Paula Benassuly ARUDA[1]
Dennis VERBICARO[2]
Jorge Azevedo CALANDRINI[3]

Argumenta
Journal Law
n. 38 p. 305-337
set/dez 2022

AS VULNERABILIDADES DO CONSUMIDOR NA UTILIZAÇÃO DE SERVIÇOS DE VIDEOCONFERÊNCIA

CONSUMER VULNERABILITIES IN THE USE OF VIDEOCONFERENCE SERVICES

LAS VULNERABILIDADES DEL CONSUMIDOR AL UTILIZAR LOS SERVICIOS DE VIDEOCONFERENCIA

Como citar este artigo:
ARUDA, Paula, VERBICARO, Dennis, CALANDRINI, Jorge. As vulnerabilidades do consumidor na utilização de serviços de videoconferência. Argumenta Journal Law, Jacarezinho – PR, Brasil, n. 38, 2022, p. 305-337

Data da submissão:
04/08/2021
Data da aprovação:
05/11/2022

SUMÁRIO:

1. Universidade Federal do Pará - Brasil
2. Universidade Federal do Pará - Brasil
3. Universidade Federal do Pará - Brasil

RESUMO:

O presente artigo tem o objetivo de apresentar o agravamento das vulnerabilidades do consumidor

na utilização de serviços de videoconferência, sob as perspectivas técnica, situacional e social a partir dos riscos decorrentes da hiperconfiança nas plataformas virtuais. O método foi o dedutivo e a metodologia foi a teórico-bibliográfica nacional e estrangeira. O artigo adverte que a imersão tecnológica do consumidor impõe o aprimoramento da tutela dos dados pessoais para um exercício de controle no ambiente digital, analisando a falha de segurança da plataforma Zoom Vídeo à luz da legislação brasileira sobre o tema.

ABSTRACT:

This article aims to demonstrate the worsening of consumer vulnerabilities in the use of videoconference services, under the technical, situational and social perspectives from the risks arising from hyperconfidence in virtual platforms. The method was the deductive and the methodology was the national and foreign theoretical-bibliographic. The article warns that the technological immersion of the consumer imposes the improvement of the personal data's protection for an exercise of control in the digital environment, analyzing the security flaw of the Zoom Video platform in the light of brazilian legislation on the subject.

.

RESUMEN:

O trabajo tiene como objetivo demonstrar el empeoramiento de las vulnerabilidades dos consumidores en la utilización de servicios de videoconferencia, en las perspectivas técnica, situacional y social de los riesgos derivados de la hiperconfiencia en plataformas virtuales. El método utilizado fue el deductivo y la metodología fue la teórica bibliográfica nacional y extranjera. El artículo advierte que la inmersión tecnológica del consumidor impone la mejora de la tutela de los dados personales para un ejercicio de control en ambiente digital, analizando los fallos de seguridad de la plataforma Zoom Video a la luz de la legislación brasileña.

PALAVRAS-CHAVE:

Imersão tecnológica; Vulnerabilidade; Proteção de dados.

KEYWORDS:

Technological immersion; Vulnerability; Data protection.

PALABRAS CLAVE:
Inmersión tecnológica; Vulnerabilidades; Protección de dados.

INTRODUÇÃO

A inovação tecnológica da sociedade e o aprimoramento da internet possibilitaram um consumo constante no ambiente digital com a possibilidade do comércio e oferta de serviços eletrônicos. Percebe-se nesta conjuntura, uma dicotomia entre o consumo presencial (analógico) e o virtual (digital), evidenciando-se tais modificações na inexistência de barreiras geográficas para realizar compras e obter serviços na internet e na comodidade de consumir no ambiente digital.

Diante desse contexto de evolução tecnológica, o consumidor está mais conectado ao mundo cibernético, incorporando os serviços virtuais como um hábito. A internet apresenta benefícios ao consumidor e proporciona rapidez e acessibilidade ao usufruir de bens e serviços, como por exemplo, utilizar aplicativos de videoconferência para se comunicar em qualquer parte do mundo. Entretanto, deve-se resguardar a tutela dos dados pessoais e o sigilo da privacidade virtual, reprimindo as práticas negligentes no ambiente digital.

Desta forma, o artigo investigará o agravamento da vulnerabilidade social, técnica e situacional do consumidor na utilização de aplicativos de videoconferência, o que resulta em uma vulnerabilidade na proteção dos dados pessoais dos usuários. Considera-se como hipótese inicial que os dados pessoais possuem íntima ligação com a privacidade. A privacidade é a faculdade do indivíduo de ter informações pessoais apenas para si e ter o direito de não ser divulgada para estranhos, sendo então os dados pessoais uma parcela da personalidade e da privacidade do indivíduo na sociedade da informação.

Neste sentido, o artigo explanará sobre a imersão tecnológica do consumidor, perpassando pelo agravamento das vulnerabilidades nesse contexto. No segundo tópico será elucidada a importância da proteção da privacidade virtual e a tutela dos dados pessoais na sociedade da informação.

Na segunda parte do estudo, será analisado o caso da plataforma

Zoom Clouds Meetings para ilustrar às vulnerabilidades dos usuários e por fim demonstrar que a inércia estatal na regulamentação acentua à vulnerabilidade do consumidor nesta matéria, fazendo com que o consumidor e as instituições judiciais tenham que tomar ações propositivas para a resolução dos conflitos.

1. A CONFIANÇA E A IMERSÃO TECNOLÓGICA DO CONSUMIDOR

A tecnologia mostra-se como instrumento indispensável para o desenvolvimento da sociedade, possibilitando grandes avanços socioeconômicos. O aprimoramento da internet e da tecnologia foram responsáveis por introduzir o consumidor no mundo digital, o que possibilitou grande facilidade para consumir através do comércio eletrônico.

Cláudia Lima Marques em seu livro "A confiança no mercado eletrônico e a proteção do consumidor" salienta a importância da boa–fé durante o consumo analógico e como os fornecedores sempre buscaram pautar suas relações jurídicas nesse instituto (ALL, 2005, p. 287). No meio digital, a boa-fé transforma-se na confiança entre consumidor e fornecedor, levando a autora a falar sobre um novo paradigma acerca da confiança nas relações digitais (ALL, 2005, p. 286)

Claudia Lima Marques aduz que, o direito contratual vive e viveu em crise. A primeira crise surgiu na Revolução Industrial, pois houve a massificação das relações contratuais, o que resultou na supressão da autonomia privada em função dos contratos de adesão tornarem-se o principal instrumento de circulação de bens e serviços. A segunda crise diz respeito a crise da pós-modernidade, onde os serviços e os bens imateriais assumem o centro das contratações. Enquanto a terceira crise, é a crise da confiança devido a crescente prestação de serviços de alta técnica, com extrema complexidade, gerando uma carga de desconfiança dos consumidores sobre a segurança e qualidade dos bens e serviços postos no mercado (MARQUES, 2016, p. 165-185)

Observa-se essa crise da confiança no início do comércio digital, onde entende-se que no espaço virtual quanto maior à distância e a impessoalidade do fornecedor, torna-se mais importante buscar a confiança do consumidor (MUCELIN, 2020). Logo, verifica-se como estimular a confiança era necessário para que o consumidor se aprofundasse nas

oportunidades do mundo virtual.

Para que ocorresse a imersão do consumidor no ambiente virtual, foi necessário primeiramente estimular o consumo digital como um espaço descentralizado e democrático, aumentando o acesso a essa modalidade de consumo. Após a democratização do acesso, foi preciso que às empresas fornecessem a confiança para o consumidor se sentir seguro em efetuar compras no meio virtual. Por se tratar de um novo meio de consumo, era necessário instigar a ideia de que o comércio eletrônico era seguro e principalmente confiável (VERBICARO, 2020).

Adquirir confiança do consumidor era fundamental para o desenvolvimento dessa nova forma de consumo, pois no meio digital, o consumidor perde a possibilidade do tato com o produto, de experimentar ou de tirar suas dúvidas pessoalmente. Isto ocorre, pois o consumidor e o fornecedor não estão no mesmo espaço e tempo, o que ocasiona uma desconfiança do consumidor na hora de realizar a compra com medo do produto não ser entregue, ou não ser o produto adquirido no ato da compra ou este está com defeito (VERBICARO; MARTINS, 2018, p. 374).

De fato a confiança para realizar uma compra na internet é fundamental, o consumidor busca empresas familiares, sabendo que não haverá riscos ao utilizar o comércio eletrônico, como por exemplo, não ter seu cartão clonado e saber que seus dados serão protegidos na compra. Porém, observa-se que com os consumidores habituados ao mundo digital, o ambiente de desconfiança foi desaparecendo e dando lugar à uma confiança sistêmica, ocorrendo o fenômeno da hiperconfiança.

