelmente, deslocado para o ambiente digital, com especial atenção à relativização forçada de alguns importantes direitos da personalidade diante do novo capitalismo de vigilância (ZUBOFF, 2018) na coleta, tratamento e destinação dos dados pessoais nas relações de consumo e foi além.

A superexposição da intimidade e da privacidade no ambiente virtual, a funcionalização da liberdade de escolha pelo assédio de consumo, impulsionado por uma inteligência artificial cada vez mais invasiva em nossa rotina diária, a partir dos dados pessoais coletados mediante consentimento viciado ou involuntário, tudo implica na necessidade de atualização do direito do consumidor, justamente para incorporar esse novo debate, a partir de um necessário diálogo entre a Lei 8.078/90 (Código de Defesa do Consumidor) e a Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais).

Nesse ambiente virtual, contudo, há novas oportunidades, como a possibilidade de um maior engajamento coletivo a partir da construção de identidades para um modelo de consumo consciente e responsável, de modo que os consumidores, através dessa maior articulação política e de uma cidadania instrumental (VERBICARO, 2019), possam exercer uma força contra majoritária em relação à grande influência das plataformas eletrônicas durante o acelerado processo de imersão tecnológica do consumidor e os riscos daí decorrentes, sobretudo se considerarmos a atuação errática do Estado no seu importante papel regulador.

O consumidor, pensado individualmente e a partir do novo conceito de vulnerabilidade algorítmica, terá maiores dificuldades para resistir ao poderio econômico dos grandes "guardiões de acesso" (*Gatekeepers)* que, geralmente, atuam de forma concentrada no mercado de consumo, mediante contratos que resguardam sua posição jurídica de superioridade em relação ao usuário final, limitando seus deveres e dificultado a possibilidade de questionamento judicial na hipótese de danos.

Da mesma forma, diante da assimetria informacional, este consumidor digital estará mais propenso a erros técnicos, escolhas ruins e riscos às recorrentes falhas de segurança na proteção de seus dados pessoais sensíveis tutela dos dados pessoais, sem falar do crescente assédio que alimenta uma maior compulsão para o consumo.

Conforme Gilles Lipovetsky (2008, p. 38), à medida em que as sociedades enriquecem, vem a surgir de forma incessante novos anseios de consumo. "Quanto mais se consome, mais se quer consumir", pois a era da abundância é inafastável da esfera das satisfações desejadas e da incapacidade de suprimir os volúveis desejos de consumo.

Esse consumidor digital, ao manusear sites, redes sociais e plataformas eletrônicas favorece o abastecimento e o tráfico de dados pessoais. Na maioria das vezes, tais dados são fornecidos voluntariamente pelo titular e, quando armazenados, se constituem como uma informação valiosa que pode permitir a identificação precisa dos desejos do indivíduo, através da criação de um perfil de consumo pelo uso de algoritmos de inteligência artificial.

Esse mercado de dados se converte em verdadeira atividade econômica, na medida em que sua coleta e tratamento revelam uma nova espécie de poder contemporâneo, esse que motiva empresas e países a se debruçarem rumo ao aperfeiçoamento do controle da maior quantidade de dados que possam lhe conceder vantagens publicitárias e administrativas, conforme Doneda (2011).

Nesse sentido, Antonialli e Cruz (2017), alertam a respeito dos efeitos diretos da coleta irrestrita e mercadológica de dados pessoais, na medida em que esse fenômeno tem gerado não somente a possibilidade de manipulação de dados em grande escala – *big data* -, como também, veio a permitir que o mercado, em sua categoria publicitária, viesse a se tornar mais assertivo e proativo, levando a propaganda direcionada ao seu público-alvo baseado em seus dados colhidos. Tal estratégia é resultado das práticas de segmentação de marketing conhecidas como "marketing *one-to-one*", as quais se mostram como alternativas poderosas ao antigo modelo de publicidade em massa, na medida em que são utilizados bancos de dados e meios interativos para entregar ao

consumidor o produto e/ou serviço mais próximo de suas reais necessidades, além de fidelizá-lo com a satisfação de ir ao encontro de seus desejos de consumo.

Tais práticas comerciais, embora rentáveis e conquanto adaptadas para a realidade da intermediação direta da tecnologia e da Internet nas relações privadas, devem ser submetidas a severa investigação por parte dos juristas, principalmente, no que tange aos princípios basilares que regem as relações civis e consumeristas no ordenamento jurídico brasileiro.

Há de se destacar, também, o processo de transição entre paradigmas na transformação da realidade política, jurídica e social que fomentaram um debate racional motivado para as mudanças necessárias para a criação de um direito privado solidário, calcado no compartilhamento de autoridade política, na construção de uma base jurídica plural e no exercício de uma participação política qualificada do consumidor, naquilo que se denomina cidadania instrumental do consumidor (VERBICARO, 2019).

Os objetivos da pesquisa envolvem a reflexão acerca da intangibilidade de dados pessoais pelo consumidor digital, pormenorizando os mecanismos nacionais e estrangeiros de proteção de suas informações pessoais e sensíveis. Buscar-se-á compreender as formas de tratamento dos dados pessoais coletados pelos fornecedores no ambiente digital em todas as fases da negociação, tal como verificar a eficácia e aplicabilidade das normas que visam regular essa modalidade das relações de consumo no cenário digital, com vistas a melhor preservação da privacidade e segurança do consumidor.

O método de pesquisa foi o dedutivo, desenvolvido essencialmente através de pesquisa teórico-bibliográfica. Os materiais utilizados foram a bibliografia nacional e estrangeira nas áreas do Direito do Consumidor, Digital e da Sociologia. Objetivando-se um maior rigor na coleta de dados durante a pesquisa de campo, veio a ser utilizada a metodologia da análise crítica de discurso (PACHECO GUIMARÃES, 2012), a qual vê o discurso como representações do mundo, que demonstram que o conhecimento foi socialmente construído. O objeto de estudo visa desvelar o que há por meio da linguagem, isto é, as relações de poder, as situações de vulnerabilidade e as construções de interpretações (MELO, 2009). Tal análise crítica se dá com a coleta de dados, a análise desses e os resultados alcançados, isto é, o analista reflete sobre os elementos que foram encontrados. Sendo tal método relevante para a proposta desta pesquisa, uma vez que essa objetiva refletir sobre a vulnerabilidade algorítmica na coleta, tratamento e uso indevido dos dados pessoais pelo consumidor digital, vindo a detalhar os mecanismos de tutela jurídica.

Logo, o artigo possui como estrutura, isto é, aborda primeiramente sobre a imersão tecnológica na era do consumidor do capitalismo de vigilância e a consequente vulnerabilidade

algorítimica; em segundo lugar, a tutela normativa dos dados pessoais em âmbito nacional e internacional; em terceiro ponto, preocupa-se em abordar acerca das informações obtidas pelo aplicativo de delivery iFood, ou seja, a análise do modelo de coleta de dados; em quarto ponto, o empoderamento do consumidor digital; e, por fim, elucida-se sobre os impactos positivos e mudanças concretas no comportamento empresarial.

