

Artigos

DA (IR)RESPONSABILIDADE DOS MECANISMOS DE BUSCAS FRENTE À VULNERABILIDADE DO CONSUMIDOR

THE (IR) RESPONSIBILITY OF SEARCH MECHANISMS AGAINST CONSUMER VULNERABILITY

Bárbara Cristina Kruse¹

Marcos Kruse²

Luiz Alexandre Gonçalves Cunha³

Resumo: A exposição de dados pessoais e sensíveis perante as artimanhas fraudulentas de malfeitores virtuais é uma realidade da pós-modernidade. As relações sociais e comerciais ocorridas no cyberspaço cada vez mais se tornam usuais e frequentes e, com isso, afetam também a ciência jurídica. Apesar das facilidades do mundo pós-moderno, as novas tecnologias também abrem brechas para golpistas, os quais se utilizam da vulnerabilidade do consumidor para angariar grandes quantias financeiras mediante ato ilícito. Dada a contextualização, o objetivo do presente artigo se faz na análise da responsabilidade civil quanto as questões consumeristas atreladas aos mecanismos tecnológicos de buscas digitais. A metodologia de pesquisa utilizada é a qualitativa baseada na revisão de literatura, busca documental e jurisprudencial. Utiliza-se a abordagem lógico-dedutiva que parte de premissas genéricas afim de particularizar o conhecimento. A presente reflexão se mostra importante para os operadores do Direito e cientistas sociais, ao passo em que se roga pela proteção do mais vulnerável da relação negocial, conforme os cânones do Código de Defesa do Consumidor (CDC).

Palavras-chave: Responsabilidade objetiva. Consumo. Golpes. Ato ilícito.

Abstract: The exposure of personal and sensitive data to the fraudulent tricks of cyber criminals is a reality of post-modernity. The social and commercial relationships that occur in cyberspace are becoming more and more common and frequent and, therefore, also affect legal science. Despite the facilities of the post-modern world, new technologies also open loopholes for scammers, who use the vulnerability of the consumer to raise large amounts of money through an illicit act. Given the context, the purpose of this article is to analyze civil liability regarding consumer issues linked to technological mechanisms of digital search. The research methodology used is qualitative based on literature review, documental and jurisprudential search. It uses the logical-deductive approach that starts from generic premises in order to particularize the knowledge. This reflection is important for legal practitioners and social scientists, while it pleads for the protection of the most vulnerable in the business relationship, according to the canons of the Consumer Defense Code (CDC).

Keywords: strict responsibility. Consumer. scam sites. unlawful act.

¹ Doutoranda em Ciências Sociais Aplicadas pela Universidade Estadual de Ponta Grossa (UEPG). Mestre Gestão do Território (UEPG). Especialista em Direito Aplicado EMAP-PR. Advogada, bacharel em geografia e licenciada em história.

² Doutorando em Direito pela Universidad Nacional de Lomas de Zamora (UNLZ). Bacharel em Direito (UEM), Economia (UEM) e Teologia.

³ Doutor em Ciências Sociais pela UFRRJ. Mestre em História Economia. Graduado em Geografia. Professor Associado da UEPG e Diretor do Setor de Ciências Exatas e Naturais-SEXATAS.

Artigo recebido em: 24 set. 2021 – Artigo aprovado em: 16 dez. 2021.

1 Introdução

A questão discutida deriva de novos *approaches* tecnológicos. Considerando que o mundo contemporâneo não é mais o mesmo daquele que exurgiu do iluminismo e suas revoluções industriais é que se considera adequada a nomenclatura pós-modernidade. Nesta pós-modernidade, aponta Stuart Hall (2001), a fragmentação da identidade moderna e o descentramento do sujeito. A pós-modernidade do século XXI, tem a ver com uma geração que nasce no bojo de um mundo digital, cibernético e totalmente tecnológico. As relações socioespaciais, neste sentido, estão em constante transformação e isto se reflete também nas questões normativas. Conforme os pressupostos analíticos de Milton Santos (2010), o mundo globalizado dimanou em relações rápidas e fluídas dando a impressão que o tempo se contraiu. Ademais, a capacidade das notícias fluírem instantaneamente para o mundo todo afeta incomensuravelmente a ciência jurídica.

Constantemente, novas relações espalhadas pelo *cyber* espaço afetam as leis e as relações sociais. Aponta Milton Santos (2006, p. 90) "a vida em sociedade se complicou ao extremo nestes últimos decênios, desafiando a hermenêutica, vistas as numerosas figuras novas introduzidas no conjunto das relações sociais". Assim, diante de novas ferramentas e inovações diárias, o Direito se torna insuficiente em algumas situações por não conseguir oferecer o necessário respaldo da justiça em tempo hábil.

Essa reflexão inicial se mostra importante para o objetivo do artigo, qual seja a análise da responsabilidade civil nas questões consumeristas atrelada aos mecanismos tecnológicos de buscas digitais. A constatação dessa lacuna jurídica se faz no bojo das relações comerciais contemporâneas, ao passo em que cada vez mais transaciona-se pela *internet* (em especial em um mundo pandêmico). A forma com que os mecanismos de buscas induzem o consumidor e o direcionam para determinadas lojas entre as quais é possível encontrar fraudulências, é que se pontua nesse artigo.

Trata-se de um assunto pouco explorado pela doutrina, porém imperioso no contexto jurídico do mundo atual já que as novas sofisticções não apenas vieram para a

comodidade e o bem das pessoas, mas como também e de forma muito significativa, para a proliferação de fraudes e ardilosos golpes. Defende-se, portanto, urgente remodelação da responsabilidade civil, especialmente considerando a vulnerabilização do consumidor perante maliciosas artimanhas tecnológicas.

A metodologia utilizada é qualitativa exploratória, fazendo-se uso da revisão de literatura, legislação e jurisprudência. Utiliza-se também, a abordagem lógico-dedutiva que parte de premissas genéricas a fim de particularizar o conhecimento. Propõe-se o reflexo da discrepância entre aqueles que detém o conhecimento das tecnológicas da informação e a vítima lesada, ora consumidora já que o Direito, conforme os princípios do Código de Defesa do Consumidor (CDC) deve zelar pela proteção do mais vulnerável.

2 Propaganda e novas tecnologias

Segundo apontam os sociólogos Gilles Lipovetsky e Jean Serroy, vivemos em um capitalismo artista em que ganha os holofotes precisamente aquele que mais se destaca perante os demais. O destaque se duplica. A estilização e a estetização do mundo contemporâneo são padrões impostos por uma cultura capitalista estética de massa, tanto por novos valores celebrados (entretenimento, games, divertimento, moda, ludismo e assim por diante), quanto através da propagação de bens materiais, tendências e símbolos difundidos e voltados para a aquisição. Por esse motivo, os pensadores já citados afirmam que “o universo industrial e comercial foi o principal artífice da estilização do mundo moderno e da sua expansão democrática” (LIPOVETSKY & SERROY, 2015, p. 30).

Este novo capitalismo se articula voltando-se para o induzimento do consumo, independentemente das reais necessidades humanas já que se trata de consumo em relação a apetites imaginários. O fetichismo da mercadoria, tal como Marx ponderara no século XIX, faz com que o produto posto na prateleira do mercado oculte as forças produtivas e as contradições da reprodução do capital (MARX, 2020). O produto em exposição no mercado, a mercadoria, vai aparecer como pronto e acabado, escondendo todo o esforço de sua

produção, desde a matéria-prima, quanto o da produção, custo ambiental, ou ainda, da relação de trabalho ali estabelecida. O consumidor, ao comprar determinado produto, compra-o de forma automática e sem se indagar o modo como se deu o processo de produção e apropriação do que foi produzido.