O que se nota, é que os usuários depositam grande fé nas plataformas sem conhecer o fornecedor ou ter qualquer contato anterior que estabeleça um vínculo de confiabilidade. Sobre a hiperconfiança, Guilherme Mucelin (2020) explana que:

> Ultrapassa-se, assim, de certa maneira, a desconfiança geral que existe no mercado de consumo e, em especial, no que se refere ao comércio eletrônico tradicional, para uma fase pós-moderna de confiança generalizada, exacerbada, abundante, circular e sistêmica – o que Claudia Lima Marques convencionou chamar de *Hiperconfiança.*

A formação da (hiper)confiança é induzida no consumidor digital através de sofisticadas técnicas, seja pelo uso do instrumento da publici-

dade até a forma de avaliação das plataformas. O estímulo da confiança do consumidor para as empresas está ligada ao valor económico que possui esse fator nas relações de consumo, sendo importante destacar a reflexão de Célia Weingarten sobre o valor económico da confiança:

> La confiabilidad de la marca y la empresa posibilita diseñar otro tipo de estratégias optimizando el beneficio económico; una empresa podrá por ejemplo ampliar y diversificar sus productos o servicios de manera mucho mas sencilla, porque a traves de la calidad de un producto el consumidor presumira la calidad de otros (la expansión de la confiabilidad se representa en otros productos con la misma marca). (WEINGARTEN, 2000, p. 40).

Em função da confiança possuir um valor económico para as empresas e ser um fator estimulado pelas companhias, faz-se necessária à sua proteção, que ocorrerá quando houver a quebra de expectativa do usuário com o serviço ofertado, resultando em uma obrigação de reparação ao vulnerável (WEINGARTEN, 2000, p. 40). Neste sentido, a responsabilização será de forma objetiva, sem necessidade de comprovação de dolo ou culpa conforme os ditames do CDC (MUCELIN, 2020).

O cenário de confiança sistêmica influenciado pelas empresas e a imersão tecnológica do consumidor desperta a necessidade de entender os agravamentos das vulnerabilidades dos usuários para o exercício de um controle, buscando salvaguardar direitos fundamentais nessas relações privadas. Esse controle se traduz especialmente no que diz respeito à regulamentação e responsabilização dos fornecedores (VERBICARO, 2020).

Na busca por incorporar o comércio eletrônico como um hábito de consumo, constatou-se que o consumidor muitas vezes estava desamparado quanto às suas dúvidas e quanto às possíveis formas de tutelar a responsabilização do fornecedor após uma experiência negativa no consumo digital, sendo importante um reforço do controle no ambiente cibernético (VERBICARO, 2020).

Nota-se que, após a fase de estímulo do acesso e confiança o ambiente digital está incorporado nos padrões de consumo da sociedade contemporânea. Entretanto, o aspecto do controle ainda está em desenvolvimento, pois em que pese às regulamentações específicas do ambiente cibernético no Brasil, como a Lei do Marco Civil da Internet e, princi-

palmente, a LGPD às violações a esses direitos não cessaram. Além de que, observa-se baixa adequação ao melhor entendimento da LGPD, por exemplo, dificilmente encontram-se players que permitam um consentimento granulado nos sites em solo nacional. Outra questão, diz respeito à satisfação dos princípios da finalidade (art. 6º, I, da lei 13.709/18), da necessidade (art. 6º, III, da lei 13.709/18) e da transparência (art. 6º, VI, da lei 13.709/18).

Portanto, com os usuários hiperconectados e hiperconfiantes na utilização dos serviços digitais, verifica-se uma profunda modificação nas relações de consumo. E nesse contexto, é fundamental analisar o agravamento da vulnerabilidade social, técnica e situacional do consumidor, pois às vulnerabilidades afetam na possibilidade de se realizar uma decisão consciente.

1.1 Do Agravamento da vulnerabilidade social, técnica e situacional do consumidor nas relações consumeristas na internet

A vulnerabilidade do consumidor é preceituada pelo art. 4º, I, do CDC, sendo uma presunção absoluta a todos os consumidores, sejam doutores ou analfabetos, essa característica intrínseca do consumidor não será descaracterizada (MIRAGEM; MAQUES, 2012, p. 198). A vulnerabilidade refere-se ao direito material, e dessa forma, mostra-se importante na responsabilização civil das plataformas, pois possibilita a inversão do ônus da prova preceituado no art. 6º, VIII, CDC.

Em artigo sobre a evolução da vulnerabilidade, os autores afirmam que a vulnerabilidade do consumidor é multifária e comporta diversos significados no mercado de consumo, os quais são resultados das desigualdades socioeconômicas entre fornecedores e consumidores. Além disso, os consumidores estão expostos a uma publicidade crescente, indutora de necessidades artificiais, que prejudicam uma escolha emancipada (GONÇALVES ANTUNES; GONÇALVES ANTUNES, 2017).

As relações consumeristas na internet estão agravando as carências sociais, informacionais, técnicas, jurídica e situacional que o indivíduo enfrenta nesse ambiente. Percebe-se que no ambiente digital às cláusulas contratuais dos serviços são pré-estabelecidas e padronizadas, não respeitando às peculiaridades dos consumidores em função dos contratos unilaterais que retiram a autonomia privada das partes contratantes (VERBI-

CARO; MARTINS, 2018, p. 375).

O ambiente virtual é marcado pelo fato do usuário possuir uma aparente autonomia da vontade, podendo apenas aceitar ou recusar o serviço, não havendo negociação para adequar à oferta a sua necessidade. Ressalte-se que, muitas vezes há insuficiência de informações prestadas pelos fornecedores na oferta, o que resulta em uma vulnerabilidade técnica-informacional (VERBICARO; VIEIRA, 2021, p. 202-203).

Desse modo, o comprador não sabe toda a extensão de informações sobre o serviço contratado em função da carência de dados claros e importantes sobre o objeto de contratação. Sendo assim, o consumidor torna-se mais passível de ser enganado ou não entender de fato o objeto contratado, pois não possui informações e possibilidade técnicas de entender os riscos da contratação (MIRAGEM; MARQUES, 2012, p. 156).

A vulnerabilidade social do consumidor diz respeito a facilidade de certos grupos da comunidade serem prejudicados no ato de consumo, levando em consideração aspectos socioeconômicos do consumidor (ARTONI, 2013, p. 25). Para Andreza Cristina a vulnerabilidade econômica social é:

> Portanto, característica da sociedade de consumo, resultante do desequilíbrio social, da limitação à manifestação de vontade que se observa quando o consumidor vai ao mercado adquirir algo de que necessite e percebe que sua vontade está limitada pela oferta, inclusive no que diz respeito à concorrência de fornecedores (BAGGIO, 2012, p. 44)

A vulnerabilidade situacional é o resultado de um determinado contexto que o consumidor está inserido, onde condições externas dificultam o consumo, desse modo, decorre de uma conjuntura de fatores externos que moldam a situação que o consumidor está vivendo (ARTONI, 2013, p. 27).

A vulnerabilidade situacional do consumidor pode ser observada nos serviços de videoconferência em função da dependência do usuário e a necessidade de concessão dos dados pessoais para usufruir do serviço. Verifica-se, assim, a vulnerabilidade situacional do consumidor em casos de dependência do usuário com o serviço prestado (VERBICARO; VIEIRA, 2021, p. 205).

Com as vulnerabilidades social, técnica e situacional agravadas no

ambiente digital à tutela da imagem, da privacidade e da proteção de dados pessoais dos usuários estão em risco. É diante desse cenário de aumento das vulnerabilidades no ambiente digital, que intensifica-se a necessidade de tutela da privacidade virtual e dos dados pessoais para reprimir às práticas negligentes das plataformas.

Na sociedade da informação exercer a privacidade virtual se tornou uma tarefa complexa. As informações pessoais estão em quantidades abundantes no ambiente digital, sendo difícil tutelar esse direito devido a concessão desses dados ser uma prática compulsória para utilização dos serviços. Observa-se, portanto, uma conjuntura de agravamento das vulnerabilidades dos consumidores, seja social, técnica-informacional e situacional, fruto da dependência do consumidor para usufruir serviços online. É diante desse contexto, que reafirma-se a importância da proteção da privacidade virtual.

2. A IMPORTÂNCIA DA TUTELA DA PRIVACIDADE E DA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Os novos serviços oriundos da evolução tecnológica apresentam incapacidades de garantir a privacidade dos seus usuários da mesma maneira que se desenvolvem. Desta forma, o consumidor hiperconectado e habituado no ambiente cibernético expõe seus dados para utilizar serviços ou realizar compras em plataformas inseguras.

O artigo 5º, X, da Constituição Federal fala em intimidade e vida privada ao invés de privacidade de maneira expressa, porém a doutrina e a jurisprudência entendem a privacidade como resguardada constitucionalmente porque entende-se que a privacidade engloba a intimidade, a vida privada e a imagem (RODRIGUES; FERREIRA, 2019, p. 186). Luiz Roberto Barroso ao falar sobre a privacidade discorre que:

> Dela decorre o reconhecimento da existência, na vida das pessoas, deespaços que devem ser preservados da curiosidade alheia, por envolverem omodo de ser de cada um, as suas particularidades. Aí estão incluídos os fatos ordinários, ocorridos geralmente no âmbito do domicílio ou em locais-reservados, como hábitos, atitudes, comentários, escolhas pessoais, vidafamiliar, relações afetivas. Como regra geral, não haverá interesse públicoem ter acesso a esse tipo de informação (BARROSO, 2004, p. 13).