2. A IMERSÃO TECNOLÓGICA DO CONSUMIDOS NA ERA DO CAPITALISMO DE VIGILÂNCIA E A VULNERABILIDADE ALGORÍTMICA DECORRENTE.

O consumidor digital se encontra despido e vulnerável para com as ações indevidas dos fornecedores, seja em decorrência do assédio de consumo, dos riscos decorrentes da coleta e uso indevido dos seus dados pessoais, pela assimetria informacional que impede o exercício adequado da liberdade de escolha, pela proliferação das cláusulas exoneratórias de responsabilidade das grandes plataformas, que atuam de forma concentrada no mercado e com o beneplácito de uma regulação errática do Estado.

No contexto da sociedade da informação, as relações e interações humanas, tal como seus intercâmbios e comunicações, transferem-se para o ciberespaço de Levy (1999, p. 92-92), isto é, um grande espaço de interconexão de computadores e de suas memórias, no sentido informático de armazenamento de arquivos e dados. Trata-se de meio virtual, fluido, hipertextual e interativo, tratável e acessível em tempo real e, por intermédio desse a humanidade pôde confiar à rede mundial suas formas de comunicação e suas memórias para livre acesso em qualquer lugar, desde que se disponha das ferramentas indispensáveis. O principal motor desta nova configuração social são os dados e a informação propriamente dita.

Diante disso, em um primeiro momento, há de se pensar nas novas práticas de utilização dos dados do consumidor, tal como as suas características. Dentre tais práticas, faz-se presente o *e-commerce*, isto é, o comércio eletrônico, o qual está em expansão e utiliza todas as ferramentas possíveis para atrair o consumidor virtual e obter os seus dados virtuais.

Com o surgimento e a popularização da World Wide Web, ou seja, da internet, em 1991, veio a possibilitar o nascimento do comércio eletrônico e, em 1995, foram fundadas duas das principais *e-commerces* do mundo, isto é, a Amazon e o Ebay. Estas empresas ajudaram a revolucionar a maneira de se comprar e vender todo tipo de produto pela internet. Finalmente o comércio

eletrônico iria encontrar o grande público e se transformar num fenômeno de massa (FREIRE; SALGADO, 2019).

Posteriormente, o e-commerce veio a se expandir, dividindo-se em tipos, de modo que há o Business-to-Business (B2B), o qual diz respeito sobre a troca de produtos, serviços ou informações entre entidades empresariais. No B2B, o público-alvo são empresas e não o consumidor final. Os compradores B2B se preocupam com o processo de compra, que deve ser eficiente e integrado de ponta a ponta. O que caracteriza o tipo de comércio eletrônico que uma empresa pratica não é o produto, mas sim a atividade fim que a mercadoria é destinada. Isso define o modelo de negócio do e-commerce e os figurantes que atuam nesse modelo (FREIRE; SALGADO, 2019).

Mas também há o *Business-to-Consumer* (B2C), que se dá quando a venda ocorre entre uma empresa e o consumidor final. Por ter interação direta com o cliente final, em tal modalidade de e-commerce a usabilidade e o design das plataformas virtuais são fatores cruciais para atrair e reter clientes. Também há o *Business-to-government* (B2G), o qual é referente ao comércio entre empresas e o setor público. Além do *Consumer-to-Consumer* (C2C), esse que é relativo a interação direta de um consumidor para com o outro (FREIRE; SALGADO, 2019).

À vista disso, há um consenso sobre o grande potencial para a expansão do e-commerce no Brasil. Dados de 2015 do *WebShoppers (E-bit*) e do *Top 500 Guide Internet Retailer* tornaram claro que o Brasil é o 10º maior mercado de e-commerce do mundo. De modo que em 2014, conforme levantamento de Guissoni, Oliveira e Teixeira (2016), suas vendas totalizaram R$ 35,8 bilhões, crescendo 25% em relação ao ano anterior e representando mais da metade das vendas na América Latina (53,3%). Os compradores on-line passaram de 32 milhões em 2011 para 61,6 milhões em 2014. As compras via mobile somaram R$ 53 milhões em 2011 e chegaram a quase R$ 3 bilhões em 2014.

Nessa mesma lógica de apropriação dos dados pessoais do consumidor, os aplicativos de delivery, dentre eles, o iFood, Uber eats, 99 food. Essas plataformas provocaram grande transformação no modo de consumir alimentos, uma vez que o cardápio está na tela do smartphone, tablet ou computador, além da possibilidade de se conseguir descontos, bem como receber isenções na taxa de serviço, além da possibilidade, via aplicativo, de avaliar a comida e o entregador, atribuindo gorjeta se assim desejar.

Segundo Monty (2018), esta relação virtual apresenta problemas, isto é, quais são os aspectos físicos desses produtos digitais que estariam afetando a experiência de comer? O aparelho de celular portátil compreendido como algo físico permite ao cliente ter em mãos o cardápio de

um estabelecimento sem sair de casa, não tendo a necessidade de se conversar com o garçom, tirar dúvidas sobre determinado prato e, em seguida, realizar o pedido. Ademais, utilizando esses aplicativos não se ouve o barulho da cozinha, nem se vê os garçons com suas bandejas pelo salão, muito menos se sente o cheiro da comida, antes mesmo que ela chegue à mesa.

Outrossim, é colocado em questão o aspecto econômico, uma vez que o cliente não precisa ouvir a clássica pergunta "crédito ou débito?", que inúmeras vezes é realizada nos pagamentos, vindo a economizar com a taxa de serviço, tal como com o valor do estacionamento, por exemplo. Isso porque alguns restaurantes não cobram taxa de entrega por pedidos feitos via apps (MONTY, 2018).

Não há dúvidas de que a experiência sensorial e as interações sociais autênticas que apenas um restaurante poderia oferecer foram ressignificadas, não necessariamente para melhor.

Essa nova realidade e o consentimento involuntário na coleta tratamento e destinação dos dados dos consumidores são um retrato fiel do capitalismo de vigilância, expressão criada pela perspectiva de Shoshana Zuboff (2018).

Essa nova vertente do capitalismo surge do *big data*, esse enquanto elemento crucial de acumulação intencional de dados, o qual visa prever e alterar o comportamento humano por meio do controle de mercado. Segundo Figueiras (2021), o capitalismo de vigilância se baseia na monetização dos dados comportamentais ao vender o acesso em tempo real ao fluxo da vida cotidiana, visando gerar influência e modificação no comportamento dos indivíduos para fins lucrativos.

A lógica do *big data* levou a informatização da economia, isto é, quando tudo pode ser convertido em dados digitais. Cada tipo de dado possui uma finalidade específica e a sua extração é o motor do *big data*. As redes sociais são como armadilha de captura de atenção para que os usuários possam gerar dados suficientes para vender nichos de mercado específico aos fornecedores, os quais conseguem projetar e canalizar com certo grau de certeza de consumo para quem seria mais adequado um anúncio de produto.

Bruno, Cardoso, Kanashiro et al (2018), destacam que o capitalismo de vigilância se expandiu de maneira gradual durante a última década, vindo a incorporar novas políticas e relações sociais, também que apesar de ser possível que o *big data* seja configurado para outros usos, esses não excluem suas origens no projeto de extração alicerçado na indiferença formal acerca das populações que são sua fonte de dados e seus alvos finais.

No documentário "Shoshana Zuboff em Capitalismo de Vigilância / VPRO Documentário"[3], esse visto por mais de 3 (três) milhões de pessoas, a própria Zuboff esclarece que há o argumento por parte das empresas, de que os dados são coletados para que o serviço prestado seja melhorado. Ela afirma que, na verdade, que esses dados são analisados para produzir padrões do comportamento humano, vindo a prever preferências de grupos específicos, Shoshana Zuboff chama de "excedente comportamental", isto é, corrente de dados repletas de previsões comportamentais, o que poderá ser canalizado para o consumo.