A propaganda, neste sentido, nada mais é do que outro “truque” da reprodução do capital. Através da propaganda, induz-se o desejo, a vontade, bem como irreleva a preeminência da necessidade do item. Ora, é claro que existe uma minoria da população que estuda os perfis, analisa os comportamentos e executa as ações em todos os níveis, inclusive o mercadológico (CHOAMSKY, 2014). É através dessa minoria que se impõe um padrão de consumo que se pode chamar ideológico. A propaganda funciona aí como recurso eficaz de imposição de um protótipo e também como ferramenta de persuasão quanto ao que se deve vestir, comer, calçar, que novo brinquedo se deve brincar, e a nova onda do momento.

De modo efetivo, a grande maioria das armadilhas da publicidade, no contexto deste novo mundo tecnológico, estão inseridas na *internet*, a qual cada vez mais vai se tornando um nicho rentável e de reprodução do capital.⁴ A virtualidade das relações sociais, abarcou também as transações financeiras, eis que é muito mais cômodo comprar *on-line* do que deslocar-se até a loja física. E mais, além do transtorno de não achar determinado produto, não ter muitas opções, ou ainda, ter que recorrer a vários deslocamentos para conseguir comparar preços, é fato que o comércio eletrônico ganhou amplitude incomensurável nos últimos anos.

3 Da utilização para golpes e fraudes

O grande imbróglio de se viver num mundo altamente tecnológico é que tais facilidades e rentabilidades, também promovem a abundância de malfeitores que aguardam

⁴ A referência fundamental quanto ao futuro é de Snider e Ziporyn (2008) que apontaram, em artigo de 1992, que a internet traria uma revolução completa no modo como as pessoas haveriam, de comprar as coisas no futuro. De fato, as previsões destes autores se confirmaram e até foram superadas com o advento da manipulação de enormes bancos de dados com o explícito objetivo de induzir e fomentar vendas.

as oportunidades e as falhas informacionais, para agirem e aplicarem golpes ingentes. Após a concretização da lesão do consumidor, se torna até simplificado golpistas sumirem, deixando poucos rastros ou ainda, deixando vestígios difíceis de serem descobertos a tempo de ressarcir as vítimas acometidas por ato ilícito. A questão que se pontua no artigo retrata *sites* com aspectos idôneos, supostamente pertencentes a lojas fidedignas e com todas formalidades visivelmente preenchidas, mas que na verdade são o início de uma cilada.

Porém, ao indagar-se alguém sobre os mecanismos de inserção neste mundo paralelo em que se faz presente a criminalidade, como é possível que os usuários cibernéticos encontrem tais sites? A resposta, na verdade, é até simples. Os consumidores são conduzidos e levados para o universo das armadilhas que lhes são preparadas. A verdade é que, não fossem os mecanismos de buscas, tais como o *Google, Yahoo, Bing* e assim por diante, *sites* que jazem no universo da criminalidade jamais seriam encontrados. Isto porque, existem tantas lojas e tantas opções, que, sem a ativa condução do consumidor, este teria dificuldades de encontrar a armadilha que lhe foi preparada. Ora, se existe uma infinidade de lojas e comércios eletrônicos, como é que aquele específico site fraudulento aparece entre os primeiros nos resultados da pesquisa virtual?

É a publicidade paga a forma mais rápida e certa de induzir a pesquisa cibernética. Anúncios golpistas são preparados e pagos para que apareçam no topo das buscas e isto com o preciso objetivo de atrair vítimas para aplicação de golpes. Mediante o pagamento, portanto, chega-se ao topo da visibilidade e induz-se o consumidor para que seja “abatido”. Parece cruel, porém a realidade é perversa com as vítimas de tais armadilhas que vulneravelmente se encontram diante de um simulacro de matiz criminoso.

A questão que se aborda é que, sendo o consumidor lesado, isto se dá pela condução para o engano, sendo que esta condução se faz como serviço remunerado pelos golpistas. Logo, não se pode falar que o *Search Engine Optimization* ou *SEO* (Otimização dos Mecanismos de Buscas), que é conjunto de técnicas pagas para que o site fraudulento esteja em evidência, seja inocente. Mais do que o *SEO*, os patrocínios de supostas lojas em *instagrams* e *facebooks* são comuns e amplamente divulgados.

Surge, em decorrência, a imperativa indagação de se saber se existe plausibilidade pretender que tais mecanismos sejam desonerados de responsabilidade. É possível, de fato, imaginar que a condução, que o caminho eleito por determinado guia até uma emboscada seja ato juridicamente irresponsável? Ainda, é possível pensar em irresponsabilização jurídica se a emboscada somente se dá se determinado caminho for trilhado?

A exposição de vulnerabilidade do consumidor na espacialidade virtual é de monta. Os mecanismos de busca acabam facilitando, direcionando, levando o comprador à situação em que será atingido por dano. Pela configuração normal do Direito, a persuasão do consumidor a determinado site fraudulento acaba ficando impune ainda que o meio necessário para a aplicação do golpe e tenha auferido remuneração para conduzir a vítima. Trata-se, em tal caso, de séria lacuna doutrinária e jurisprudencial acerca do caso, eis que, a irresponsabilização de tais facilitadores e mecanismos de busca na condução até empreendimentos fraudulentos ocasionam prejuízos que não se remediam a quem foi lesado.

4 Ofertas Golpistas

Sites recentes e até mesmo desconhecidos aparecem nos mecanismos de busca e pesquisa da *Google* e no topo da navegação cibernética graças as técnicas de *SEO*:

A prática de colocar sites maliciosos na busca é chamada de "SEO blackhat". O termo tem sua origem na união das palavras Otimização para mecanismos de busca (Search Engine Optimization – SEO) e blackhat (chapéu preto) – o termo usado para definir hackers maliciosos. "SEO" é um termo comum no mercado de desenvolvimento e manutenção de sites para qualquer técnica que tente melhorar a posição de um site nos sites de busca. Nem todo "SEO" é malicioso. Na verdade, alguns são benéficos, porque melhoram os resultados de busca para o usuário, colocando as páginas web mais relevantes para uma pesquisa em posições de destaque. O SEO blackhat é um uso distorcido dessas técnicas. O objetivo é colocar páginas irrelevantes em locais privilegiados dos resultados de pesquisa. Os criminosos fazem isso para colocar sites não apenas irrelevantes, mas maliciosos, nos primeiros resultados de pesquisas (ROHR, 2010, s.p).

De acordo com Cunha (2021, s.p) “A receita é sempre a mesma: com documentos verdadeiros, a quadrilha abre uma empresa, com CNPJ e tudo, para vender eletrônicos na internet”. Depois de um tempo, a quadrilha para de operar e “foge com o dinheiro de todo mundo e os consumidores ficam a ver navios. Semanas depois, os mesmos golpistas abrem outra empresa, com outro CNPJ e repetem tudo igualzinho, impunemente” (Ibid.). Até mesmo selos de segurança são falsificados, como o Reclame Aqui:

É isso que vem acontecendo no e-commerce brasileiro. De setembro para cá, pelo menos 2.700 pessoas caíram em fraudes como essa, conforme dados do Reclame Aqui referentes aos sites SigaOfertas.com e OfertaExpressa.com – o primeiro com sede em Goiânia e o outro, em Campinas. Só no Estado de São Paulo, segundo o Procon-SP, o número de reclamações de consumidores que compraram e não receberam (de diversas empresas) passou de apenas duas, em todo o ano passado, para 135 de janeiro a 30 de abril deste ano. “Esse é um tipo de crime que está cada vez mais recorrente”, diz Felipe Paniago, diretor de marketing do Reclame Aqui (CUNHA, 2021, s.p).