Em histórico artigo denominado "The Right To Privacy", os autores refletem sobre às interferências das tecnologias da época que ofendiam a privacidade das pessoas públicas, como por exemplo, a câmera fotográfica devido à intromissão dos jornais na vida privada dos cidadãos. Neste contexto, os autores sustentam o reconhecimento da privacidade conforme o direito de ser deixado sozinho (the right to be alone). Ressalte-se que, esse entendimento foi dado pelo Juiz Cooley e os autores o difundiram, entendendo a privacidade a partir de uma dimensão negativa, que preza por prevenção (WARREN; BRANDEIS, 1890, p. 195).

É possível observar o caráter preventivo do "the right to be alone" na doutrina nacional na seguinte elucidação:

> Dessa forma o valor da privacidade não reside nem consiste em receber determinada montante de indenização em decorrência de determinada publicação, mas na possível paz de espírito ou no alívio constante na capacidade de impedir a própria publicação tendo, portanto, um caráter preventivo (RODRIGUES; FERREIRA, 2019, p. 188).

Atualmente, é uma tarefa hercúlea exercer o direito de estar sozinho, visto que o consumidor está sendo rastreado pelas novas plataformas digitais, em um contexto do capitalismo da vigilância, que resultou em pequenos centros de vigília, os Big Other (ZUBOFF, 2019).

Com efeito, é necessário proteger os dados pessoais, pois entende-se essas informações como a parcela da personalidade do indivíduo, a fim que este possa se desenvolver na sociedade, principalmente, na sua esfera privada quanto às suas opiniões e desejos, garantindo seu livre desenvolvimento pessoal.

Todavia, a constante intromissão dos desenvolvedores na privacidade virtual dos usuários torna complexo exercer a proteção dos dados no consumo digital como explica Laura Schertel:

> Por outro, também na relação entre privados, é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais (MENDES, 2019, p. 39)

Desta forma, o Estado deve impor aos fornecedores o respeito ao tratamento dos dados, assim, evita-se que o consumidor tenha impossibi-

lidade de acesso à bens de consumo e serviço pelo fato deste se preocupar com a sua privacidade (MENDES, 2019, p. 40).

Para dar garantia ao direito constitucional à privacidade nos ambientes digitais, a Lei do Marco Civil da Internet regulamentou às diretrizes e corroborou o entendimento constitucional da proteção à privacidade quando traz em seu artigo 7º, I a inviolabilidade da intimidade e da vida privada. Infirma esse entendimento, a Lei Geral de Proteção de Dados Pessoais quando traz em seu art. 2º, IV a inviolabilidade da intimidade, honra e imagem da pessoa.

A necessidade de proteção da privacidade virtual é consequência do assoreamento constante que os usuários presenciam ao navegar no ambiente digital, visto que seus passos são rastreados constantemente pelos players (DE CASTRO, 2019). O capitalismo da vigilância colocou os dados pessoais dos usuários como o principal objetivo dos players, e neste contexto, a tutela dos dados pessoais assume uma nova dimensão.

Portanto, em decorrência do agravamento das vulnerabilidades que foram acentuadas com a inserção do consumidor no mundo virtual, a proteção da privacidade é indispensável para proteger o livre desenvolvimento pessoal, de opiniões e desejos dos cidadãos.

2.1 A evolução da tutela dos dados pessoais no Brasil

A importância da proteção de dados no ambiente digital cresceu com a inserção do consumidor no ambiente cibernético, visto que a coleta e armazenamento de dados aumentaram exponencialmente conforme o usuário incorpora os serviços digitais como um costume.

Os dados pessoais antes centralizados primordialmente com a figura do Estado se descentralizaram, fazendo com que empresas privadas possuam amplo acesso a eles no ato de consumo (MENDES, 2019, p. 39). Para Zuboff (2019) a descentralização da vigília sob os consumidores resultou no Big Other, que classifica e identifica às predileções dos usuários através da coleta de dados pessoais, resultando em um capitalismo da vigilância.

A hiperconectividade do consumidor aprofundou a coleta e tratamento de dados, pois a internet tornou-se um meio de consumo importante em grande parte dos países e, desse modo, acentua-se a necessidade de tutela dos dados no mundo. Em especial, pelos dados pessoais conterem informações preciosas e privadas dos cidadãos, correspondendo à

intimidade dos titulares dos dados, revelando um caráter personalíssimo e privado (MENDES, 2019, p. 36).

Os dados pessoais se tratados sem respeito às normas protetivas, podem ensejar diversos problemas à personalidade do consumidor. Sobre o assunto, Laura Schertel afirma que:

> Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada divulgação e utilização de informações armazenadas a seu respeito. Por se constituírem em uma parcela da personalidade da pessoa, os dados merecem tutela jurídica, de modo a assegurar a sua liberdade e igualdade. (MENDES, 2019, p. 36)

No Brasil, a primeira legislação a iniciar essa proteção de dados dos consumidores foi o CDC (lei nº 8.078/1990) em seu artigo 43º ao regulamentar os bancos de dados e autorizar seu funcionamento (MENDES, 2019, p. 44).

A Lei do Marco Civil da Internet (lei nº 12.965/2014) estabeleceu os princípios e garantias da internet no país, assim como tratou dos dados pessoais ao dispor em seu artigo 3º, III que "o uso da internet é regido pelo princípio da proteção de dados". Também, define em seu artigo 7º, VII sobre o não fornecimento à terceiros de dados pessoais dos consumidores sem o livre consentimento do titular sobre àquele compartilhamento.

Contudo, em 2018, houve a promulgação da LGPD (lei nº 13.709/2018) que trouxe um novo paradigma sobre a proteção de dados pessoais no Brasil. A LGPD é um marco legislativo sobre a matéria de dados no Brasil e trouxe importantes conceitos, como por exemplo, os dispostos em seu artigo 5º sobre: os dados pessoais, sensíveis e anonimizados.

Os dados pessoais, preceituado pelo art. 5º, I, da lei 13.709/18, são conceituados como dados que permitem identificar ou é identificável o seu titular, em outras palavras, é uma informação individualizada que possibilita saber quem é a pessoa física detentora dos dados, como por exemplo, o Cadastro de Pessoas Físicas - CPF, Registro Geral – RG, e-mail, fotos, áudios e outras formas que permitam identificar àquela pessoa natural.

Os dados sensíveis (art. 5º, II, lei nº 13.709/2018) dizem respeito às

informações mais íntimas do usuário, como: a orientação sexual, a religião, a orientação filosófica, bem como a inclinação política daquele indivíduo, abrangendo, inclusive, a proteção da informação sobre filiação em sindicato.

Os dados anonimizados são preceituados pelo art. 5º, III, da LGPD e definidos como aqueles que não se pode identificar a pessoa que é titular dos dados através de técnicas cibernéticas, como por exemplo, o uso da criptografia (RODRIGUES; FERREIRA, 2019, p. 192).

Quanto aos dados sensíveis, eles são considerados de tal forma, pois possuem o potencial discriminatório elevado, desse modo, pode-se danificar a personalidade daquele usuário se forem compartilhados indevidamente. Desta maneira, o consentimento inequívoco e informado preconizado pela LGPD (art. 5º, XII, lei nº 13.709/18) ao usuário faz-se mais imprescindível quando se tratar de dados sensíveis.

Desta forma, nota-se como os dados sensíveis são uma extensão de informações profundas da vida íntima do usuário e devido a isso, a privacidade desses dados se sobrepõem às relações privadas, constituindo-se como um direito fundamental na contemporaneidade (MENDES, 2019, p. 41).

Importante ressaltar que o CDC é uma legislação de vanguarda, que trouxe discussões que reverberaram para outros campos do direito no Brasil, como o dirigismo contratual mediante normas imperativas que restringem a autonomia privada, caracterizada por ser absoluta no Código Civil, de 1916. A matéria do consumidor infirma novamente a dianteira da discussão de temas inovadores no país ao debater a proteção de dados e privacidade virtual nas relações de consumo.

Com a promulgação da LGPD, com as regras e princípios sobre a internet estipulados pelo MCI em conjunto com o CDC, é possível aplicar um diálogo de fontes para a proteção dos usuários no ambiente digital em solo nacional, reforçando o controle no ambiente cibernético a partir da interpretação mais favorável ao consumidor.

3. O CASO DA EMPRESA ZOOM VÍDEO COMMUNICATION

3.1 O Crescimento devido à pandemia da COVID-19

Em 2020 ocorreu à pandemia da COVID-19[1], ocasionando a decretação deste status pela Organização Mundial da Saúde. Como medida

para coibir as infecções do vírus, foi necessária a adoção do isolamento social. Assim, a pandemia agravou a imersão do consumidor no ambiente digital que já era conhecida, dado ao fato de ser o único meio para consumir devido ao fechamento do comercio presencial (analógico).