A sistemática do capitalismo de vigilância está nos pequenos detalhes, cada vez mais os mecanismos de inteligência artificial conhecem sobre as seres humanos e os seus interesses, por exemplo, o Google sabe onde estão e o que pensam, o Facebook conhece os amigos e as preferências, uma vez que coletam informações do rastro digital deixados, sabem até os erros gramaticais que os sujeitos cometem, também as cores que gostam, a frequência que visitam determinadas páginas, quão rápido digitam, quantas horas dormem, a velocidade que dirigem e quantos passos dão, eis os dados residuais que contribuem para tal vigilância ser cada vez mais aperfeiçoada.

Oliveira, Andrade e Santos (2020, p. 44), entendem que as redes sociais, sobretudo, o Facebook, "têm sido uma poderosa fonte de compartilhamento de dados e manutenção ativa do capitalismo de vigilância. O Facebook foi lançado em 2004 e tinha como principal objetivo melhorar a comunicação dos alunos da Universidade de Harvard. Entretanto, essa plataforma é hoje uma das mais potentes formas de extração de dados dos usuários".

Oliveira, Andrade e Santos (2020) também esclarecem que o poderio do Facebook se torna tão presente na vida dos usuários que, ao utilizarem aplicativos ou criarem contas em plataformas para acessar conteúdos da internet, o registro de novo usuário pode ser realizado através do login no Facebook, mas o que parece ser opção mais fácil para o sujeito, esconde riscos, haja vista os dados coletados.

Ao passo que os estudos sobre capitalismo de vigilância têm alcançado notoriedade, o assunto está sendo abordado nas mídias digitais, como no documentário da Netflix "O Dilema das Redes", esse abarca alguns dos desenvolvedores das grandes plataformas digitais, como o Facebook, Google e Instagram, revelando como ocorre a extração e manipulação dos dados, também apresenta uma história de ficção sobre como uma família vivencia as redes sociais e os impactos que podem ser percebidos na vida cotidiana. Tal extração pode gerar que determinados

[3] VPRO DOCUMENTÁRIO. Shoshana Zuboff em Capitalismo de Vigilância / VPRO Documentário. Disponível em: <https://www.youtube.com/watch?v=hIXhnWUmMvw>. Acesso em: 20 jan. 2021.

conteúdos sugestionados em nossas redes sociais resultem em ações direcionada, ou seja, é possível influenciar desde escolhas de compras à representantes políticos de discursos alinhados às informações que disponibilizamos nas redes. Tais escolhas direcionadas podem comprometer a percepção dos usuários, vindo a forjar identidades e visões de mundo (OLIVEIRA; ANDRADE; SANTOS, 2020).

Portanto, é relevante tentarmos mensurar o que seria essa atitude predatória do sistema, Zuboff cita como um exemplo o jogo Pokemon Go, o qual faz com que seus usuários coletem os pokemons em lojas, restaurantes, bares – esses que compram passe no jogo -, sendo estimulado o consumo naqueles locais pelo público-alvo do jogo, uma vez que são obrigados, caso queiram coletar o pokemon, a efetivar, segundo ela, a "passada" no local. Em tal exemplo, usuários com determinados padrões de preferência são direcionados para estabelecimentos que lhe agradem, logo, o jogo vai além e faz com que o sujeito social se faça presente em um lugar específico, o qual foi definido pelo fornecedor que comprou o passe – substituindo a publicidade direcionada[4]. Quanto mais hiperconectados os sujeitos estão, mais fornecem seus dados pessoais, mais vulneráveis se tornam e tendem a ser mais manipulados. A solução não seria a simples desconexão, mas sim a procura coletiva por soluções, uma delas, o controle normativo dessas práticas abusivas a partir do reconhecimento dessa vulnerabilidade algorítmica.

3. A TUTELA NORMATIVA DOS DADOS PESSOAIS EM ÂMBITO NACIONAL E INTERNACIONAL

Há de se verificar os dispositivos normativos que visam proteger os dados pessoais em âmbito nacional e internacional, no que diz respeito a sua eficácia e aplicabilidade diante da complexidade das relações digitais. Sendo assim, tem-se na legislação infraconstitucional a Lei nº 12.965/2014 – Marco Civil da Internet (MCI); a Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD); a Lei 8.078/1990 – Código de Defesa do Consumidor (CDC) e, em seara internacional, o General Data Protection Regulation 2016/679 (GDPR).

Deste modo, vem a ser destacado que, diante da complexidade das relações digitais, o MCI possui eficácia e aplicabilidade reduzida. O MCI, conforme Tomasevicius Filho (2016), surgiu em decorrência de problemas envolvendo a invasão de privacidade praticada por um Estado contra o

[4] VPRO DOCUMENTÁRIO. Shoshana Zuboff em Capitalismo de Vigilância / VPRO Documentário. Disponível em: <https://www.youtube.com/watch?v=hIXhnWUmMvw>. Acesso em: 20 jan. 2021.

outro, de modo que o governo brasileiro pressionou o Congresso Nacional para a aprovação de uma lei sobre comportamentos na esfera virtual, denominada "Marco Civil da Internet" ou de "Constituição da Internet", termo esse equivocado pela própria estrutura internacional da rede, para assim tentar regular o âmbito virtual, com direitos e deveres dos usuários e provedores de internet no Brasil.

Apesar do Marco Civil da Internet ter sido bastante festejado por ser a lei que veio a disciplinar os direitos e deveres dos usuários da rede, não foram evidentes mudanças substanciais, uma vez que esta lei não acrescentou muito pouco nada à legislação vigente, sobretudo em matéria de tutela de dados pessoais.

À vista disso, a expectativa gerada com a discussão dessa lei ocorreu pela crença errônea de que as normas contidas na Constituição Federal, no Código Civil, no Código Penal, nos Códigos de Processo Civil e Penal, no Código de Defesa do Consumidor, bem como no Estatuto da Criança e do Adolescente, além da lei sobre interceptação de comunicações (Lei n.9.296/96) não teriam aplicação nas relações jurídicas estabelecidas na internet (TOMASEVICIUS FILHO, 2016).

Há de se destacar, também, que é aspecto intrigante do Marco Civil da Internet a ingenuidade do legislador brasileiro de manter a pretensão de solução de problema de escala mundial, com efeitos extraterritoriais, por meio de uma lei nacional, pois a própria estrutura da internet permite que as violações dos direitos das pessoas ocorram em qualquer parte do mundo, passando ao largo da jurisdição brasileira. Parece confessar essa dificuldade, ao afirmar-se, no art.2º, I, do Marco Civil da Internet, que um dos fundamentos da disciplina do uso da internet é o "reconhecimento da escala mundial da rede". (TOMASEVICIUS FILHO, 2016, p. 276–277).

A LGPD busca regular a tutela dos dados pessoais e como eles são administrados, de forma que o seu intuito seja sempre o respeito aos direitos individuais, tratando os dados com transparência e responsabilidade (BEZERRA, 2019, p. 31). A LGPD é um grande avanço normativo e representa maior controle dos dados pessoais dos consumidores.