Preços atrativos do site fraudulento muitas vezes são um chamariz para a vítima. Ofertas são lançadas diariamente e o preço um pouco abaixo da concorrência por si só não tem o condão de permitir a identificação de um possível golpe. O problema pontuado no artigo é que diversos sites, como por exemplo: Oferta expressa, *Free Shop* Informática, *New Best Shop*, Siga Ofertas, 123 Importados, *Compufree*, *Aquarius*, CeRural, dentre muitos outros, apareciam entre os primeiros nos mecanismos de buscas ou de comparação de preços utilizados (PROCON-SP, 2021). Na explicação de Altieres Rohr (2021, s.p), golpistas vem contratando os serviços da “plataforma de publicidade do Google para impulsionar sites falsos aos primeiros resultados de buscas (...)”. Trata-se, portanto, de sites falsos que muitas vezes não possuem lojas físicas, produtos ou estoque⁵. Deste modo, as técnicas de impulsionamento pagas acabam fazendo com que sites recém colocados na *internet* permaneçam no topo e com maior visibilidade.

⁵ Ou ainda, de início, alguns sites operam da forma correta, ou seja, entregando as mercadorias adquiridas. Porém em pouco tempo e após atingir certa credibilidade, o site começa a atrasar os pedidos até sumir completamente (CUNHA, 2021).

Nas buscas, dá-se o caso de *links* redirecionados pelos mecanismos, os quais induzem o consumidor ao golpe. O caso diz respeito a golpes confeccionados por especialistas da *internet*, que disponibilizam telefones para contato, e-mail de suporte, supostos endereços físicos e, alguns, até mesmo CNPJ que pode ser verificado.⁶ Outros, inclusive, até mesmo nota fiscal emitem após a confirmação de pagamento. Os golpistas conseguem dinheiro fácil e em grande volume em curto lapso temporal e posteriormente “somem” do meio cibernético⁷. Com isso, desaparecem também os canais de atendimento da loja e também qualquer vestígio do mesmo. Engana-se, no entanto, que é somente o consumidor leigo e desavisado que cai nesse tipo de golpe dada sua sofisticação e formas convincentes de defraudar vítimas (CUNHA, 2021).

Neste contexto, a paga da publicidade, por se dar em mecanismos de buscas acomete na irresponsabilidade no evento fraudulento. Entrementes, é perfeitamente possível que os mecanismos de buscas fomentem a desenvoltura de dispositivos ou utilizar-se de tecnologias já existentes no intuito de averiguar a credibilidade de *sites* que anunciam nos seus espaços (como por exemplo confirmação da identidade e dados daquele do anunciante). A indagação, portanto, ocorre no (des)interesse dos mecanismos de buscas em disponibilizar algo que possa atravancar algo que envolve grande aporte financeiro. O que se vislumbra, portanto, é que este tipo de checagem e informação não corresponde aos interesses comerciais das empresas que oferecem este tipo de disponibilização prioritária da veiculação da propaganda.

Segundo o Relatório da Segurança Digital no Brasil⁸, realizado pela empresa Dfndr-lab, no ano de 2018, em uma amostragem de 35 mil pessoas, evidenciou-se que 64,6% dos

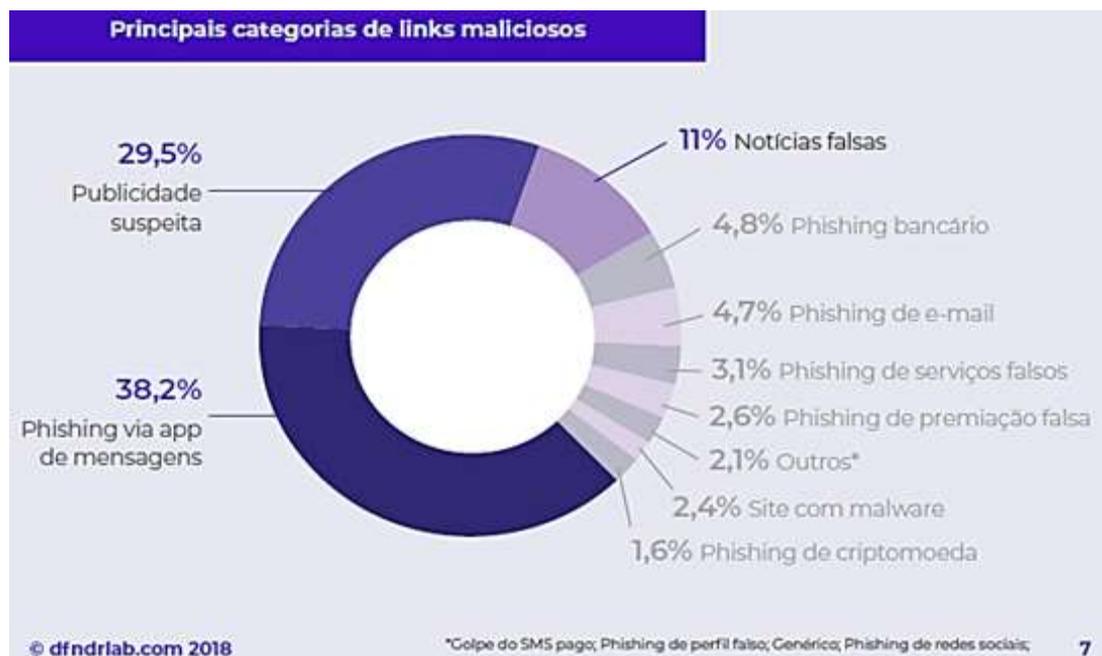
⁶ É o caso mencionado na reportagem do Fantástico “Quadrilha que usava sites falsos de compras”, disponível no youtube: <https://www.youtube.com/watch?v=i_fc41-bzh8>, acesso em 12 setembro 2021.

⁷ Na reportagem da Uol, por Lilian Cunha (2021), em entrevista com profissionais do Reclame Aqui, Felipe Paniago mencionou que os sites golpistas seguem uma espécie de receita de bolo: “Eles seguem esse modelo para atrair mais gente. Muitos até pagam anúncios na internet. Posam de bonitinhos até atingirem um certo faturamento. Depois de terem faturado o que queriam, as empresas somem com o dinheiro do consumidor, sem ter entregado boa parte do que venderam. No caso de Goiás, os sócios da Siga Ofertas sequer constituíram advogados para responder à ação judicial. Simplesmente ignoraram o fato de estarem sendo processados”. Já para Valquírio Cabral Junior, esses golpistas “dificilmente vão ser punidos. A Justiça é muito lenta e esse pessoal é rápido”.

⁸ “O Relatório da Segurança Digital no Brasil é produzido pelo dfndr lab, laboratório de cibersegurança da PSafe, que utiliza técnicas de inteligência artificial e *machine learning* e conta com um time de especialistas em segurança digital.

brasileiros já foram impactados por informações falsas. Além disso, a pesquisa demonstra a amplitude das informações tecnológicas, pois 1 em cada 5 brasileiros já foi potencialmente alvo de *cyber* ataques. Destaca-se, ainda, o número de quase 30% dos *links* maliciosos estarem em publicidades suspeitas:

Figura 1: *Links* maliciosos conforme o Relatório de Segurança Digital no Brasil:



Fonte: Dfndrlab, 2018, p. 7

Para Andrea Fernandes, presidente do Movimento Compre & Confie, “falta uma regulamentação ao mercado nacional de comércio eletrônico” (CUNHA, 2021, s.p). Além disso, o Relatório demonstra um espraiamento da publicidade permitida pela *internet*, inclusive como algo em constante crescimento. A estimativa da PSafe é que em 2021, 150 milhões de brasileiros foram vítimas de golpes virtuais (BRÊTAS, 2021). Deste modo, está se falando de uma sistemática de fraudes em larga escala que se processa pelo uso intensivo

Os dados do relatório são gerados pelas detecções de ciberataques aos smartphones Android dos mais de 21 milhões de usuários do aplicativo de segurança dfndr *security*. Por meio de uma aplicação pioneira da tecnologia anti *hacking*, o app é capaz de checar links maliciosos em aplicativos de mensagens e redes sociais e identificar se pode ser golpe ou *fake news*. Atualmente, o dfndr *security* é o principal aplicativo de segurança para smartphones que alerta sobre notícias falsas, sendo também o único meio de gerar dados sobre a circulação deste tipo de conteúdo em aplicativos de mensagens” (DFNDRLAB, 2018, p. 6).

da tecnologia e que são dificultosas as formas efetivas de reparação do dano nas vias práticas forenses. Conforme aponta a entrevista realizada por Pedro Zambarda (2013) com um advogado atuante nesse tipo de imbróglio:

Em caso de empresas falsas criadas apenas para arrecadar dinheiro com calotes, Dori Boucault recomenda que a pessoa faça denúncias à Polícia Civil, para promover investigações. “Mesmo com as autoridades, vai ser difícil achar essas empresas no mundo virtual. Se ela for mesmo de fachada, fica tudo mais difícil para que você recupere seu dinheiro perdido” (ZAMBARDA, 2013, s.p).