Com o fechamento do comércio analógico houve o aumento da dependência dos serviços tecnológico, como por exemplo, os serviços de videoconferência. Nessa conjuntura, nota-se o agravamento das vulnerabilidades dos usuários, especialmente, a técnica, situacional e social em função da dependência de serviços tecnológicos para continuar exercendo as atividades do dia a dia. Um bom exemplo para ilustrar às vulnerabilidades do consumidor ao utilizar os serviços de videoconferência é o caso da empresa de videoconferência Zoom.

A empresa Zoom Vídeo Communication durante a pandemia da Covid-19, obteve um lucro de 4 bilhões de dólares devido ao crescimento de acesso em 1.900% na plataforma conforme informação do CEO Eric Yuan para a comunidade (PEQUENAS EMPRESAS GRANDES NEGÓCIOS, 2020). A valorização da empresa Zoom se deve a alta demanda pelo uso do aplicativo causada pela pandemia. Assim às reuniões familiares, íntimas, de trabalho ou as aulas são realizadas através de videoconferência.

Em matéria jornalística alude-se que, antes da declaração da pandemia pela Organização Mundial da Saúde, ainda em dezembro, a empresa tinha 10 milhões de participantes nas reuniões e em março de 2020, o número subiu para 200 milhões de usuários nas reuniões (ESTADO DE MINAS, 2020).

O aplicativo obteve muitos downloads conforme consta na reportagem do Jornal El País ao trazer que: "Com as pessoas isoladas em suas casas, o número de downloads desse aplicativo cresceu 86% em um mês, segundo o portal Crunchbase." (GARCIA, 2020). Segundo outra matéria jornalística, o aplicativo Zoom é o mais popular nos Estados Unidos e enseja preocupações das autoridades competentes (ÉPOCA NÉGOCIOS, 2020).

O contexto da pandemia da Covid-19 impôs restrições de consumo, onde condições externas influenciam na decisão do consumidor, havendo o agravamento da vulnerabilidade situacional do usuário e por consequência o acentuamento de vulnerabilidades como a técnica-informacional e social. Desta maneira, os aplicativos de videoconferência se

tornaram primordiais para a manutenção mínima da normalidade, fazendo com que o consumidor além de emergir totalmente no ambiente virtual para consumir também emerja para se comunicar.

A empresa de videoconferência possui a plataforma Zoom Clouds Meetings que fornece um serviço "gratuito", permitindo comunicar-se com qualquer pessoa que queira em qualquer canto do mundo com áudio e imagem. Entretanto, é importante questionar se o serviço oferecido é realmente gratuito, pois estes recebem ganhos indiretos como Laura explica:

> Conforme interpretação dominante da jurisprudência, um serviço pode ser oferecido gratuitamente ao consumidor e, ainda assim, ser considerado remunerado, tendo em vista que obtém ganhos indiretos. É o que ocorre com diversos serviços e aplicações na internet, que, embora aparentemente gratuitos, se remuneram por meio de publicidade e da comercialização dos dados de navegação do usuário (MENDES 2016, p. 39).

Além dos dados pessoais serem o grande desejo dos players, os aplicativos induzem a confiança do consumidor, como por exemplo, na forma de avaliação do seu serviço, onde a reputação é classificação pelos próprios usuários. A reputação é medida com base na pontuação aferida pelo consumidor, podendo o usuário atribuir de 0 a 5 estelas para o serviço da plataforma.

Em julho de 2021, o aplicativo Zoom Clouds Meetings conta com uma avaliação em torno de 4,7 em um total de 5 "estrelas" e encontra-se entre os aplicativos mais bem avaliados para "Negócios" da Apple Store[2]. Todavia, essa confiança sistêmica revela-se problemática ao atestar o abuso desse alicerce fundamental nas relações onlines, como por exemplo, na comprovação a partir de um vazamento de dados de uma rede de 200 mil pessoas que publicavam resenhas falsas na Amazon em troca de produtos (VEGA, 2021).

Outro exemplo, é a matéria do Washington Post que revelou a falta de controle da Apple Store, ao atestar que a loja virtual da empresa está repleta de aplicativos fraudulentos. O The Post analisou que o método utilizado por esses desenvolvedores fraudulentos para enganar os consumidores foi o sistema de avaliação, pois utilizavam-se de classificações inautênticas de clientes para subir no ranking da Apple Store, fornecendo uma sensação de legitimidade e confiança (ALBERGOTTI; ALCÂNTRA,

2021).

Observa-se que o sistema de avaliação transmite uma hiperconfiança no consumidor, pois o usuário acredita que pela avaliação a plataforma seja confiável. Nota-se, neste contexto, como o consumidor está realizando negócios baseados totalmente na confiança, sem conhecer o fornecedor e apenas se atendo em avaliações anteriores. Guilherme Mucellin ao tratar sobre o tema aduz que:

> Em outros termos, essa confiança, ou melhor, a hiperconfiança é a disposição das pessoas em cooperar em determinado sistema, mesmo que não se conheça os parceiros contratuais, como no caso do consumo compartilhado; é sopesar atuações passadas de internautas, não com base na proximidade, mas com base em todos os dados e informações pretéritos de comportamento estruturados em *scores* (MUCELIN,2020, grifos do autor).

Percebe-se como a conjuntura pandêmica influenciou na dependência dos indivíduos no ambiente digital. O contexto, agrava-se, ao perceber os riscos que a confiança sistêmica traz aos consumidores, especialmente, na intensificação das vulnerabilidades dos usuários, fazendo com que o usuário tenha que se expor para utilização de serviços inseguros.

Neste ambiente de confiança excessiva, é possível vislumbrar a responsabilização das plataformas com a quebra de expectativa do consumidor com o serviço ofertado, e nesse caso, é cabível a responsabilização de forma objetiva. Para a concretização dessa responsabilidade é importante a utilização do diálogo de fontes para tutelar os danos na internet, facilitando a proteção desse direito (MENDES, 2016, p 41).

Portanto, apresentada o agravamento das vulnerabilidades dos usuários e o contexto de confiança exacerbada na internet, será analisado como essa conjuntura torna o ambiente digital um local de riscos difusos, especialmente, no risco de violação dos dados pessoais dos usuários.

3.2 O tratamento negligente de dados, às falhas da empresa Zoom Vídeo Communication e a análise das violações sob a ótica do Código de Defesa do Consumidor, Lei do Marco Civil da Internet e Lei Geral de Proteção de Dados Pessoais

O Jornal El País em matéria intitulada "Problemas de privacidade e segurança sacodem sucesso do Zoom na pandemia de coronavírus" traz

que o The New York Times investigou o cruzamento de dados sem o consentimento e a devida informação aos usuários da plataforma que isso ocorria (GARCIA, 2020). A denúncia evidencia grave violação ao direito proteção dos dados pessoais e revela o tratamento negligente da empresa com os dados dos usuários. A reportagem explicou como ocorreu o tratamento negligente dos dados pessoas dos usuários:

> Uma investigação do *The New York Times* revelou nesta quinta-feira que o aplicativo contava com uma função de garimpagem de dados, acionada assim que a sessão era iniciada, e que unia automaticamente os nomes dos usuários e as direções de e-mail com os perfis do Linkedin. Tanto fazia se durante a chamada alguém utilizasse um pseudônimo ou optasse pelo anonimato. Se um usuário ativava o serviço Linkedin Sales Navigator, podia acessar os perfis desta rede social de outros participantes da videochamada ao clicar em um ícone junto aos seus nomes (GARCIA, 2020).

Ao analisar o caso à luz da legislação brasileira constata-se que às práticas do aplicativo Zoom Clouds Meetings descumprem os princípios da finalidade (art. 6º, I, da lei 13.709/18), adequação (art. 6º, II, da lei 13.709/18), necessidade (art. 6º, III, da lei 13.709/18), transparência (art. 6º, VI, da lei 13.709/18) e da responsabilização dos agentes de tratamento (art. 6º, X, da lei 13.709/18).

Além disso, a prática da empresa viola o disposto no artigo 4º do CDC, que protege a transparência e harmonia através da Política Nacional das Relações de Consumo. Também, viola-se o artigo 6º, III e os artigos 30º e 31º do CDC, bem como o disposto no artigo art. 2º, III, da LGPD. Trata-se de artigos que versam sobre o dever informacional ao consumidor, um dever de intrínseca ligação com a confiança nas relações de consumo, que inclusive, constituem deveres anexos as partes contratantes (BAGGIO, 2012, p. 51).

Sobre a necessidade do dever informacional, verifica-se que a informação possui grande valor aos fornecedores, pois são utilizadas como controle para adaptar às ofertas e influenciar às decisões da sociedade de consumo. Dessa forma, a proteção do dever de informação ao consumidor garante uma nova roupagem à oferta, permitindo o consentimento e decisão refletida (VERBICARO; MARTINS, 2018, p. 380).