Ressalta-se que durante a produção da LGPD houve cautela para que a lei estivesse em sintonia com uma dimensão da privacidade, sobretudo em uma perspectiva virtual, de modo que a adoção de conceitos como "*Privacy by Design"* demonstraram a preocupação do legislador em gerar mecanismos que pudessem proteger o indivíduo, assim como tutelar o próprio dado em si, desde sua captação até sua eventual exclusão, demonstrando que é reconhecido um valor na informação em si, valor resultante da forma como uma sociedade contemporânea e hiperconectada percebe as informações e como elas são preciosas e dignas de proteção (BEZERRA, 2019).

Todavia, a legislação supracitada exclui o tratamento de dados pessoais para fins jornalísticos, de segurança pública, defesa nacional, segurança do Estado, bem como atividades de investigação e repressão de infrações penais, de acordo com Mobile time (2019). Ademais há de se destacar que a LGPD vem a ser restrita, pois segmenta o seu alcance, que é muito mais amplo, sem falar que oferece pseudo-soluções que apenas "arranham" a superfície do problema, vindo a gerar uma falsa sensação de conformidade integral, conforme Cio (2019). Por fim, destacar-se-á que a lei é ampla demais para que se cobre seu cumprimento às empresas de qualquer porte, assim como as sanções administrativas parecem conflitante com a temporalidade da lei e desmedidas a real capacidade do governo de fiscalizar, de acordo Cio (2019).

Também, é crucial explanar acerca do Código de Defesa do consumidor, esse que possui eficácia e aplicabilidade extensos, uma vez que possui normas de ordem pública e interesse social que, apesar das suas três décadas de vigência, continua atual e eficaz sobretudo através do controle pré-contratual da assimetria informacional, da relativização da vontade no consentimento e pelo reconhecimento da responsabilidade civil das plataformas por eventuais danos ao consumidor.

Embora o texto da lei tenha sido formulado num período em que a internet já demonstrava seu potencial em desenvolvimento, as transações eletrônicas se encontravam ainda em estágio relativamente primário, deixando de haver normas especificamente voltadas para o comércio virtual. Não obstante, inexiste divergência quanto à sua aplicação na tutela de interesses de consumidores e fornecedores para conflitos oriundos das transações virtuais, mesmo porque diversos dispositivos podem ser aplicados a essas transações por analogia (MELO; VASCONCELOS, 2012).

Além disso, há de se colocar em questão o respaldo internacional, isto é, o GDPR, o qual dispõe sobre o tratamento, processamento, transferência, fiscalização e responsabilização quanto a dados pessoais. Estabelece novo regramentos sobre a proteção de dados pessoais e a livre circulação de dados e revoga a Diretiva nº 95/46/CE do Parlamento Europeu e do Conselho, cuja finalidade é a proteção das liberdades e dos direitos fundamentais. Ressalta-se que a elaboração da GPRD foi baseada em 20 anos de atividade doutrinária, legislativa e jurisprudencial europeia. Nesse contexto, incorpora o espírito e aperfeiçoa a abordagem da Diretiva nº 95/46/CE (SEGUNDO, 2019). Salienta-se que o regulamento possui extraterritorialidade, vinculando qualquer empresa que ofereça bens ou serviços relacionados à coleta de dados (RÉGIA, 2018).

Apesar de ser uma legislação extremamente relevante e pioneira, também possui fragilidades, vindo a afetar na sua eficácia e aplicabilidade, dentre elas, haverá imposição regional da tecnologia global sendo efetiva restrições de privacidade e inovação por parte dos fornecedores,

tendendo a gerar grandes despesas e incertezas. Outro ponto é que o GDPR pode vir a interferir nas decisões e nos conjuntos de dados armazenados e coletados em *blockchains* – cadeia de blocos e em cada um consta um arquivo e hash, garantindo que as informações desse bloco não foram violadas - privados e públicos emergentes, conforme a Forbes Technology Council (2018). Além disso, beneficia as grandes empresas, pois possuem verba para investir em suas equipes de tecnologia e jurídica para o cumprimento da regulamentação, todavia, as pequenas e médias empresas podem estar menos preparadas e mais vulneráveis a multas e penalidades. Mas também tenderá a reduzir os serviços gratuitos, uma vez que esses utilizam os dados como produto, segundo a Forbes Technology Council (2018).

Deste modo, fica evidente que o alicerce normativo do consumidor, embora sólido e em permanente atualização, também exige a construção coletiva de uma Política Nacional para a Tutela de Dados Pessoais no Brasil, estabelecendo-se metas e compromissos recíprocos entre o Estado, agentes econômicos e sociedade de consumidores.

Em relação ao Estado, espera-se que reassuma seu papel regulador no mercado, através do exercício do poder de polícia fiscalizatório e melhor aparelhamento de órgãos governamentais estratégicos no controle preventivo e repressivo, como no caso da Autoridade Nacional de Proteção de Dados Pessoais.

Os agentes econômicos do mercado deverão aprimorar, sobretudo em suas plataformas eletrônicas, políticas de transparência, privacidade e segurança dos dados pessoais, evitar o assédio de consumo, bem como estimular modelos de *compliance* para corrigir, preventivamente, distorções.

A sociedade de consumidores, por sua vez, deverá seguir um modelo de consumo responsável, em que o exercício qualificado da liberdade de escolha, buscando interagir com companhias idôneas e com histórico positivo e confiável no trato das informações sensíveis dos consumidores, diminuirá o risco pelo uso indevido dos seus dados pessoais.

Essa nova vulnerabilidade algorítmica do consumidor fica evidente em casos como o do vazamento de dados dos usuários do iFood Brasil, os quais foram expostos por erro no aplicativo de delivery no dia 19 de junho de 2020, segundo relatos nas redes sociais. Em tal situação, os sujeitos acessavam o aplicativo e viam pedidos e endereços de outros usuários – o residencial, o comercial, além do histórico de endereços. "Fui olhar e era de um lugar em que eu nunca havia visto antes. Olhei no histórico dos pedidos e percebi que nenhum dos que estavam lá era meu". "Percebendo que havia algo de errado, fui nas outras abas e vi que nenhuma das informações, de endereços, chats iniciados e pedidos, eram minhas. E toda vez que atualiza aparecia uma informação diferente. De diferentes datas e cidades". "Tive acesso também aos endereços dos

perfis que o iFood me atribuía aleatoriamente. Tanto o residencial, comercial e histórico de endereços utilizados. Achei bem perigoso" (FOLHA DE SÃO PAULO, 2020).

Tal situação deixou o consumidor em uma situação de extrema exposição, uma vez que seus dados pessoais foram expostos sem consentimento prévio a terceiros não autorizados, podendo vir a acarretar inúmeros danos, além da situação da perda de confiança, requisito fundamental nas compras online.

Em resposta, a empresa se posicionou por meio de nota, afirmando que tal instabilidade no sistema não decorreu de ataque cibernético e que durou apenas 30 minutos – tempo suficiente para que vários consumidores tivessem os seus dados pessoais expostos e fossem lesados - e que os dados virtuais foram exibidos de forma aleatória, de modo que não era possível que os usuários fizessem pedidos por outras pessoas ou acessassem contas de terceiros (FOLHA DE SÃO PAULO, 2020).

Vê-se, portanto, não apenas que as plataformas não estão preparadas para oferecer uma tutela transparente e segura dos dados pessoais dos consumidores, quiçá terem uma postura ética para reconhecer as falhas, buscando não apenas mitigar os danos, para aprimorar o serviço.