A reportagem disponibilizada pelo *Youtube* apresentada pela “Record TV Goiás”, menciona o caso da fraude do site “Siga Ofertas” que foi tirado do ar e que vendia produtos, mas, não os entregava. O delegado responsável pela operação menciona que são inúmeras vítimas. O que ainda chama atenção na reportagem é a entrevista com aqueles consumidores que compraram os produtos, mas nunca receberam, eis que eles mencionaram que “parecia uma loja idônea”, “uma loja que tinha CNPJ”, “a loja estava no topo do Google;⁹ havia “facilitação de acesso no chat” (RECORD TV, 2020, s.p).

Outra questão pontuada, é o fato de as empresas não possuírem prévias reclamações ou qualquer outra evidência de fraude até que ocorria o sumiço da empresa do mundo virtual. Isto pois, dá-se o caso de empresas que ficam apenas poucos meses *online*, até alavancarem grandes quantias de dinheiro como preparação para a fuga. É o caso, por exemplo, da empresa *Compufree* que antes da fuga *online* possuía nota ótima (9,0) no Reclame Aqui e 93,3% de reclamações respondidas e resolvidas (SOUZA, 2021). As reclamações negativas e de não recebimento do produto somente passaram a ocorrer após o sumiço virtual da empresa, momento em que o golpe perante aquele que efetuou uma compra já havia se consumado (CUNHA, 2021)¹⁰. Tratam-se, assim, de crimes contra o

⁹ Uma das vítimas menciona aos 3:55 minutos do vídeo supracitado da Record TV, a questão de o site estar no topo do mecanismo de buscas.

¹⁰ No judiciário e até mesmo no Procon, os entraves da responsabilização já começam pela citação, pois o endereço pode não mais existir ou pode constar na Carta para citação (via A.R) “*mudou-se*”. Ademais, encontrar o suposto administrador também é difícil pois contumazmente o golpista se utiliza de identidade falsa ou de outra pessoa (laranja). O bloqueio das contas bancárias, geralmente se faz frustrado, eis que os golpistas sacam ou transferem a

consumidor, os quais são cometidos com a cumplicidade indireta e irresponsável dos mecanismos de busca.

Ainda que as proteções legais ao consumidor estejam previstas nas normas, inclusive na Lei nº 12.965 de 2014, que aborda sobre o uso da *internet* no país e assegura a aplicação das normas consumeristas para as relações executadas na plataforma on-line, conforme o artigo 7º, XIII, (BRASIL, 2014), pode-se dizer que existe uma lacuna doutrinária e jurisprudencial quanto a responsabilidade dos mecanismos de buscas e dos anúncios pagos exibidos por estes. Lacuna, no entanto, não significa a inexistência de julgados, mas sim apontar a não incidência de responsabilidade daquele que foi o “fio condutor” ao evento danoso. O que se pontua, deste modo, é a falta de homogeneidade decisória acerca do tema, bem como na ausência da consciência jurídica em relação ao mesmo.

A Apelação do Tribunal de Justiça do Estado de São Paulo, 1011391-95.2015.8.26.0005, de junho de 2016, evidencia que é possível responsabilizar o provedor de aplicações quanto ao conteúdo ilícito:

AÇÃO DE OBRIGAÇÃO DE FAZER C/C PEDIDO DE INDENIZAÇÃO Empresa autora que postula a exclusão de site fraudulento criado em seu nome na Internet para venda de mercadorias, e a reparação dos danos morais sofridos Sentença de extinção do feito sem resolução de mérito, sob o argumento de que o Google não tem legitimidade *ad causam* passiva. Desacerto Réu, na condição de provedor de aplicações, é parte legítima para responder pelos pleitos decorrentes de conteúdo ilícito gerado por terceiros, nos termos do Marco Civil da Internet e da anterior jurisprudência consolidada Possível o julgamento desde logo do mérito da lide pelo Tribunal, nos termos da legislação processual civil aplicável Ação parcialmente procedente Pleito cominatório formulado perdeu o objeto, diante da retirada espontânea do conteúdo ilícito da Internet por terceiro. Pedido de indenização por danos morais que, contudo, comporta acolhida Possibilidade de responsabilização do requerido, na condição de provedor de aplicações, pelo conteúdo ilícito

totalidade do montante arrecadado pelo esquema ilícito no preparo da fuga. Na prática, o próprio judiciário tem dificuldades de perceber o montante financeiro do golpe aplicado porque pressupõe relações interpartes. Isto vale dizer que o judiciário não consegue encontrar ferramentas para transcender a relação jurídica entre golpista e consumidor mesmo que o golpe se aplique contra os consumidores de forma massiva. É similar o caso do uso de notícias inverídicas transmitidas massivamente por redes de comunicação social a exemplo das notícias vinculadas à *fake news* eleitorais (incluindo aqui o *kit gay*). Este problema que originalmente foi deixado de lado continuou a tomar vulto e o próprio STF, por meio do inquérito das *fake news* entendeu que não é possível ignorar o poder destrutivo do ilícito veiculado sob forma massiva.

gerado por terceiros e disponibilizado na Internet, em virtude de sua inércia após o recebimento de notificação extrajudicial do lesado Jurisprudência anterior do C. STJ já vinha se posicionando nesse sentido Previsão do art. 19 da Lei n. 12.965/14, no sentido de que o provedor de aplicações só pode ser responsabilizado civilmente por ato de terceiro após o descumprimento de ordem judicial específica determinando a remoção de conteúdo ilícito, não deve ser interpretada literalmente, pena de ser considerada inconstitucional Danos morais à autora decorrentes da ofensa à sua imagem, seu bom nome e seu conceito social Pessoa jurídica passível de sofrer prejuízos de ordem extrapatrimonial Inteligência da Súmula 227 do STJ. Devida a fixação da indenização em R\$ 30.000,00, valor este que bem atende às funções ressarcitória e punitiva da reparação Ação parcialmente procedente. Recurso parcialmente provido.

(TJ-SP - APL 1011391-95.2015.8.26.0005 SP 1011391-95.2015.8.26.0005, Relator: Francisco Loureiro, Data de Julgamento: 07/06/2016, 1ª Câmara de Direito Privado, Data de Publicação: 07/06/2016).

Apesar da decisão poder ser considerada certa ainda existe a lacuna prática da decisão, na medida em que somente considera o recaimento da responsabilidade ao mecanismo de busca previamente notificado para a exclusão de conteúdos ilícitos. Aliás, a indagação quanto a efetividade da necessidade dessa notificação é legítima, eis que não se coage a ação prévia do buscador, ou seja, antes do anúncio ou do redirecionamento do *link* golpista. Ora, depois do dano perpetrado a notificação por si só se faz, muitas vezes, ineficaz.