No caso do cruzamento de dados, chama a atenção à falta do con-

sentimento (art. 5º, XII, lei nº 13.709/18) que o controlador precisa obter do consumidor para realizar o compartilhamento de dados com outras plataformas. Nesta situação, a plataforma Zoom viola a disposição sobre o compartilhamento preceituado pela LGPD, e viola o artigo 7º, VII, do MCI, que dispõe sobre o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei".

Um avanço da LGPD é a possibilidade do usuário saber qual entidade privada o controlador compartilhou os dados pessoais, conforme o preceituado pelo artigo 18º, VII da lei nº 13.709/18. Assim, garante-se ao consumidor o direito de informação sobre os seus dados, reforçando o vanguardismo da legislação ao compreender os dados como um direito personalíssimo. Desse modo, é possível que o consumidor afetado solicite às informações sobre o compartilhamento dos seus dados pessoais a empresa Zoom.

A reportagem do El País também traz o depoimento da advogada Natalia Martos, que elucida como houve a coleta de dados sem que o consumidor tenha consentido, conforme se nota:

> O comando em questão servia para que a própria empresa ativasse um kit de desenvolvimento de software um kit de desenvolvimento de software (mais conhecido pela sigla inglesa SDK) do Facebook que permitia tanto a rede social como o aplicativo recolher informações como o endereço do IP, tipo de aparelho, o sistema operacional, a localização e o fuso horário da conexão sem o consentimento dos usuários (GARCIA, 2020).

A reportagem jornalística do Estado de Minas, reforça a discussão sobre a fraqueza do sistema do aplicativo, pois relata um ataque de hackers que ocorreu na plataforma. O ataque permitiu que dados de vários usuários da plataforma fossem comercializados no mercado ilegal da internet, a "Dark Web" por preços irrisórios (ESTADO DE MINAS, 2020).

Outro caso que mostra a vulnerabilidade do consumidor em função da dependência da tecnologia e por questões técnicas, foi a revelação do diretor de tecnologia de uma empresa de segurança digital, que afirmou ao The Washington Post ter encontrado mais de 15 mil vídeos gravados por usuários da plataforma Zoom utilizando uma ferramenta gratuita na

internet (GARRET, 2020).

Neste caso relatado, verifica-se uma violação direta à proteção de dados, violando o artigo 7º, III, da lei nº 12.965 que dispõe sobre a inviolabilidade e sigilo das comunicações. Bem como, violação com os dados pessoais (art. 5º, I, da lei 13.709/18), mas principalmente os sensíveis (pelo art. 5º, II, da lei 13.709/18), pois conversas íntimas estão na rede sem o devido consentimento do art. 5º, XII da LGPD.

Diante dessas violações, percebe-se a importância da LGPD no ordenamento jurídico nacional, especialmente, em função das vulnerabilidades dos usuários para garantir sua proteção, evidenciada na utilização de serviços de videoconferência.

Neste sentido, serão abordados medidas cabíveis de controle, seja de garantia dos direitos à responsabilização das plataformas. Na seara administrativa, é possível a responsabilização da empresa Zoom Vídeo Communication pelos danos causados em solo nacional, pois o artigo 12º da Lei do Marco Civil da Internet dispõe sobre sanções administrativas no caso de violação da privacidade e sigilo das comunicações privadas (MENDES, 2016, p. 50).

Também, os consumidores lesados no país podem requerer a exclusão de dados tratados conforme o art. 18º, VI, da LGPD, através do direito de peticionar perante a Autoridade Nacional de Proteção de Dados que está tipificado no art. 18º, § 1º, da Lei nº 13.709/18 ou perante organismos de defesa do consumidor conforme o art. 18º, § 8º, da LPGD. Ressalta-se que, a defesa dos interesses e dos direitos pode ser tutelada de forma individual ou coletiva, como preceitua o art. 22º da LGPD.

3.3 Zoomboming

Foi denunciada pelos usuários a ação que ficou conhecida como "Zoomboming". A ação é caracterizada quando uma pessoa indesejável entra em uma reunião aberta, assim a transmissão é invadida. Os invasores colocam conteúdos inadequados como pornografias ou até o aparecimento do intruso, como por exemplo, o caso que ocorreu na Noruega, onde um homem adulto nu entrou em uma aula de alunos menores de idade, ensejando o abandono do aplicativo pela escola (ROHR, 2020).

O evento "Soluções de saúde para COVID-19 panorama das pesquisas no Brasil e nos EUA e sistema imune em tempos de confinamento" foi

alvo dos "zoomboming". Os intrusos colocaram imagens e saudações nazistas na plataforma do Zoom, constrangendo todos que participavam da conferência. Foi esclarecido por Adriana Cohen, gestora de comunicação da empresa contratada para fazer o evento que: "não se tratava de uma live pública, pois ela foi feita dentro de um plano comercial adquirido, ou seja, não era gratuita e, teoricamente, deveríamos estar protegidos deste tipo de ataque" (SOPRANA, 2020).

Observa-se nesses casos, especialmente, a vulnerabilidade técnica dos usuários que é intensificada pela dependência da situação, notando-se a influência da vulnerabilidade situacional e técnica nas ações do zomboming. Desse modo, o usuário não dispõe de técnicas e informações apropriada para defender-se de ataques de intrusos, colocando-se em situação extremada de vulnerabilidade.

As ações dos invasores demonstram clara violação da vida privada dos usuários, sua imagem e intimidade (art. 5º, X, CF) e a inviolabilidade das comunicações privadas e o seu sigilo (art. 7º, II, lei nº 12.965/14). Os casos ilustram às vulnerabilidades enfrentados pelo consumidor na utilização de serviços de videoconferência, que são permeados por uma confiança sistêmica, reforçando a necessidade de controle no ambiente digital.

Verifica-se, portanto, que além das negligencias no tratamento de dados, a plataforma Zoom é desprotegida quanto a ataque de hackers, assim expõem-se a imagem dos usuários por causa da fraqueza do seu sistema, quebrando às expectativas legítimas dos usuários com a confiabilidade e segurança do serviço de videoconferência.

3.4 A Desconfiança na empresa Zoom Vídeo Comunication faz com que Google e órgãos de diversos governos façam advertências, limitem ou proíbam o uso da sua plataforma

Diante do cenário de falta de confiança das instituições com o aplicativo, o Instituto Nacional de Segurança Cibernética, da Espanha, publicou um comunicado advertindo o uso da plataforma pelo sistema Windows, pois seria passível que hackers tivessem acesso a arquivos do computador de quem está utilizando a plataforma (GARCIA, 2020).

Em matéria jornalística intitulada "Zoom entra na mira da justiça de Nova York por problemas de segurança" a secretaria de justiça, ao anali-

sar todas as práticas da empresa Zoom Vídeo Communication, concluiu sobre a insegurança da plataforma. Foram solicitados esclarecimentos a empresa em carta enviada pela secretária de justiça de Nova York. Na carta à organização, a procuradora geral Letita James, pede que a empresa especifique que tipo de informação o aplicativo recolhe, com que propósitos e as quais outras entidades os dados dos consumidores são entregues (ÉPOCA, 2020).

Ainda no cenário dos Estados Unidos da América, o Senado baniu a transmissão pelo aplicativo Zoom pelas falhas no sistema, demonstrando desconfiança das instituições com o serviço ofertado (MEHTA, 2020). Seguindo os passos e demonstrando preocupação com a segurança do aplicativo, o Ministro de Relações Exteriores, da Alemanha, restringiu o uso do aplicativo pelo órgão de relações exteriores em conversas confidenciais após matéria do jornal "Handelsblatt newspaper" concluir que o software do Zoom tem uma grande fraqueza (REUTERS, 2020).

Com restrições mais rigorosas, o governo de Taiwan proibiu o uso do aplicativo por todas as agências governamentais, assim como as escolas que utilizavam o serviço. Isso ocorreu devido à desconfiança com a segurança e principalmente pelo fato dos servidores de criptografia do aplicativo ficar na China. Com as divergências políticas entre China e Taiwan, o governo de Taiwan optou pela proibição total do aplicativo (ALECRIM, 2020).

Além de órgãos de diversos países, a empresa GOOGLE proibiu os seus funcionários de utilizarem o Zoom em seus dispositivos. A equipe de segurança da empresa enviou um e-mail aos funcionários notificando o fim do uso do aplicativo, conforme aponta a matéria ao reportar que "dentro da empresa, os funcionários que recorrem ao Zoom para conversar com familiares e amigos só poderão fazê-lo a partir de agora via navegador (não exige a instalação de um cliente no computador) ou celular" (ALECRIM, 2020).