4. AS INFORMAÇÕES OBTIDAS PELO APLICATIVO DE DELIVERY iFOOD

Com o objetivo de compreender como se dá a coleta, tratamento e fluxo de dados do consumidor ao utilizar um aplicativo de delivery foi analisada a política de privacidade do iFood, o qual conforme o Huffpost (2018) é o principal aplicativo de delivery da América Latina. Tal análise da política de privacidade foi realizada com base em cinco perguntas, isto é, quais são os dados solicitados? Como os dados são coletados? Como os dados são utilizados? Como as informações são armazenadas? Como os dados são descartados? De modo que foram encontradas tais informações:

A respeito do primeiro questionamento "quais são os dados solicitados ao usuário?", foram encontrados que são 4 tipos de dados, isto é: a) dados tipo 1 - no ato da inscrição via usuário registrado: nome, data de nascimento, CPF, e-mail, endereço, senha, telefone e preferências de contato; b) dados tipo 2 - no ato da inscrição via redes sociais: Facebook acessa as informações pessoais na conta, ou seja, nome, e-mail, gênero, idade e telefone (as informações obtidas dependem das configurações de privacidade da rede social); c) dados tipo 3 - complementação: dados de Pagamento (caso seja online), informações de localização (a localização fornecida será

considerada como dado cadastral, Lei 12.965/2014, MCI) e informações do dispositivo móvel (endereços IP, tipo de navegador e idioma, provedor de serviços de internet, páginas de consulta e saída, sistema operacional, informações sobre data e hora, dados sobre a sequência de cliques, fabricante do dispositivo, operadora, modelo, redes, Wi-fi número de telefone, entre outras informações que podem ser coletadas); d) dados tipo 4 - dados não-pessoais: idade do usuário, preferências individuais, idioma, CEP e código de área, informações sobre as atividades dos usuários no uso do website ou aplicativo.

Sobre o segundo questionamento, ou seja, "como os dados são coletados?", encontrou-se que há a coleta no ato da inscrição via usuário registrado; no ato da inscrição via redes sociais; durante a utilização do website ou do aplicativo. Acerca do terceiro apontamento, isto é, "como os dados são utilizados (tratamento)?", compreendeu-se que, conforme a política de privacidade, são utilizados para promover, melhorar e desenvolver os serviços; também para efetivar a avaliação de restaurantes; além disso, para efetivar a comunicação entre a empresa e o consumidor – via avisos e notificações; mas também para aprimorar a segurança e melhorar os serviços e as ofertas; para enviar publicidade ou materiais promocionais (podem compartilhar as informações de marketing com parceiros que possuam política de privacidade com níveis de proteção compatíveis com a do iFood, para desenvolver campanhas mais relevantes para interessados); para administrar promoções; e também para a consecução das finalidades previstas na política de privacidade.

Além disso, a respeito do quarto questionamento, ou seja, "como as informações são armazenadas?", encontrou-se que são guardados em serviços de nuvem confiáveis de parceiros. Acerca do quinto apontamento, isto é, "como os dados são descartados?", compreendeu-se que são com a solicitação de exclusão da conta pelo usuário, também que as informações pessoais fornecidas ao iFood durante a utilização dos serviços serão excluídos definitivamente sempre que a legislação assim o exigir. Mas também vem a ser esclarecido sobre o sexto questionamento, ou seja, "como os dados pessoais são protegidos?", encontramos que se dão por meio do *privacy by design*.

Diante disso, compreende-se que a política de privacidade do iFood, versão de atualização de 15 de setembro de 2020 é bem clara e de fácil compreensão por qualquer usuário, de modo que coletar tais dados e analisá-los criticamente para que resultados fossem alcançados não foi uma tarefa árdua, mas sim interessante. Em primeiro ponto, ficou evidente que quatro são os tipos de dados requeridos por parte do iFood e esses fazem toda a diferença para essa empresa, uma vez que inúmeros são os tratamentos – os quais serão explanados posteriormente.

Em segundo ponto, também foi bem explícito como os dados são coletados pelo iFood, isto é, inscrição via usuário registrado – quando o sujeito opta por se cadastrar e preencher um formulário de perguntas pessoais -, via redes sociais – as informações da rede solicitada são direcionadas ao iFood, dependendo das configurações de privacidade do sujeito em relação ao serviço da rede social -, ou durante a utilização do site ou do app - são fornecidos dados de pagamento (para pagamentos online), informações de localização e informações dos dispositivos (endereços IP, tipo de navegador e idioma, provedor de serviços de Internet (ISP), páginas de consulta e saída, sistema operacional, informações sobre data e horário, dados sobre a sequência de cliques, fabricante do dispositivo, operadora, modelo, redes Wi-Fi, número de telefone, entre outras que poderão ser coletadas pelo iFood).

Em terceiro ponto, ficou claro como os dados são utilizados, ou seja, para que os serviços sejam aprimorados, seja efetiva a avaliação dos restaurantes, além de ser efetivo o diálogo entre a empresa e o usuário (via avisos e notificações), mas também para melhorar a segurança e os serviços, além de canalizar publicidade específica ao usuário, administrar promoções e dar prosseguimento nas finalidades previstas na política de privacidade da empresa.

Em quarto ponto, foi notório na política de privacidade como os dados pessoais dos usuários são armazenados, ou seja, em serviços de nuvem confiáveis de parceiros, os quais podem estar localizados no Brasil ou em outros países, os quais forneçam serviço de armazenamento de nuvem confiáveis e usualmente utilizados por empresas de tecnologia, tais como Estados Unidos da América (EUA) e em países da América Latina e da Europa.

Em quinto ponto, frisa-se que também foi claro e evidente compreender como se dá o descarte dos dados do usuário, isto é, por meio de solicitação de exclusão da conta, sendo excluídos definitivamente, sempre que a legislação assim o exigir, as informações pessoais fornecidas ao iFood durante a utilização dos serviços. Todavia, pontos problemáticos foram encontrados: a) em alguns casos, afirmam que podem reter as informações do usuário mesmo que ele exclua a conta, tais como nas hipóteses de guarda obrigatória de registros previstas na lei aplicável, se houver uma questão não resolvida relacionada a conta, ou caso seja necessário para os supostos interesses comerciais legítimos, como prevenção de fraudes e aprimoramento da segurança dos nossos usuários; b) o iFood destaca que poderá realizar transferências internacionais de dados para outros países, tais como Estados Unidos da América e para países da União Europeia e da América Latina, a fim de realizar algumas das atividades envolvidas nos serviços prestados ao usuário, bem como para poder obter informações que possam contribuir para o aperfeiçoamento dos serviços.

Em qualquer caso de compartilhamento com parceiros localizados em outros países, afirmam que estabelecem contratualmente que o parceiro possua padrão de proteção de dados e segurança da informação compatível com a política de privacidade do iFood, a fim de que os dados do usuário sejam sempre protegidos nos termos da política supracitada; c) ademais o iFood também pode compartilhar com terceiros as informações coletadas dos usuários em algumas hipóteses: para outros usuários do iFood; com empresas do Grupo iFood; em alteração de controle societário do iFood; provedores de serviços e outros parceiros; restaurantes parceiros do iFood; serviços de redes sociais e outros provedores de aplicação; para publicidade e serviços de análise; d) em sexto e último ponto, ficou evidente na política de privacidade que os dados pessoais são protegidos contra perda, roubo ou quaisquer modalidades de uso inapropriado, tal como contra acesso não autorizado, divulgação, alteração e destruição, por meio do princípio *privacy by design*, vindo a respeitar e proteger os dados do usuário em todos os processos, com a utilização de técnicas de criptografia, monitoramento e a realização periódica de testes de segurança. Por fim, o iFood destaca que não é possível asseverar totalmente a não incidência de interceptações e violações dos sistemas e bases de dados do iFood, visto que a organização de segurança da internet está em constante aperfeiçoamento.