Assim, a decisão do TJ-SP acima mencionada, pode-se dizer que continua fomentando seu uso para a execução do crime, pois só se incidirá a culpa após a notificação. Não se trata apenas de um meio de informação, mas sim do pagamento de publicidade e técnicas de *SEO* para que a vítima chegue até o golpe. Diante do elencado, indaga-se se é válido dizer que qualquer conteúdo pode ser veiculado já que se trata de propaganda paga, ainda que se induza a fraudes?¹¹

Por certo, tal situação de ilícito massivo não está contemplada pelos princípios da boa-fé e transparência da publicidade, tampouco zela-se pela publicidade adequada, clara

¹¹ A pressão social formatou a necessidade de se coibir a publicidade de *ilícitos* flagrantes, a exemplo das propagandas de cunho sexual. Todavia, a evidência da propaganda massiva de *fake news* e a condução das massas para resultados desejados pelo direcionamento da propaganda mostra que não é possível deixar as coisas como estão (EMPOLI, 2019). A condução das massas se dá também nas questões políticas situação que demanda a enérgica tomada de posição até para a salvaguarda da democracia como valor político a ser mantido.

e precisa, conforme o estabelecido no CDC (BRASIL, 1991). Trata-se sim, de anúncio enganoso, que não reflete a verdade e nem a lisura do que se está anunciado. A questão que deve ser levantada é como coagir os mecanismos de buscas a adotarem medidas de segurança visando antever o dano e vítimas?

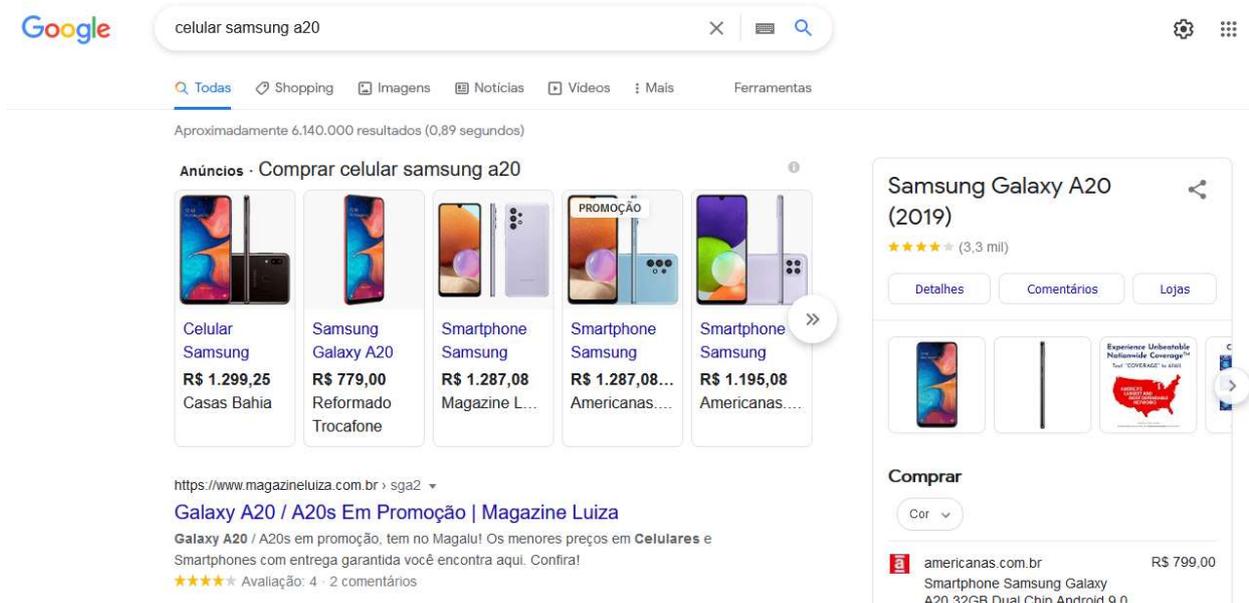
Uma forma eficiente de reparar a vítima, bem como de constranger a empresa na adoção de mudanças quanto à segurança do que se anuncia dar-se-ia pela aplicação da responsabilidade objetiva, ou seja, na comprovação do dano e do nexo causal. Tal responsabilidade poderia recair solidariamente na demanda judicial, tanto para *site* golpista quanto ao mecanismo de busca. A comprovação do nexo causal poderia se dar, de maneira simples, com um *print screen*, por exemplo, do *link* fraudulento aparecendo no topo das buscas e nos locais de anúncio.

A aplicação da inversão do ônus da prova, facultada no CDC em casos de verossimilhança das alegações ou hipossuficiência do consumidor (TJDFT, 2020), também seria válida e importante na lide, pois, assim, sobre o mecanismo de buscas recairia o ônus da comprovação de que não houve o pagamento publicitário daquele *link* redirecionado exclusivamente à lesão. Há de se mencionar também, a dificuldade do consumidor no conjunto probatório, eis que todo o aparato tecnológico, informacional e de publicidade pertence exclusivamente aos mecanismos de buscas, o que por si só aponta a hipossuficiência do consumidor:

(...) A hipossuficiência deve ser aferida pelo juiz no caso concreto e, se existente, poderá fundamentar a inversão do ônus da prova (CDC, art. 6º, VIII). É possível, por exemplo, que em demanda relativa a cobranças indevidas realizadas por operadora de telefonia celular, o juiz determine a inversão do ônus da prova tendo em vista a hipossuficiência do cliente (não é razoável exigir do consumidor a prova de que não fez determinadas ligações. É razoável, por outro lado, exigir da operadora semelhante prova. É preciso, para deferir a inversão, analisar a natureza do serviço prestado, o grau de instrução do consumidor, etc.). A hipossuficiência diz respeito, nessa perspectiva, ao direito processual, ao passo que a vulnerabilidade diz respeito ao direito material. Já a presunção de vulnerabilidade do consumidor é absoluta. Todo consumidor é vulnerável, por conceito legal. A vulnerabilidade não depende da condição econômica, ou de quaisquer contextos outros (BRAGA NETTO, 2014, p. 472).

Para ilustrar o que se argumenta, veja-se a seguinte situação: uma rápida busca no mecanismo de busca *Google*, fez com que em 0,89 segundos mais de 540 mil resultados surtissem. De 540 mil resultados, os que aparecem entre os primeiros não foram colocados de forma aleatória, mas sim mediante o pagamento publicitário. Logo, a vítima ao adentrar em um *site* desconhecido por ela, a título exemplificativo o “Reformando Trocafone”, isso só se faz possível graças ao induzimento do mecanismo de busca. Na verdade, o mecanismo de busca é a causa de o consumidor adentrar no site, bem como a sua motivação para um possível dano. Tal situação não pode ser desconsiderada quando se incide nas relações de consumo:

Figura 2: Pesquisa de Celular no *Google*



Fonte: *Google.com*

A vítima, no caso prático, utilizou-se de um serviço disponibilizado pelo mecanismo de busca e ainda que o mesmo aparente ser ofertado de forma gratuita, a verdade é que a transação comercial no meio cibernético permanece invisível ao usuário comum, assim como o fetichismo da mercadoria para Marx. A questão, portanto, é profunda e deve ser

posta a crítica e a reflexão dos operadores do direito, doutrinariamente, juridicamente e, também, legalmente.

Atualmente, com toda a normatividade acerca dos dados lançados online, faz-se ainda necessário um controle nos conteúdos pagos e anunciados na internet. Evidentemente que se trata de assunto complexo. Uma pesquisa realizada pelo grupo de defesa dos direitos do consumidor, "*Witch*", no Reino Unido, aponta que *Google* e *Facebook* possuem dificuldades em banir anúncios falsos:

Segundo Adam French, especialista em direitos do consumidor da "*Which?*", as descobertas mostram que tanto o Facebook, quanto o Google, deixaram seus usuários "preocupantemente expostos a golpes", e sugeriu que o governo do Reino Unido apresentasse uma legislação para eliminar o problema. "As plataformas online devem ter a responsabilidade legal de identificar, remover e prevenir conteúdo falso e fraudulento em seus sites", disse ele. "Incluir golpes na Lei de Segurança Online é algo urgente e o governo precisa agir agora."

Como parte da proposta de Lei de Segurança Online do governo britânico, as empresas de tecnologia que permitem aos usuários postar seu próprio material ou falar com outras pessoas online podem ser multadas em até 18 milhões de libras (cerca de R\$ 136 milhões) ou 10% de sua receita anual (o que for maior), por não conseguir remover conteúdo "prejudicial aos usuários" (MACIEL, 2021, s.p).