No Brasil, a Agência Nacional de Vigilância Sanitária (ANVISA) emitiu um comunicado no dia 06 de abril, informando que proibiu o uso do aplicativo Zoom. No comunicado a ANVISA informou sobre o bloqueio da plataforma:

> A área de Tecnologia da Informação (TI) da Anvisa participa de diversos *sites* especializados em segurança, com especia-

> listas do mundo todo e de diversas especialidades, a fim de se manter atualizada sobre os principais acontecimentos da área de segurança e sobre os alertas de vulnerabilidade em ferramentas largamente utilizadas. Isso permite a adoção de medidas de segurança de forma rápida e proativa, identificando possíveis vulnerabilidades nas ferramentas utilizadas internamente pela Anvisa.
>
> Nos *sites* em questão, foram apontadas vulnerabilidades do Zoom Meeting que, quando exploradas por *hackers*, permitem o acesso não autorizado à câmera e ao microfone, viabilizando o roubo das credenciais dos usuários e de informações trocadas nas reuniões (BRASIL, 2020).

Apesar de todos os fatos apresentados sobre as fraquezas do sistema da plataforma Zoom Clouds Meetings, da empresa Zoom Vídeo Communication, o aplicativo continua operando e com grande popularidade. Evidencia-se a vulnerabilidade do consumidor no ambiente online ao utilizar serviços postos no mercado que não garantem segurança na medida da sua confiabilidade.

O caso do Zoom reforça a preocupação com os dados no mundo inteiro, pois verifica-se como às vulnerabilidades dos consumidores dificultam ainda mais a proteção dos seus dados pessoais na internet. Intensifica-se a preocupação devido às empresas atuarem de maneira globalizada e cada país possui sua legislação específica quanto à proteção dessas informações.

Com o alto nível de intromissão das empresas na vida privada dos indivíduos, às vulnerabilidades dos consumidores ficam mais evidentes e ao mesmo tempo às empresas buscam se beneficiar dessa situação. Como pode ser observado no caso de aplicativos que acessam indevidamente o microfone do dispositivo do usuário sem sua autorização, assim como a localização sem informar adequadamente que isso ocorre no momento da contratação (BARRETO, 2019).

Também, nota-se essa intromissão na privacidade do consumidor quando um site realiza a análise do perfil de consumo a partir do rastreamento dos passos do consumidor no ambiente virtual, permitindo ao fornecedor oferecer bens e serviços que o consumidor tenha interesse. Os dados possibilitam às empresas oferecer serviços e produtos personalizados ao consumidor, sendo muito provável que a oferta irá interessar ao

destinatário, atuando como um instrumento importante para a competição no comércio digital (VERBICARO; MARTINS, 2018, p. 378).

Diante das análises sobre a empresa Zoom Vídeo Communication, ilustra-se que o consumidor é a parte mais desprotegida na relação de consumo digital. Às suas vulnerabilidades estão acentuadas nesse ambiente, assim, torna-se fulcral a ação ampla por parte do Estado para promover a tutela de direitos fundamentais do cidadão, porém, verificam-se debilidades estatais para a efetivação dessa matéria.

4. A INÉRCIA ESTATAL NA PROTEÇÃO DE DADOS PESSOAIS E AÇÕES PROPOSITIVAS

Às vulnerabilidades do consumidor nas relações consumeristas agravam-se com a insuficiência estatal. Isto decorre da falta de ação do Estado sobre a matéria, e principalmente, da lentidão para que ocorresse a vigência da legislação específica. A LGPD foi promulgada em 2018, entretanto só em setembro de 2020 que a lei tornou-se vigente.

No dia 26 de agosto de 2020, o Senado Federal tratou a medida provisória nº 959/2020 que adiava o início da vigência da LGPD conforme o art. 4º. Ocorre que o referido artigo foi considerado prejudicial, assim, o adiamento nele previsto não aconteceu. No entanto, a LGPD não entrou em vigor imediatamente, mas somente após sanção ou veto do restante do projeto de lei de conversão, conforme o do art. 62º, § 12 da Constituição Federal, o que ocorreu apenas no final de 2020 (SENADO FEDERAL, 2020).

Notou-se a morosidade das instituições competentes para definir a vigência da lei, o que demonstrou como a inércia estatal é prejudicial ao consumidor na tutela dessa matéria. Está inércia também pode ser observada no exemplo do caso do veto presidencial sobre o artigo que regulamentava a criação da "Autoridade Nacional de Proteção de Dados - ANPD" quando a LGPD foi promulgada em 2018, atrasando a constituição da autoridade fundamental para a aplicabilidade da lei.

Um ano depois da promulgação da LGPD, houve a afirmação da Autoridade Nacional de Proteção de Dados, pela lei nº 13.853/19, como órgão da administração direta, vinculada a presidência da república. A ANPD terá natureza transitória e poderá ser transformada em autarquia vinculada à Presidência da República após dois anos, dependendo do cri-

tério do governo (SENADO FEDERAL, 2019).

Percebe-se que a inércia estatal para a vigência da lei e o real funcionamento da ANPD produz efeitos negativos na proteção dos dados e privacidade virtual (VERBICARO; VIERA, 2021, p. 209). Ressalte-se que, o desafio para a efetivação da LGPD em solo nacional perpassa pela necessidade do funcionamento da Autoridade Nacional de Proteção de Dados e a sua independência técnica e financeira.

A criação da ANPD no Brasil se caracteriza por uma morosidade que causa insegurança jurídica. Essa omissão revela a inércia do Estado na regulamentação de um tema complexo e importante. Essa insuficiência estatal resulta na falha do dever de fiscalização do Estado sobre as empresas no mundo virtual, visto que essa competência é da ANPD conforme o artigo 55-Jº, IV, da LGPD. Desse modo, a ANPD mostra um desenvolvimento lento e uma atuação insipiente na sua competência regulamentadora, fiscalizadora e educativa até o momento.

4.1 Ações propositivas

Às leis como o CDC, a Lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais garantem um diálogo de fontes para a responsabilização das plataformas que violam os direitos assegurados dos consumidores.

A partir do diálogo de fontes e da teoria da confiança nas relações de consumo, é possível que o usuário busque a responsabilização de maneira objetiva em função da frustração das legítimas expectativas do consumidor com a segurança dos seus dados pessoais (BAGGIO, 2012, p. 99).

Logo, nos casos relatos da empresa Zoom, onde ocorre às frustrações das legítimas expectativas do consumidor quanto ao tratamento de dados conforme às legislações e às falhas de segurança que expõem informações privadas, devem ensejar reparação ao vulnerável pela confiança quebrada.

Essa possibilidade de responsabilização fica mais evidente ao perceber a confiança como um valor economico e instigado pelos players. Desse modo, tratamentos de dados ilegais, falhas de segurança que resultem em vazamento de dados ou danos à imagem e personalidade dos usuários devem ser tutelador a partir da frustração das legítimas expectativas dos consumidores com as plataformas.

Neste sentido, a utilização da tutela coletiva conforme o art. 83 do CDC, mostra-se como um caminho para a responsabilização e reparação dos danos coletivos por casos similares ao do Zoom. Ressalte-se que, a LGPD reafirma a possibilidade de utilização da tutela coletiva nesta matéria conforme o tipificado no seu art. 22º, caput.

No Brasil, a tutela coletiva é cabível nas relações consumeristas, conforme o artigo 1º, II, da lei nº 7.347/85 (LACP). O instituto da tutela coletiva possui amplo alcance no ordenamento pátrio, admitindo-se provimentos jurisdicionais, condenatórios, constitutivos, declaratórios, executivos lato sensu e mandamentais. Ressalta-se que a tutela coletiva admite a inversão do ônus financeiro da prova ao demandando, um importante e necessária medida para a defesa do vulnerável nesses casos. Quanto aos seus efeitos, percebe-se um sistema híbrido no âmbito dos direitos individuais homogêneos, pois o indivíduo do grupo pode optar em continuar na ação coletiva (right to opt in) ou escapar dos efeitos da decisão da ação coletiva (right to opt out) (VERBICARO, 2017, p. 98/99).

O Termo de Ajustamento de Conduta (TAC) inserido pelo artigo 113º do CDC, que instituiu o parágrafo 6º no artigo 5º da LACP, também se mostra como uma via interessante para solucionar o conflito de violação de danos coletivos, pois se caracteriza por ser uma espécie de transação coletiva no âmbito extrajudicial. O art. 82º do CDC traz os legitimados que detêm competência para a celebração desse instituto para efetivar obrigações específicas de fazer, não fazer, dar, bem como pecuniárias (VERBICARO, 2017, p. 105).

Importante ressaltar que o TAC só pode ser redigido por órgão público, excluindo às associações representativas de defesa do consumidor, apesar de que muitas se fazem presentes como intervenientes ou testemunhas das obrigações estabelecidas no termo. Entretanto, defende-se que a execução coletiva do TAC na via judicial pode ser de iniciativa de outros legitimados, caso se verifique que o órgão responsável pela formalização do instrumento protele ou se recuse a dar efetividade às obrigações acordadas. Nota-se que, o TAC é uma espécie de reconhecimento de má conduta por parte do infrator, assumindo a responsabilidade pelo ato ilícito e, também, comprometendo-se em reparar os danos causados à coletividade (VERBICARO, 2017, p. 106/107).