Sendo assim, compreende-se que a relação de consumo em âmbito virtual é uma questão muito complexa, que envolve muitas variantes e que, mesmo que a política de privacidade da referida empresa seja clara e evidente, não deixa de colocar o consumidor em uma posição de vulnerabilidade extrema, uma vez que os seus dados podem ser exportados e fornecidos a terceiros parceiros da iFood, logo, fazer um simples pedido de comida vem a ser algo complexo.

Também há outro ponto a se destacar, isto é, apesar da política de privacidade ser clara, não significa que os usuários estarão protegidos de um consentimento involuntário, erros, ou mesmo de incidentes de segurança *(Data breach*) por parte dos *gatekeepers*, como esclarecido no decorrer deste artigo.

Em resumo, é preciso aprimorar o controle dos dados através de uma atuação conjunta do Estado, agentes econômicos e coletividade de consumidores.

5. O EMPODERAMENTO DO CONSUMIDOR DIGITAL

Como visto anteriormente, a sociedade de consumidores tem um papel fundamental nesse contexto, exercendo sua cidadania instrumental (VERBICARO, 2019), para melhor ocupar os

espaços políticos deliberativos no combate às práticas abusivas no uso, tratamento e destinação de seus dados pessoais, pelas plataformas eletrônicas.

O exercício da liberdade positiva desse consumidor que se vê como parte integrante de um grupo ressignifica o ideal de solidariedade nas relações de consumo digitais, de modo que por meio de uma nova consciência de união social via internet, tal sociedade deverá se autorreconhecer como heterogênea, complexa, além de tutelar o pluralismo jurídico, visando assim garantir as modificações concretas no comportamento empresarial acerca dos deveres éticos para com o consumidor.

Logo, há de se pensar de que maneira o sujeito pode agir de modo coletivo, vindo a auxiliar na proteção dos dados pessoas, além de vir a se empoderar. Atualmente, existem algumas alternativas nesse sentido tais como os sites de compartilhamento de experiências, como o Reclame Aqui, plataformas de mediação online como o consumidor.gov, as redes sociais, assim como crescente utilização do boicote à empresas que ajam na infralegalidade.

A plataforma Reclame Aqui, com 20 anos de existência – com mais de 26 milhões de casos resolvidos - e com mais de 90 mil empresas cadastradas – dado de 2020 -, informações essas disponíveis no site do Reclame Aqui (2020) conecta consumidores e empresas para auxiliar na resolução de problemas. Além disso, possui uma lista extensa de funcionalidades disponíveis, dentre elas, inclui o ranqueamento das melhores empresas para se fazer negócios, essas categorizadas por setores de serviço ou venda; bem como a disponibilização de estatísticas acerca da resolução das reclamações por cada companhia, como taxa de solução, tempo de resposta e pontuação do atendimento; assim como possui uma lista de reclamações, de um lado a resposta da empresa e, do outro torna claro se o problema foi ou não solucionado (ALMEIDA; CIRQUEIRA; LOBATO, 2017, p. 108).

O Reclame Aqui funciona como mediador entre compradores e os fornecedores, sendo o maior portal brasileiro de reclamações e talvez seja também o maior responsável pelo ciberativismo do consumidor, em conjunto com as redes sociais. Tal plataforma age de forma simples e altamente veloz, assumindo assim o papel do PROCON - órgão oficial de proteção dos direitos do consumidor. Além das reclamações, os usuários podem se informar sobre as opiniões de outros consumidores com relação ao serviço e/ou produto de uma determinada empresa, mas também sobre o seu atendimento para com os clientes. (COELHO, QUEIROZ, CALAZANS et al, 2016, p. 9)

A operação começa com um cadastro rápido do usuário, esse que deve criar login e senha para fazer reclamações ou ter acesso às diversas informações que o site proporciona. De modo que

não são aceitas reclamações anônimas, nem a utilização de apelidos por parte dos usuários, vindo a resguardar a seriedade do ambiente. Todo o sistema é controlado automaticamente pelo site e nenhuma interferência é aceita na interação entre a empresa reclamada e o cliente, vindo a garantir confiabilidade ao processo. O caráter de utilidade pública do Reclame Aqui faz com que as empresas sintam necessidade de tratar todas as questões de forma rápida e satisfatória, com o objetivo de minimizar os danos que podem acontecer em decorrência dos relatos publicados (COELHO, QUEIROZ, CALAZANS et al, 2016, p. 10).

Nesse sentido, fica claro que a relação dos consumidores para com a tecnologia tem ocasionado mudanças na lógica das relações de consumo virtuais. A plataforma Reclame Aqui está sendo uma grande aliada dos sujeitos para cobrar melhorias e posicionamentos por parte dos fornecedores – sendo empoderador -, além de ser um mecanismo de auxílio social, uma vez que um consumidor pode alertar o outro sobre determinada empresa e suas práticas éticas – ou antiéticas.

Destaque-se, também, os sistemas de reputação por estrelas nas próprias plataformas eletrônicas, que impactam diretamente na sua "imagem" perante outros consumidores, influenciando no processo de tomada de decisão. Tais sistemas estimulam a confiança por parte dos consumidores para com os fornecedores, em detrimento das diversas avaliações e comentários produzidos por outros sujeitos sociais. Conforme Filho (2018, p. 45), o sistema de reputação indica ser o substituto possível no mundo on-line para os métodos tradicionais de geração de confiança e de reputação do mundo físico. De modo que no Brasil os sistemas mais conhecidos são E-Bit e o Reclameaqui.com.br.

Por conseguinte, destaca-se que a atuação dos Sistemas de Reputação (SRP) vem a se basear em dois conceitos principais: confiança e reputação. O conceito de confiança define, sob o ponto de vista de um indivíduo, o quanto ele confia em outro indivíduo. Para que um indivíduo seja confiável se faz necessário que ele tenha atitudes positivas (honestas e colaborativas) em relação às entidades que dele dependem. À vista disso, a confiabilidade é a capacidade de um indivíduo ser confiável e a confiança é uma consequência da confiabilidade. A necessidade de se conhecer mais o comerciante antes das tomadas de decisão veio a incentivar a criação de sistemas de reputação, cujos serviços realizam um papel fundamental no contexto contemporâneo do comércio eletrônico atual (LOPES, 2006).

De fato, a própria definição de confiança apresenta versões variadas, que estão relacionadas a diferentes ontologias, uma vez que da perspectiva da psicologia, confiança é definida como "uma tendência de confiar em outros indivíduos"; do ponto de vista da psicologia social, confiança é

definida como "uma cognição acerca da entidade em questão"; já do ponto de vista da sociologia, confiança é entendida como "uma característica do ambiente institucional" (LOPES, 2006, p. 47).