A questão posta nesse artigo, portanto, diz respeito à publicidade paga, ou seja, ao anúncio e a facilidade de golpistas em atingirem um vasto público cibernético. Não se trata de qualquer redirecionamento de site, mas sim de um *link* com visibilidade, daquele que está entre os primeiros quando o consumidor busca um produto qualquer, daquele redirecionamento que é possível graças ao anúncio pago. A facilidade com que o *Google*, *Facebook*, *Instagram*, entre outros, oferecem para aquele que paga pela publicidade não pode ser desconsiderada.

O *Google Ads*, divulga como publicidade própria: "alcance novos clientes, promova o perfil da sua empresa e alcance resultados que importam para você, e com a ajuda de experts quando você precisar. Nós igualamos o valor que você investir, até R\$150**". Para gozar da visibilidade, basta selecionar o tipo de campanha com uma conta no *Google*:

Figura 3: Anúncio do *Google Ads*



Selecione como você quer alcançar sua meta

Visitas ao site

Site da sua empresa

Ligações telefônicas

Visitas à loja

Downloads do aplicativo

Fonte: Retirado do *Google Ads*.

De igual forma ocorre com o *Instagram*, o qual faculta ao usuário fazer a propaganda de si mesmo afirmando que, com o simples pagamento de R\$ 1.000,00 por dia, é possível atingir entre 67.000 a 180.000 pessoas.

Figura 4: Anúncio no *Instagram*



Fonte: Retirado do *instagram*.

A questão se coloca, outrossim, é se o simples pagamento faz com que qualquer site possa ter visibilidade, inclusive aqueles voltados para golpes e fraudes. Não existe nenhum mecanismo ou filtro por parte dos anunciantes para o controle de tal situação, até porque, de fato, o que se vende pelos mecanismos de busca é exatamente a publicidade sem haver importe *a priori* do conteúdo do que se publiciza.

A dissipação da informação é feita de imediato para um número irrestrito de pessoas, ora vítimas, as quais jamais teriam conhecimento de determinado site se não fosse o facilitador de buscas e os anúncios. É oportuno mencionar também que para se chegar na Figura 4 no *Instagram*, o próprio aplicativo indaga a faixa etária que se quer atingir, o sexo, a localidade, o público alvo (por exemplo, estudantes ou profissionais) e assim por diante. Ou seja, tais mecanismos atuam com o cruzamento de dados, os quais são utilizados propositalmente para atingir determinada pessoa. Não se trata de um acaso publicitário, mas sim de uma divulgação realizada a partir de um estudo cuidadoso de perfis.

5 Reflexões críticas e lesão de Direitos Fundamentais

A facilitação do caminho do golpe é que contribui e atua os mecanismos de busca. Resta, portanto, indubitável que ocorre falha na prestação de serviços e esta falha se dá pelo serviço dissimulado (já que oculta fraude e ilícito) disponibilizado ao consumidor de informações cibernéticas. Este consumidor de fato e de direito torna-se vulnerável na navegação de sites e propagandas anunciadas. Deste modo, mostra-se indubitável aplicar-se extensivamente o artigo 14 do CDC, que analisa a responsabilidade objetiva nas relações de consumo:

Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (BRASIL, 1990, s.p).

Se o mecanismo de busca auferir ganhos com a publicidade paga, é certo que ele assume o risco da intermediação e redirecionamento fraudulento. Trata-se, pois, de um serviço defeituoso por não fornecer a segurança adequada que dele se espera, causando transtornos e resultados diversos do pretendido inicialmente. Enquadra-se perfeitamente a responsabilidade independente de culpa e de forma objetiva para os casos aqui discorridos. Por evidente também, sem o mecanismo de busca, técnicas de *SEO* e anúncio pago, não seria possível a alta visibilidade a anúncios e sites golpistas. O induzimento da ferramenta ao golpe, se caracteriza como prática abusiva e, também, como propaganda enganosa, conforme os cânones do CDC:

Art. 37. É proibida toda publicidade enganosa ou abusiva.

§ 1º É enganosa qualquer modalidade de informação ou comunicação de caráter publicitário, inteira ou parcialmente falsa, ou, por qualquer outro modo, mesmo por omissão, capaz de induzir em erro o consumidor a respeito da natureza, características, qualidade, quantidade, propriedades, origem, preço e quaisquer outros dados sobre produtos e serviços.

§ 2º É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita

valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança.

§ 3º Para os efeitos deste código, a publicidade é enganosa por omissão quando deixar de informar sobre dado essencial do produto ou serviço (BRASIL, 1991, s.p) (grifo nosso).

A questão que se coloca no escrito, é que o ressarcimento das vítimas de modo efetivo se faz dificultoso pela empresa golpista, eis que seu anúncio se fez justamente para a realização da prática criminosa. Logo, a irresponsabilidade dos mecanismos de buscas que conduzem o consumidor para uma emboscada, na prática, atua como estímulo para golpistas, pois o descobrimento do seu site fraudulento somente se faz com a ajuda da ferramenta.

Por isso, defende-se que a responsabilização dos mecanismos de buscas de forma objetiva em situações de publicidade paga. Tal rigidez poderia demandar, por exemplo, a exigência de documentos da empresa anunciante, confirmação da identidade por reconhecimento facial, número de telefone e assim por diante. O fato é que, da forma como é posta atualmente, o anúncio pago sem qualquer verificação de idoneidade torna-se um estímulo para práticas criminosas e ilícitas, dada a facilidade para aplicação do golpe.

Logo, ao Estado de nada adianta enrijecer leis penais para crimes cibernéticos e estelionatos virtuais, pois na realidade concreta isso não impede o crime, tampouco intimida *hackers* e malfeitores virtuais. É o caso, por exemplo, da Lei 14.155 de 2021 que assevera os crimes de invasão de dispositivo informático e torna mais graves crimes cometidos de forma eletrônica (BRASIL, 2021). Ora, na verdade, pode-se dizer que tal lei somente fomenta o que se denomina de Direito Penal Simbólico e Promocional, ao passo que aumentar penas e endurecer os dispositivos legais criminais, ainda assim mostra-se ineficaz para a reparação da vítima¹².

¹² Por Direito Penal Simbólico, entende-se a confecção de novas legislações que tem o condão de conter o clamor público, conferindo a falsa impressão de tranquilidade social. Essas respostas legislativas, por vezes, acalantam os clamores sociais, entretanto, não modificam a realidade existente, sendo assim, simbólicas. O Direito Penal Simbólico se faz pela necessidade de ação que a sociedade demanda, porém não emerge resultado efetivo (SALIM; AZEVEDO, 2019). Já o Direito Penal Promocional se faz na consecução de leis penais com finalidades políticas, dado que esta é “um poderoso instrumento de desenvolvimento e transformação social (função promocional). Essa função é criticada por parte da doutrina, uma vez que o Direito Penal deixa de ser utilizado pelo legislador como modo de controle social

O que se pondera no presente escrito é a lacuna doutrinária e jurisprudencial civilista de proteger o elo mais vulnerável da relação contratual. A aplicação da responsabilidade objetiva aos mecanismos de buscas garantiria a reparação financeira da vítima¹³, bem como possivelmente forçaria a tais mecanismos adotar medidas de proteção ao consumidor, visando evitar lides e prejuízos judiciais. O consumidor ao utilizar o serviço disponibilizado por grandes empresas (mecanismos de buscas), tem-se falhado seu serviço ao adentrar em sites golpistas. Não é possível desproteger o consumidor vulnerável que fica à mercê de práticas abusivas que induzem um consumo que age sem probidade e sem boa-fé.

O *marketing* digital e os serviços de *SEO* sabem que aproximadamente 75% dos usuários virtuais não passam da primeira página do resultado de busca e a paga publicitária se faz exatamente para isso (SOLDI, 2018). Não se trata de um mecanismo inocente que aleatoriamente coloca loja qualquer no topo da pesquisa. Se assim fosse, inclusive, não se defenderia a responsabilização de tais mecanismos.