Além disso, os usuários podem fazer uso do art. 18 da LGPD e so-

licitar a informação sobre dados tratados, compartilhados e até solicitar a exclusão de dados com consentimento mediante petição perante a Autoridade Nacional de Proteção de Dados, conforme o tipificado no art. 18º, § 1º, da lei 13.709/18 ou perante organismos de defesa do consumidor conforme o art. 18º, § 8º, da LPGD.

Percebe-se com o caso exposto, que mesmo com os avanços legislativos na proteção de dados pessoais e da privacidade virtual, o consumidor está em situação desfavorável na relação. Além disso, o Estado mostra-se moroso para instituir um controle no ambiente online, restando ao consumidor agir de forma proativa para tutelar seus direitos. Neste sentido, às ações propositivas através de um diálogo de fontes ou de uma atuação dos legitimados do art. 83º do CDC mostram-se como caminhos interessantes e viáveis para a reparação de danos causados por serviços de videoconferência.

5. CONSIDERAÇÕES FINAIS

Percebe-se que, com a imersão tecnológica do consumidor há uma (hiper)confiança induzida no mundo digital devido à utilização de técnicas pelas empresas que seduzem novos usuários com a imagem de segurança e confiabilidade. Isto decorre da confiança possuir um valor economico para às empresas, permitindo maior fiabilidade no mercado de consumo. Tal cenário de confiança sistêmica agrava às vulnerabilidades dos consumidores, fazendo com que estes estejam em situação ainda mais desfavorável perante os players. Desse modo, vislumbra-se uma responsabilidade pela confiança dos fornecedores em função da frustração das legítimas expectativas dos usuários com a proteção dos seus dados pessoais a partir de um diálogo de fontes.

Nota-se que a partir da promulgação da LGPD, a tutela dos dados e da privacidade virtual ganha uma nova dimensão no Brasil, contudo, com o agravamento das vulnerabilidades dos usuários, é imprescindível um controle mais profundo no ambiente virtual. Sendo assim, a proteção da privacidade é fundamental para reprimir violações de direitos no ambiente digital, pois os dados pessoais constituem parcela da privacidade do titular, possuindo caráter personalíssimo e de direito fundamental na sociedade da informação.

Ao analisar o caso da empresa Zoom Vídeo communication, per-

cebe-se às vulnerabilidades que o consumidor enfrenta nos serviços de videoconferência, demonstrando como este é a parte mais desprotegida na relação. Os motivos para o acentuamento das vulnerabilidades decorre das insuficiências informacionais dos fornecedores, do tratamento negligente de direitos fundamentais do indivíduo, bem como às rotineiras falhas de segurança que o consumidor é exposto.

Depreende-se que, a inércia estatal causa uma insegurança sobre o tema, acentuando às vulnerabilidades dos usuários. Em decorrência dessa inércia, a fiscalização sobre às empresas no mundo virtual não ocorre, visto que a competência é de uma autoridade que possui uma atuação insipiente, gerando um ambiente digital de altos riscos aos usuários.

Conclui-se, portanto, que além do agravamento das vulnerabilidades dos usuários ao utilizar serviços de videoconferência, evidenciado no contexto da pandemia da COVID-19, a inércia estatal acentua ainda mais essa problemática. Em função dessa conjuntura, verifica-se a importância da tutela dos dados pessoais nas relações consumeristas na internet para promover o direito constitucional da privacidade e de proteção ao consumidor.

Para tanto, é necessário resolver a morosidade de atuação da ANPD, mas também devido a essa situação, o consumidor deve assumir à dianteira para buscar a responsabilização das plataformas, abandonando a figura de expectador, esperando o Estado, para uma figura de ator na resolução dos conflitos consumeristas na internet. Desse modo, o vulnerável deve buscar o judiciário, visto que esse apresenta-se como a última salvaguarda para proteção de direitos fundamentais em ambiente de pouco controle.

Neste sentido, o consumidor dispõe da tutela coletiva que apresenta benefícios como, a inversão do ônus da prova ao demandando e a possibilidade de se esquivar dos efeitos da decisão coletiva. Além da via judicial, há duas formas extrajudiciais para tutelar os direitos violados: o art. 18 da LGPD que permite solicitar informações ao operador sobre a existência de tratamento de dados, compartilhamento e até a exclusão, e o TAC que se caracteriza por ser uma transação coletiva no âmbito extrajudicial, que impõem obrigações específicas às empresas.

REFERÊNCIAS

ALBERGOTTI, Reed; ALCÂNTARA, Chris. Apple Store bem controlada

da Apple está repleta de golpes. **The Washington Post.** Estados Unidos. 06 de Junho de 2021. Disponível em: App Store da Apple tem muitos golpes - The Washington Post. Acesso em 05 de Jun de 2021.

ALECRIM, Emerson. Zoom é banido até do Google e chama especialistas para deter a crise. **Technoblog.** São Paulo. 09 de Abril de 2020. Disponível em: https://tecnoblog.net/333553/zoom-banido-google-contrata-especialistas-seguranca-crise/ . Acesso em: 27 de Mai de 2021.

ALL, Maria Paula. Confiança no Mercado eletrônico e a Proteção do consumidor (um estudo dos negócios jurídicos de consumo no comércio eletrônico) por Claudia Lima Marques. **Caderno de pós-graduação em Direito- PPGDir/UFRGS**. Número 2. p 285-293. Porto Alegre. Mar 2005. Disponível em: Confiança no Comércio Eletrônico e a Proteção do Consumidor (Um Estudo dos Negócios Jurídicos de Consumo no Comércio Eletrônico) por Claudia Lima Marques | Semantic Scholar. Acesso em 05 Jul 2021.

ARTONI, Patrícia. **Vulnerabilidade situacional afetando a intenção comportamental: Um estudo no setor de serviços automotivos.** 2013. 132 f. Tese (Doutorado em Administração de empresas) – Faculdade Getúlio Vargas, São Paulo, 2013. Disponível em: bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/11104/Tese_PatriciaReginaCaldeiraDareArtoni.pdf?sequence=1. Acesso em 05 de Jul 2021.

Aplicativo Zoom reforça segurança após problemas. **Estado De Minas** Internacional. Belo Horizonte. 16 de Abr 2020. Disponível em: https://www.em.com.br/app/noticia/internacional/2020/04/16/interna_internacional,1139342/aplicativo-zoom-reforca-seguranca-apos-problemas.shtml . Acesso em 27 de Maio 2021.

BAGGIO, Andreza Cristina. **O direito do consumidor brasileiro e a teoria da confiança.** São Paulo. Editora Revista dos Tribunais, 2012.

BARRETO, Diogo. Liga espanhola multada por espiar telemóveis**. Jorna Sábado- PT**. Portugal. 12 de Maio de 2019. Disponível em: https://www.sabado.pt/mundo/europa/detalhe/liga-espanhola-multada-por-espiar-telemoveis. Acesso em 23 Ago 2021.

BARROSO, Luis. Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa. **Revista De Direito Administrativo**, nº *235*, p. 1-36. Jan/Mar 2004. Disponível em: Vis-

ta do Colisão entre Liberdade de Expressão e Direitos da Personalidade. Critérios de Ponderação. Interpretação Constitucionalmente Adequada do Código Civil e da Lei de Imprensa (fgv.br). Acesso em 08 Jul 2021.

BRASIL. Lei nº 13.709, 14 de Agosto de 2018**. Institui a Lei Geral de Proteção de Dados.** Diário Oficial da União Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 28 de Jun 2021.

BRASIL. Lei nº 12.965, 23 de Abril de 2014. **Institui Marco Civil da Internet**. Diário Oficial da União Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 28 de Jun 2021.BRASIL. Lei nº 8.078, 11 de Setembro de 1990**. Institui o Código do Consumidor.** Diário Oficial da União Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em 29 de Jun 2021.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988

BRASIL. Lei nº 7.347, de 24 de Julho de 1985. *Lei de Ação Civil Pública***.** Diário Oficial da União Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm . Acesso em 05 de Jul 2021.

BRASIL. Ferramenta Zoom é bloqueada na ANVISA**.** *Portal da Agência Nacional De Vigilância Sanitária.* Brasília. 06 de Abr 2020. Disponível em: http://portal.anvisa.gov.br/noticias/-/asset_publisher/FXrpx9qY7FbU/content/solucao-zoom-bloqueada-na-anvisa/219201 . Acesso em 27 de Jun de 2021.

BUSVINE, Douglas. German foreign ministry restricts use of Zoom over security concerns. **Reuters**. United States. 8 de Abr 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-germany-zoom/german-foreign-ministry-restricts-use-of-zoom-over-security-concerns-report-idUSKBN21Q1SC. Acesso em: 27 de Mai 2021. Conheça a história do criador da Zoom que ganhou 4 bilhões com a pandemia. **Jornal Pequenas Empresas Grande Negócios**. São Paulo. 25 de abr. de 2020. Disponível em: https://revistapegn.globo.com/Startups/noticia/2020/04/coronavirus-conheca-historia-do-criador-da-zoom-que-ganhou-us-4-bilhoes-com-pandemia.html. Acesso em: 13 Mai 2021.