O consumidor.gov é uma plataforma oficial, criada pelo Ministério da Justiça, com o objetivo de mediar a solução de conflitos de consumo, desafogando o Judiciário e estimulando soluções consensadas entre consumidores e agentes econômicos. Todavia, não pode ser usada como sucedânea da jurisdição, ou mesmo como condição prévia à propositura de demandas, pois conquanto seja apreciável investir nos modelos de mediação online, a cultura litigiosa brasileira, a dificuldade de acesso à internet e a hipossuficiência técnica e jurídica da grande maioria dos consumidores, ainda torna essa via alternativa distante e potencialmente prejudicial à uma solução justa e equilibrada do conflito.

Por fim, o boicote de marcas e empresas vem ganhando um maior protagonismo nas relações de consumo, sobretudo no âmbito digital das redes sociais, quando comportamentos ilícitos em relação à pessoas, animais e ao meio ambiente ganham projeção nacional e impactam negativamente a imagem institucional da marca (*branding*), algo que reverbera junto ao grande público consumidor, agora muito mais consciente de como sua liberdade de escolha é decisiva para moldar comportamentos empresariais desejáveis.

É inegável que houve impactos positivos e modificações efetivas no comportamento das empresas acerca dos seus deveres éticos para com os consumidores pelas iniciativas de empoderamento referidas acima, pois favorecem um espaço de discussão prévio entre os sujeitos da relação, como conduzem a uma possível solução alternativa do conflito ao Judiciário, tudo através da construção coletiva do diálogo.

Esse consumidor consciente, ao compartilhar suas experiências, reclamações, sugestões e avaliações tende a gerar mudanças reais na atuação do empresário, uma vez que diante do risco de exposição negativa no âmbito virtual, eventual displicência no atendimento e uma postura refratária a mudanças podem determinar sua irrelevância, ou mesmo desaparecimento no mercado, justamente pela perda de confiança do consumidor e de competividade em reação aos seus pares.

O empresário contemporâneo precisará se reinventar, pois se cada vez mais influenciado pelo valor da marca no ambiente competitivo do comércio eletrônico, devendo assumir uma postura mais responsável, entregando ao consumidor, cada vez mais seletivo, algo além de um bom preço ou condição de pagamento, revelando outras habilidades que criem uma relação de confiança com o cliente, fidelizando-o.

Enfim, não há dúvida que, após a pandemia, haverá uma nova "normalidade nas relações de consumo, motivo pelo qual o consumidor deverá estar atento aos comportamentos predatórios,

reprimindo-os, através das inúmeras ferramentas jurídicas colocadas à sua disposição, como a Lei 8078/90 (Código de Defesa do Consumidor), mas também valorizar iniciativas autenticamente virtuosas no mercado, que ilustram uma nova categoria de fornecedores responsáveis e comprometidos com a vertente identitária do consumo, tão valorizada nesse contexto de crise social e econômica.

6. CONCLUSÃO

O consumidor digital se encontra em situação de vulnerabilidade agravada, haja vista o crescente assédio de consumo, assimetria informacional, consentimento involuntário nos contratos eletrônicos, erros técnicos, as falhas no processo de produção, mas principalmente pelo tratamento inadequado e inseguro de seus dados pessoais.

A coleta e a destinação irregular dessas informações sensíveis acaba sendo utilizada para traçar perfis, criar modelos estético-comportamentais e definir nichos específicos de consumo, comprometendo não apenas a autonomia decisória do consumidor, em razão da influência negativa do assédio de consumo, hoje vedado pelo inciso VI, art. 54-C do Código de Defesa do Consumidor, mas a própria privacidade, pelo suo clandestino de seus dados pessoais na nova perspectiva do capitalismo de vigilância.

Num primeiro momento, preocupou-se em apresentar as novas práticas abusivas quanto ao uso indiscriminado dos dados do consumidor, através do comércio eletrônico, em suas diferentes modalidades, a saber: Business-to-Business (B2B), Business-to-Consumer (B2C), Business-to-government (B2G) e Consumer-to-Consumer (C2C), mas também entender as vicissitudes dessa coleta de informações sensíveis por meio dos aplicativos de delivery, dentre eles, com especial atenção aquela adotada pelo iFood.

Em um segundo momento, abordou-se o novo capitalismo de vigilância, a partir da perspectiva de Shoshana Zuboff, com vistas à acumulação intencional dos dados pessoais, monetizando informações comportamentais, influindo nas escolhas e ações humanas, dando ensejo a uma nova vulnerabilidade sensível do consumidor: a algorítmica.

Abordou-se a tutela normativa dos dados pessoais em perspectiva nacional e internacional, identificando-se o alcance do Marco Civil da Internet (MCI), da Lei Geral de Proteção de Dados Pessoais (LGPD), do Código de Defesa do Consumidor (CDC) e, na seara internacional, do *General Data Protection Regulation* 2016/679 (GDPR), preocupando-se em verificar a eficácia e aplicabilidade das mesmas.

É inegável que a LGPD foi um grande avanço normativo e representa um maior controle dos dados pessoais dos consumidores, mas possui algumas lacunas e imprecisões, precisando de um maior tempo de experimentação social e permanente diálogo como CDC para que seja avaliada sua eficácia.

Por fim, demonstrou-se a importância do empoderamento do consumidor, através do exercício qualificado de sua liberdade de escolha, construindo uma identidade coletiva por meio de sua cidadania instrumental, mitigando os efeitos dessa vulnerabilidade, bem como corrigindo distorções no comportamento empresarial por meio de novas ferramentas de interação social, tais como os sites de compartilhamento de experiências, plataformas de mediação online, sistemas de autoavaliação de qualidade e atendimento, assim como o grande alcance das redes sociais, capazes de influir na relevância ou não de fornecedores no competitivo mercado digital.

REFERÊNCIAS

ALMEIDA, Gustavo R. T. de ; CIRQUEIRA, Douglas Rocha ; LOBATO, Fábio M. F.. Improving Social CRM through eletronic word-of-mouth: a case study of ReclameAqui. In: WORKSHOP DE TRABALHOS DE INICIAÇÃO CIENTÍFICA - SIMPÓSIO BRASILEIRO DE SISTEMAS MULTIMÍDIA E WEB (WEBMEDIA) , 2017, Gramado. **Anais** [...]. Porto Alegre: Sociedade Brasileira de Computação, 2017 . p. 107-110. ISSN 2596-1683.

ANTONIALLI, Dennys; CRUZ, Francisco Brito. **Privacidade e Internet**: desafios para a democracia brasileira. Fundação FHC/Centro Edelstein, 2017.

BEZERRA, André Luís Martins. **A Lei 13.709/18 e os novos desafios da proteção de dados pessoais e identidade**. Trabalho de Conclusão de Curso - Faculdade de Direito do Recife – CCJ - Universidade Federal de Pernambuco - UFPE - Recife, 2019. Disponível em: <https://repositorio.ufpe.br/handle/123456789/36323>. Acesso em: 10 fev. 2020.

BRASIL. Lei nº 8078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**: Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, Seção 1, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em: 06 dez. 2016.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Marco Civil da Internet**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, Seção 1, 24 abr. 2014. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14 jan. 2017.

BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (orgs). **Tecnopolíticas de vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018.

CIO. **Escape das armadilhas da LGPD**, 2019. Disponível em: <https://cio.com.br/escape-das-armadilhas-da-lgpd/>. Acesso em: 15 fev. 2020.