No entanto, a própria propaganda da empresa de comunicação e *SEO*, afirma-se:

94% dos links que as pessoas clicam são resultados orgânicos.
68% de todos os cliques da busca orgânica vão para os primeiros três resultados.
75% dos usuários não passam da primeira página do resultado de busca.
Os dados acima mostram a importância de investir em *SEO* no *Inbound Marketing*. Estar bem ranqueado organicamente (de preferência estar na primeira página da busca) e ter conteúdo de qualidade são formas de aumentar suas possibilidades de ser encontrado na hora que seu público procura pelo seu serviço ou produto. Investir em *SEO* é aumentar suas possibilidades de gerar clientes (SOLDI, 2018, s.p).

subsidiário (*ultima ratio*)” (Ibid., p. 40). No caso em tela, se mostra evidente que o aumento da pena de delitos cibernéticos não oferece resultados, eis que além de não inibir o crime, não modificou a realidade que já está posta.

¹³ Aqui tem-se uma situação realmente importante e interessante já que se aponta lacuna doutrinária e jurisprudencial e não lacuna legislativa. O vazio não é legal e sim, de correta aplicação do que consta prescrito. A causa fundamental da lacuna jurisprudencial é a relativa inadaptação do judiciário a novos paradigmas jurídicos. Exemplo disto são as dificuldades relativas ao domicílio do golpista, ações interpartes apenas em fraudes massivas, proteção inadequada de dados quando estes estão conectos a empreendimentos fraudulentos e não menos importante, inadequações relativas à personalidade jurídica conformada a laranjas que assumem voluntária ou involuntariamente a irresponsabilização criminoso. Assumir-se como responsável pelo crime pode ser compensador.

Atualmente, no entanto, a tendência doutrinária e jurisprudencial é desonerar a responsabilidade quanto aos provedores de pesquisa. Nessa linha de pensamento, a Ministra do Superior Tribunal de Justiça e do Tribunal Superior Eleitoral, Fátima Nancy Andrichi conclui ser “ilegítima a responsabilização dos provedores de pesquisa pelo conteúdo do resultado das buscas realizadas por seus usuários” (ANDRIGHI, 2012, p. 68)¹⁴. A crítica a ser feita, entretanto, é que a discussão ignora a existência do pagamento publicitário, bem como no redirecionamento de *links* mediante alta visibilidade dos mecanismos de buscas.

Assim, a ausência da responsabilização dos mecanismos de buscas deixa de mãos atadas a parte mais vulnerável da relação consumerista, ou seja, o consumidor que permanece à mercê de artimanhas informacionais que induzem fraudes e golpes. Pode-se dizer assim que tal situação vem a colidir com aqueles princípios básicos que norteiam a legislação consumerista, ao passo que não se coloca o consumidor em segurança quanto a um serviço ofertado pelo mecanismo de busca. Neste sentido, a adoção da responsabilização objetiva e solidária entre o que se anuncia virtualmente e a empresa faz-se fundamental na estruturação de procedimentos que visem a idoneidade e a segurança das transações comerciais na *internet*.

Outra questão extremamente delicada a ser mencionada ainda, é que quando o consumidor se faz persuadido para o *site* fraudulento, a efetivação da suposta compra se faz como violação de direitos fundamentais¹⁵ prescritos na constituição como a intimidade,

¹⁴ O pensamento da Ministra é “Em suma, pois, tem-se que os provedores de pesquisa: (i) não respondem pelo conteúdo do resultado das buscas realizadas por seus usuários; (ii) não podem ser obrigados a exercer um controle prévio do conteúdo dos resultados das buscas feitas por cada usuário; e (iii) não podem ser obrigados a eliminar do seu sistema os resultados derivados da busca de determinado termo ou expressão, tampouco os resultados que apontem para uma foto ou texto específico, independentemente da indicação do URL da página em que este estiver inserido” (ANDRIGHI, 2012, p. 74).

¹⁵ Os direitos fundamentais consistem na sintaxe da liberdade nas Constituições, bem como na hermenêutica que transcende os métodos interpretativos da escola clássica da velha hermenêutica positivista. Os direitos fundamentais, para Paulo Bonavides (2006) seriam as prestações do Estado, as garantias institucionais, o sentido objetivo da norma e a qualificação valorativa. São normas objetivas da CF que regulam as relações dos indivíduos com o Estado. Discorre Luís Fernando Sgarbossa (2010, p. 60-61) acerca da constitucionalização do modelo de Estado Social, ao passo que direitos sociais “passaram a integrar o grupo dos direitos fundamentais, ao lado dos direitos e liberdades clássicos (civis e políticos). Trata-se aqui do advento de um novo modelo de direitos fundamentais, os direitos fundamentais sociais (*Sozialen Grundrechte*)”. Portanto, os direitos fundamentais possuem o duplo caráter de direitos subjetivos do indivíduo, bem como fundamentais para a ordem objetiva da coletividade. Assim, o que se reflete neste artigo são os

liberdade, privacidade, segurança, honra e também da imagem. Isto ocorre porque ao efetuar o cadastro, a vítima insere dados como registro geral (RG), cadastro de pessoa física (CPF), endereço, informações do cartão de crédito (inclusive do código de segurança) e assim por diante, os quais podem ser reutilizados para aplicação de novos golpes. Discorre o artigo 5º, inciso X, da Constituição Federal que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” (BRASIL, 1988).

Neste contexto, um simples *site* voltado para aplicação de golpe torna-se também um possível instrumento de armazenamento de dados pessoais e sensíveis, fato que expõe, fragiliza e desprotege ainda mais a vítima. Conforme as reportagens já mencionadas nesse artigo, ambas elucidavam o uso de identidades falsas pelos golpistas (RECORD TV, 2021). Nesse sentido, é perfeitamente possível que os dados ali inseridos ainda sejam utilizados em clonagem de documentos e outros crimes. A controvérsia, portanto, é profundamente e totalmente legítima que seja levantada em discussão qualificada, eis que, estamos falando de relações que envolvem vítimas consumidoras e, de outro lado, mecanismos de buscas bilionários, que poderiam dificultar e conseqüentemente diminuir o número de vítimas de sites confeccionados unicamente para o crime.

6 Considerações finais

A irresponsabilização dos mecanismos de buscas quanto à publicidade e o anúncio pago, contribuem para a exposição do consumidor às artimanhas maliciosas e golpes virtuais. A irresponsabilização favorece assim, malfeitores que se utilizam da ferramenta para ampliar o número de vítimas, bem como na condução daquele vulnerável ao caminho da fraude que se arquitetada e se produz pelo uso do ferramental de buscas. Emerge daí que tais sites possuem credibilidade aparente e passam a impressão de idôneos sendo que alguns, inclusive, anunciam em *marketing places* de outras grandes empresas, como é o caso da

direitos fundamentais básico-jurídicos-constitucionais do particular, como cidadão, como é o caso da violação da intimidade e da vida privada do usuário do *cyber* espaço.

Compufree e outras empresas listadas pelo Procon-SP, lista essa frequentemente atualizada, de empresas com anúncios no site submarino, lojas americanas, *Walmart*, dentre outras.

Uma simples busca no *Google*, por exemplo, atina milhares ou milhões de sites em poucos segundos, no entanto apenas aqueles que pagam anúncios e serviços de *SEO* permanecem propositalmente no topo das buscas. Nesse raciocínio, devido à grande amplitude da busca, sites desconhecidos e novos jamais conseguiriam ser encontrados na busca se não fosse pela condução dos *sites* de buscas e pesquisas. A forma com que o mecanismo induz o consumidor ao golpe, se faz totalmente obliterada nas decisões judiciais, já que não se considera a integralidade das conexões comerciais vinculadas à consecução do ilícito golpista.