DATA SCIENCE ACADEMY. Análise de dados e fatos- a cronologia do coronavírus covid-19. **Data Science Academy**. 23 Mar de 2020.

Disponível em: http://datascienceacademy.com.br/blog/analise-de-dados-e-fatos-a-cronologia-do-coronavirus-covid-19/. Acesso em: 28 Jun 2021.

DE CASTRO, Bárbara. Direito digital na era da Internet das coisas- O direito à privacidade e o sancionamento da Lei Geral de Proteção de Dados Pessoais. Caderno Âmbito jurídico. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/direito-digital-na-era-da-internet-das-coisas-o-direito-a-privacidade-e-o-sancionamento-da-lei-geral-de-protecao-de-dados-pessoais. Acesso em 26 Jun 2021.

GARCIA, Jorge. Problemas de privacidade e segurança sacodem sucesso do zoom na pandemia de coronavírus**. Jornal EL País.** São Paulo. 07 de Abr 2020. Disponível em: https://brasil.elpais.com/retina/2020-04-07/problemas-de-privacidade-e-seguranca-sacodem-sucesso-do-zoom-na-pandemia-de-coronavirus.html. Acesso em: 27 de Mai 2021.

GARRET, Filipe. Zoom é seguro? Veja dicas para usar o programa de videoconferência. **TechTudo.** São Paulo. 06 de Abr de 20200. Disponível em: https://www.techtudo.com.br/listas/2020/04/zoom-e-seguro-veja-dicas-para-usar-o-programa-de-videoconferencia.ghtml. Acesso em: 27 de Mai 2021.

GONÇALVES, Antunes Fábio; GONÇALVES Antunes Patrícia. A evolução do conceito de consumidor e o princípio da vulnerabilidade. Caderno Âmbito jurídico. Disponível em: https://ambitojuridico.com.br/edicoes/revista-164/a-evolucao-do-conceito-de-consumidor-e-o-principio-da-vulnerabilidade/. Acesso em: 04 Jul 2021.

MENDES, Laura Schertel**. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis.** Caderno Especial LGPD. p. 35-56. São Paulo: Ed. RT, novembro 2019. Disponível em: https://www.bing.com/search?q=A+Lei+Geral+de+Proteção+de+Dados+Pessoais%3A+um+modelo+de+aplicação+em+três+níveis.&cvid=bff2b7c5ef18417d97fd36380387a82e&aqs=edge..69i57j69i64.424j0j9&FORM=ANAB01&PC=DCTS. Acesso em 05 Jul 2021.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**. vol. 106.. p. 37-69. São Paulo: Ed. RT, jul.-ago. 2016. Disponível em: O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor | Revista de Direito do Consumidor (emnuvens.com.br). Acesso

em 05 Jul 2021.

MIRAGEM, Bruno; MARQUES, Claudia Lima. **O novo direito privado e a proteção dos vulneráveis.** São Paulo: Ed Revista dos Tribunais, 2014.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais**. 8. ed. São Paulo: Revista dos Tribunais, 2016.

MEHTA, Ivan. US Senate reportedly bars its members from using Zoom. **The Next Web**. United States. 10 de abril de 2020. Disponível em: https://thenextweb.com/us/2020/04/09/us-senate-reportedly-bars-its-members-from-using-zoom/. Accesso em 27 de Mai 2021.

MUCELIN, Guilherme. Conexão online e hiperconfiança: os players da economia do compartilhamento e o Direito do Consumidor. São Paulo: RT, 2020. [*e-book*; cap. 4].

ROHR, Altieres. Porque o Zoom é alvo de desconfiança e quais são as alternativas para videoconferência?. **Globo-G1**. Rio de Janeiro. 07 Abr 2020. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/04/07/por-que-o-zoom-e-alvo-de-desconfianca-e-quais-sao-as-alternativas-para-videoconferencia.ghtml. Acesso em: 27 de Mai 2021.

RODRIGUES, Yuri Gonçalves dos Santos. FERREIRA, Keila Pacheco. A privacidade no ambiente virtual: avanços e insuficiências da Lei Geral de Proteção de Dados no Brasil (Lei 13.709/18*)*. **Revista de Direito do Consumidor.** São Paulo:2019. Vol. 122/2019, p. 181 - 202. Disponível em: A Prnaci Dade No Ambiente Virtual: Avanços E Insuficiências Da Lei Geral De Proteção De Dados No Brasil (Lei 13.709/18) | Revista de Direito do Consumidor (emnuvens.com.br). Acesso em 05 Jul 2021.

SOPRANA, Paula. Imagens nazistas invadem entrevista coletiva com imunologistas brasileiros no Zoom. **Jornal Folha De São Paulo**. São Paulo. 6 de abr. de 2020. Disponível em: https://www1.folha.uol.com.br/mercado/2020/04/coletiva-de-imprensa-com-imunologistas-brasileiros-e-alvo-de-ataque-no-zoom.shtml?origin=facebook#_=_. Acesso em: 27 de Mai 2021.

SENADO FEDERAL. Lei que cria Autoridade Nacional de Proteção de Dados é sancionada com vetos. **Senado Federal.** Brasília. 09 de

Jul 2019. Disponível em: https://www12.senado.leg.br/noticias/materias/2019/07/09/lei-que-cria-autoridade-nacional-de-protecao-de-dados-e-sancionada-com-vetos. Acesso em 23 Jun 2021.

SENADO FEDERAL. Nota de esclarecimento- Vigência da LGPD. **Senado Federal.** Brasília. 27 de Ago 2020. Disponível em: https://www12.senado.leg.br/assessoria-de-imprensa/notas/nota-de-esclarecimento-vigencia-da-lgpd . Acesso em 05 Jul 2021. VEGA, Guillermo. Desvendada rede de 200.000 pessoas que publicavam resenhas falsas na Amazon em troca de produtos grátis. **Jornal El país**. Brasil. 2021. Disponível em: Desvendada rede de 200.000 pessoas que publicavam resenhas falsas na Amazon em troca de produtos grátis | Tecnologia | EL PAÍS Brasil (elpais.com). Acesso em 29 de Jun 2021.

VERBICARO, Dennis. Privacidade e segurança no comércio eletrônico em tempos de Covid-19. **Canal PUC-PR Youtub**e. 1 vídeo (22m- 52 m) Disponível em: PUCPR - #3 - Privacidade e segurança no comércio eletrônico em tempos de Covid-19 - YouTube . Acesso em 1 de Jul 2021.

VERBICARO, Dennis. Resgatando a importância da transação coletiva de consumo no Brasil. Revista Jurídica UNICURITIBA. Vol. 03, n°. 48. Curitiba. 2017. p. 94-117. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Juridica UNICURITIBA_n.48.05.pdf . Acesso em 23 Jun de 2021.

VERBICARO, Dennis; Martins, Ana Paula Pereira. A contratação eletrônica de aplicativos virtuais no Brasil e a nova dimensão da privacidade do consumidor. **Revista de Direito do Consumidor.** Vol. 116.. p. 369-391. São Paulo: Ed. RT, mar. – abr. 2018. Disponível em: A contratação eletrônica de aplicativos virtuais no Brasil e a nova dimensão da privacidade do consumidor | Revista de Direito do Consumidor (emnuvens.com.br). Acesso em 05 Jul 2021.

Zoom entra na mira da justiça de Nova York por problemas de segurança. **Jornal Época Negócios**. São Paulo. 13 de Abr 2020. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2020/04/zoom-entra-na-mira-da-justica-de-nova-york-por-problemas-de-seguranca.html Acesso em: 27 de Mai 2021. WARREN, Samuel D; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review** 193.1890. p. 193-220.Disponível em: http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 26 de

Jun 2021.

ZUBOFF, Shoshana. **The age of surveillance capitalism.** PublicAffairs. 2019. [*e-book*; cap. 1].

WEINGARTEN, Célia. El valor economico de la confianza para empresas y Consumidores. **Revista de Direito do Consumidor.** vol. 33. São Paulo: ED RT | Jan - Mar / 2000. p. 33 – 50.

'Notas de fim'

1 A COVID-19 é a denominação do vírus sars-cov-2 que surgiu em 2020. A descoberta do vírus respiratório surgiu em meados de Fevereiro na cidade de Wuhan na China, devido à alta denuncia de uma pneumonia de causa desconhecida. O vírus possui alta capacidade de contágio, se proliferando em diversos países do mundo e em função disso houve a decretação de pandemia pela Organização Mundial da Saúde. Para que houvesse a contenção da propagação do vírus foi necessária à adoção do isolamento social. Sendo assim, ocorreu o fechamento de diversas atividades econômicas que não eram essenciais para a manutenção da vida com a finalidade de diminuir a locomoção e aglomeração dos cidadãos. Disponível em <http://datascienceacademy.com.br/blog/analise-de-dados-e--fatos-a-cronologia-do-coronavirus-covid-19/> Acesso em 28 Ago 2020.

2 Conforme nota-se no site da Apple Store. Disponível em< ⁋ ZOOM Cloud Meetings na App Store (apple.com)> Acesso em 04 Agosto 2021.