COELHO, Gabriela Rocha Barros; QUEIROZ, Georgina Venancio de; CALAZANS, Janaina de Holanda Costa et al. A consolidação de sites de reclamação online como uma alternativa eficaz no intermédio das relações de consumo: um estudo de caso do site Reclame AQUI 2016. **Portal Intercom**, 2016. Disponível em: <https://www.portalintercom.org.br/anais/nordeste2016/resumos/R52-1828-1.pdf>. Acesso em: 10 de maio de 2020.

DONEDA, Danilo. A Proteção Dos Dados Pessoais Como Um Direito Fundamental. **Revista Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FILHO, Ulysses Pereira Pacheco. **Como o sistema de reputação baseado em avaliação mútua é utilizado por participantes provedores da economia compartilhada?** Tese de Mestrado. Fundação Getúlio Vargas – FGV, São Paulo, 2018.

FORBES, Technology Council. 15 Consequências inesperadas do GDPR. Disponível em:< https://forbes.com.br/negocios/2018/08/15-consequencias-inesperadas-do-gdpr/#foto13>. Acesso em: 17 jul 2020.

FOLHA DE SÃO PAULO. iFood sofre falha e expõe dados de usuários. Disponível em: <https://www1.folha.uol.com.br/mercado/2020/06/ifood-sofre-falha-e-expoe-dados deusuarios.shtml>. Acesso em: 17 mar. 2020.

FREIRE, Daniele Araujo; SALGADO, Érika Baptista. **E-commerce no brasil: panorama geral e principais desafios**. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Federal do Rio de Janeiro – Rio de Janeiro, 2019. Disponível em: < http://www.monografias.poli.ufrj.br/monografias/monopoli10030160.pdf>. Acesso em: 13 mar. 2020.

GUISSONI, L. A.; OLIVEIRA, T. V. de.; TEIXEIRA, T. Um novo momento para o ecommerce. **GV Executivo**, v. 15, n. 1, janeiro-junho, 2016. Disponível em: <https://rae.fgv.br/gv-executivo/vol15-num1-2016/novo-momento-para-commerce>. Acesso em: 21 jan. 2020.

HUFFPOST. Como o iFood se tornou o maior aplicativo de delivery de comida da América Latina. Disponível em: < https://www.huffpostbrasil.com/2018/04/18/como-oifood-se-tornouo-maior-aplicativo-de-delivery-de-comida-da-america-latina>. Acesso em: 15 mai 2020.

FOLHA. iFood sofre falha e expõe dados de usuários. Disponível em: <https://www1.folha.uol.com.br/mercado/2020/06/ifood-sofre-falha-e-expoe-dadosdeusuarios.shtml>. Acesso em: 17 mar. 2020.

IFOOD. Política de Privacidade. Disponível em: <https://www.ifood.com.br/privacidade>. Acesso em: 19 mai 2020.

LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LIPOVETSKY, Gilles. **A Felicidade Paradoxal**. São Paulo: Companhia das Letras, 2008.

MARQUES, Claudia Lima. BENJAMIN, Antonio Herman V. BESSA, Leonardo Roscoe. **Manual de Direito do Consumidor**. 5 ed. São Paulo: Editora dos Tribunais, 2013.

MELO, Iran Ferreira de. Análise do discurso e análise crítica do discurso: desdobramentos e intersecções. **Revista Eletrônica**, v. 05, n. 11, 2009, ISSN 1807-5193. Disponível em: <http://www2.eca.usp.br/Ciencias.Linguagem/Melo_ADeACD.pdf>. Acesso em: 20 jul 2020.

MELO, Lília Maranhão Leite Ferreira de; VASCONCELOS, Fernando Antônio de. As relações de consumo eletrônicas e a proteção do consumidor virtual sob o prisma do código de defesa do consumidor. CONPEDI, p. 01-24, 2012. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=f87e955fd6b89f89>. Acesso em: 20 fev 2020.

MOBILE TIME. Uma análise do conflito entre LGPD e o decreto 10.046. Disponível em: <https://www.mobiletime.com.br/noticias/07/11/2019/o-conflito-entre-lgpd-e-o-decreto-10-046-em-analise/>. Acesso em: 05 jan. 2020.

MONTY, Renata. Consumo de comida por aplicativos. **Comunicon**, v. 03, n. 01, p. 1-14. Disponível em: <http://anaiscomunicon2018.espm.br/GTs/GTPOS/GT2/GT02_MONTY.pdf>. Acesso em: 14 fev. 2020.

OLIVEIRA, Evellin Bianca Souza; ANDRADE, Larisse Silva; SANTOS, Maria Rita. Capitalismo de vigilância: uma discussão filosófica sobre a influência de redes sociais na autoimagem da mulher. **Revista Linguagem em (Re)vista**, vol. 15, n. 30, ago./dez. Niterói, 2020. Disponível em: < http://www.filologia.org.br/linguagememrevista/30/02.pdf>. Acesso em: 10 jan. 2021.

PACHECO GUIMARÃES, Cleber. Análise Crítica do Discurso: Reflexões sobre Contexto em van Dijk e Fairclough. **Eutomia**. v. 1, n. 09, p. 438-457, 2012. Disponível em: <https://periodicos.ufpe.br/revistas/EUTOMIA/article/view/959>. Acesso em 20 jul 2020.

RECLAMEAQUI. Reclame AQUI celebra 20 anos de história conectando empresas e consumidores. Disponível em:<https://noticias.reclameaqui.com.br/noticias/reclame-aquicelebra-20-anos-de-historia-conectando empresas_3871/>. Acesso em: 19 jun 2020.

RÉGIA, Vitória. Principais pontos para entender o regulamento geral de proteção de dados. **Jus** 2018. Disponível em: <https://jus.com.br/artigos/70481/principais-pontos-para-entender-o-regulamento-geral-de-protecao-de-dados-gdpr>. Acesso em: 18 jun 2020.

SILVA, Élvio Ribamar Ferreira Silva. **(In) efetividade do CDC no direito de arrependimento das relações de consumo via comércio eletrônico**. Trabalho de Conclusão de Curso – Fundação Universidade Federal de Rondônia – Rondônia, 2016. Disponível em: <https://ri.unir.br/jspui/handle/123456789/1423>. Acesso em: 17 abr. 2020.

SILVA, Marcelo Pereira da. Problemas sem Solução e Atendimento Ruim. **Intercom**, 2017. Disponível em: < https://portalintercom.org.br/anais/nacional2017/resumos/R12-2443-1.pdf>. Acesso em: 10 de maio de 2020.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet**: uma lei sem conteúdo normativo. Estudos Avançados, v. 30, n. 86, p. 269-285, 2016. Disponível em: <http://www.scielo.br/scielo.php?pid=S010340142016000100269&script=sci_arttext&tlng=pt >. Acesso em: 04 nov. 2019.

VERBICARO, Dennis. **Consumo e Cidadania**. Identificando os espaços políticos de atuação qualificada do consumidor. 2. ed. Rio de Janeiro: Lumen Juris, 2019.

ZUBOFF, Shoshana. **Big Other**: Capitalismo de vigilância e perspectivas para uma civilização de informação. In BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (orgs). Tecnopolíticas de vigilância: perspectivas da margem. São Paulo: Boitempo, 2018.

Recebido em: 19/04/2021
Aprovado em: 13/04/2023

Editor:
Dr. Leonardo da Rocha de Souza

Editoras executivas:
Saskia Assumpção Lima Lobo
Clarice Aparecida Solpesa Peter
Layra Linda Rêgo Pena