Os mecanismos de busca não agem de boa-fé no negócio jurídico pois tudo se faz validado pelo pagamento. Não importa ao intermediário quem recebe o pagamento, se a empresa contratante da propaganda é idônea ou, ainda, se ela efetivamente existe e pode cumprir com os termos do anúncio que veicula. O fato é que, para criminosos, os mecanismos de busca agem em seu benefício, inclusive no fornecimento de dados para a concretização da suposta compra. Tal situação, coloca em risco direitos fundamentais da pessoa humana já que a rede do empreendimento golpista toma os dados do comprador e os pode expor para comprometer sua segurança e individualidade, bem como sua imagem.¹⁶

Por isso, imperioso que o Judiciário adote uma nova linha jurisprudencial, qual seja, a de adotar nas decisões os critérios de fixação da responsabilidade objetiva concernente ao uso do ferramental de busca na internet.

¹⁶ É o caso analisado por Sydow e Castro (2015), das práticas de sextorsão em que o bandido se aproveita das redes de comunicação social para capturar nas redes sociais, homens e mulheres no intuito de se conseguir informações pessoais, fotos e elementos que possam fundar o cobro de extorsão. As informações do *Facebook*, *instagram*, *linkedin* e outros, disponíveis no mundo virtual, podem servir para a captura de pessoas suscetíveis de serem golpeadas. O tema da sextorsão não é exatamente o mesmo ao qual nos referimos até aqui. Todavia, o instrumental de virtualidade para realização dos crimes é o mesmo.

Referências

- ANDRIGHI, Fátima Nancy. **A responsabilidade civil dos provedores de pesquisa via internet**. Brasília. Revista TST: vol. 78, no 3, jul./set 2012. Disponível em: <https://juslaboris.tst.jus.br/bitstream/handle/20.500.12178/34301/003_andrighi.pdf?sequence=1&isAllowed=y>. Acesso em 15 agosto 2021.
- BONAVIDES, Paulo. **Curso de direito constitucional**. 18. ed. São Paulo: Malheiros, 2006, p. 571.
- BRASIL. **Constituição da República Federativa do Brasil**. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 10 setembro 2021.
- BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em 10 setembro 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 República Federativa do Brasil], Poder Legislativo, Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em: 29 maio 2021.
- BRASIL. Lei nº 14.155, de 27 de maio de 2021. Diário Oficial [da República Federativa do Brasil], Poder Legislativo, Brasília, DF, 28 mai. 2021. Disponível em: <<https://www.in.gov.br/en/web/dou/-/lei-n-14.155-de-27-de-maio-de-2021-322698993>>. Acesso em: 23 setembro 2021.
- BRAGA NETTO, Felipe Peixoto. **Manual de Direito do Consumidor**: à luz da jurisprudência do STJ. 10ª ed. Salvador: Edições Juspodivm, 2014.
- BRÊTAS, Pollyanna. **Golpes virtuais fizeram mais de 150 milhões de vítimas em 2021 no Brasil, estima empresa de cibersegurança**. GLOBO. 2021. Disponível em: <<https://extra.globo.com/economia/financas/golpes-virtuais-fizeram-mais-de-150-milhoes-de-vitimas-em-2021-no-brasil-estima-empresa-de-ciberseguranca-rv1-1-25237943.html>>. Acesso 10 outubro 2021.
- CHOMSKY, Noam. **Mídia**: Propaganda e Manipulação. São Paulo: Martins Fontes, 2014.
- CUNHA, Lilian. **Comprou e não recebeu?** Com golpes mais sofisticados, quadrilha falsifica até selo do Reclame Aqui. 2021. UOL. Disponível em: <https://cultura.uol.com.br/noticias/22312_comprou-e-nao-recebeu-com-golpes-mais-sofisticados-quadrilha-falsifica-ate-selo-do-reclame-aqui.html>. Acesso em 15 setembro 2021.

DFNDR LAB. **Relatório da Segurança Digital**. 2018. Disponível em: < <https://www.psafec.com/dfndr-lab/wp-content/uploads/2018/11/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-3%C2%BA-trimestre-de-2018-1.pdf>>.

EMPOLI, G. D. **Os Engenheiros do Caos**. São Paulo: Vestígio, 2019.

GOOGLE ADS. **Anúncio**. Disponível em < https://ads.google.com/intl/pt_BR/home/>. Acesso em 15 de setembro de 2021.

HALL, S. **A identidade cultural na pós-modernidade**. 6. ed. Rio de Janeiro: DP&A, 2001.

LIPOVETSKY, G. SERROY, Jean. **A estetização do mundo**: viver na era do capitalismo artista. Companhia das Letras, 2015.

MARX, Karl. **O Capital**. São Paulo: Civilização Brasileira, 2020.

MACIEL, Rui. **Google e Facebook têm dificuldades em banir anúncios fraudulentos, diz pesquisa**. Disponível em < <https://canaltech.com.br/seguranca/google-e-facebook-nao-estao-conseguindo-banir-anuncios-fraudulentos-diz-pesquisa-183507/>>. Acesso em 15 de setembro de 2021.

PROCON SP (org.). **Evite esses Sites**. 2021. Fundação de Proteção e Defesa do Consumidor. Disponível em: <https://sistemas.procon.sp.gov.br/evitesite/list/evitesites.php>. Acesso em: 08 set. 2021

RECORD TV. **Siga Ofertas**: empresa fecha as portas e tira site do ar. Goiás. Disponível em: <<https://www.youtube.com/watch?v=ctrlmLklwu7w>>. Acesso em 10 agosto 2021.

ROHR, Altieres. **Criminosos transformam resultados de buscas na web em isca para vírus**. G1. Disponível em: < <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1566061-6174,00-CRIMINOSOS+TRANSFORMAM+RESULTADOS+DE+BUSCAS+NA+WEB+EM+ISCA+PARA+VIRUS.html>>. Acesso em 04 outubro 2021.

ROHR, Altieres. **Anúncios no Google divulgam sites falsos para negociar e quitar dívidas com descontos oferecidos por WhatsApp**. G1. Disponível em: <<https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/06/15/anuncios-no-google-divulgam-sites-falsos-para-negociar-e-quitar-dividas-com-descontos-oferecidos-por-whatsapp.ghtml>>. Acesso em 10 agosto 2021.

SALIM, Alexandre; AZEVEDO, Marcelo André de. **Direito Penal**: parte geral. 9. ed. São Paulo: Jus Podivm, 2019.

SANTOS, Milton. **Por uma outra globalização: do pensamento único à consciência universal**. Rio de Janeiro: Record, 2010. 174 p.

SGARBOSSA, Luís Fernando. **Crítica à Teoria dos Custos dos Direitos**: Volume 1. Porto Alegre: Sergio Antonio Fabris Ed., 2010.

SOUZA, Abel. **Compufree é confiável?** Análise completa (+ exemplos). Disponível em: <<https://confiavel.net.br/compufree/>>. Acesso em 08 setembro 2021.

SOLDI, Caio. **75% dos usuários nunca passam da primeira página**. CVS Comunicação. 2018. Disponível em: <<https://cvscomunicacao.com.br/blog/75-dos-usuarios-nunca-passam-da-primeira-pagina-do-resultado-de-busca/amp/>>. Acesso em 17 de setembro de 2021.

SYDOW, S. T.; CASTRO, A. L. C. Sextorsão. **Revista dos Tribunais**, São Paulo, v. 959, setembro de 2015. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.959.09.PDF>

SNIDER, J. H.; ZIPORYN, T. **Future Shop**: How New Technologies will Change the Way we Shop and What we Buy. Bloomington: iUniverse, 2008 [1992].

TJDFT. **A inversão do ônus da prova se opera de forma automática no microsistema do CDC?** 2020. Disponível em: <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/jurisprudencia-em-perguntas/onus-da-prova-direito-do-consumidor/onus-da-prova/a-inversao-do-onus-da-prova-se-opera-de-forma-automatica-no-microsistema-do-cdc>. Acesso em: 08 set. 2021.