(HIPER)VULNERABILIDADE DOS USUÁRIOS DE AMBIENTES DIGITAIS: POSSIBILIDADE NO METAVERSO E MECANISMOS PROATIVOS PARA A PROTEÇÃO DE DADOS PESSOAIS E INFORMAÇÃO ADEQUADA

Nádia Carolina Brencis Guimarães
Aluna regular do Programa de Mestrado em Direito Negocial da Universidade Estadual de Londrina (UEL). Vinculada ao Projeto de Pesquisa Responsabilidade Civil e Dano: Instrumentos e Critérios Adequados à Parametrização do Quantum Ressarcitório, Reflexos Socioeconômicos e o Escopo de Efetivação dos Direitos e Interesses dos Tutelados da Universidade Estadual de Londrina (UEL).
ORCID: https://orcid.org/0000-0002-0828-1965
Email nadiabrencis@gmail.com

Ana Cláudia Corrêa Zuin Mattos do Amaral
Doutora em Direito Civil Comparado pela PUC/SP. Mestre em Direito Negocial pela Universidade Estadual de Londrina/PR. Professora e pesquisadora do Programa Mestrado e Doutorado em Direito Negocial da Universidade Estadual de Londrina/PR.
ORCID: https://orcid.org/0000-0001-8574-0347
E-mail anaclaudiazuin@live.com

Recebido em: 03/02/2023
Aprovado em: 31/07/2023

RESUMO

O Código de Defesa do Consumidor tem como princípio a vulnerabilidade dos consumidores em razão da assimetria contratual, a qual é mais acentuada quando utilizados meios informáticos, em razão do tratamento de dados pessoais pelos fornecedores. Embora o consentimento, na LGPD, seja uma das bases legais para o tratamento de dados, há dificuldades para que seja livre e esclarecido, decorrentes da ausência de compreensão adequada das consequências do tratamento de dados. O objetivo da pesquisa é analisar se há hipervulnerabilidade dos usuários por limitações à autodeterminação informativa, e como equalizar a relação consumidor-fornecedor em ambientes digitais como o metaverso. Utilizando-se de pesquisa teórico-bibliográfica e dedutiva identificou-se que a condição de hipervulnerável corresponde à uma vulnerabilidade maior devida a condições pessoais, que deixam a pessoa mais exposta à lesão, exigindo do fornecedor uma conduta mais cuidadosa. E a utilização do metaverso potencializará a coleta de dados pessoais pela observação. Doutrinariamente, a maior vulnerabilidade dos usuários de ambientes digitais pode ser identificada sob um viés subjetivo, fundamentado na condição pessoal do usuário que o torne mais suscetível à lesão. Ou sobre um viés objetivo em que todos os usuários são hipervulneráveis em razão da inferioridade informacional. Independentemente da concepção, exige-se do fornecedor e do Poder Público condutas proativas direcionadas ao empoderamento dos usuários para exercerem a autodeterminação informativa, tanto pela própria arquitetura dos ambientes virtuais quanto por Políticas Públicas de esclarecimento aos usuários sobre as implicações do tratamento de dados pessoais.

Palavras-Chave: Hipervulnerabilidade. Metaverso. Proteção de dados pessoais.

(HYPER)VULNERABILITY OF USERS OF DIGITAL ENVIRONMENTS: POSSIBILITY IN THE METAVERSE AND PROACTIVE MECHANISMS FOR THE PROTECTION OF PERSONAL DATA AND ADEQUATE INFORMATION

ABSTRACT

The Consumer Defense Code has as its principle the vulnerability of consumers due to contractual asymmetry, which is more accentuated when using computer means, due to the processing of personal data by suppliers. Although consent, in the LGPD, is one of the legal bases for data processing, there are difficulties for it to be free and clear, due to the lack of adequate understanding of the consequences of data processing. The objective of the research is to analyze whether there is hypervulnerability of users due to limitation to informative self-determination, and how to equalize the consumer-supplier relationship in digital environments such as the metaverse. Using theoretical-bibliographic and deductive research, it was identified that a hypervulnerable condition corresponds to a greater vulnerability required by personal conditions, which leave the person more exposed to injury, motivated by the provider of a more careful conduct. And the use of the metaverse will enhance the collection of personal data through observation. Doctrinally, the greater vulnerability of users of digital environments can be identified under a subjective bias, based on the personal condition of the user that makes him more susceptible to injury. Or about a goal where all users are hypervulnerable due to informational inferiority. Regardless of the design, proactive conduct is required from the supplier and the Public Power aimed at empowering users to exercise informative self-determination, both through the architecture of virtual environments and through Public Policies to clarify users about the implications of processing personal data.

Keywords: Hypervulnerability. Metaverse. Data protection.

1 INTRODUÇÃO

Hodiernamente, vive-se em uma sociedade de consumo, na qual este é incentivado como resposta à elevada produção de bens, reflexo das revoluções industriais. Da produção artesanal e praticamente personalizada, passou-se ao consumo de massa em que há padronização e automatização da produção e do fornecimento, erigindo o fornecedor à posição de superioridade por ter o domínio de diversos elementos na circulação de bens.

Portanto, os consumidores em razão da assimetria contratual estão em situação de vulnerabilidade se comparados aos fornecedores. Embora controverso, utiliza-se a hipervulnerabilidade para designar as ocasiões em que o consumidor por uma condição pessoal está mais suscetível a lesões.

A utilização dos ambientes digitais tem aumentado a cada dia, inclusive, com a utilização do metaverso. Consequentemente, os usuários estão expostos a diversas situações de violações de dados pessoais, porque apesar de consentirem com o tratamento de seus dados, não há efetiva autodeterminação informativa. Isso porque o consentimento, enquanto base legal

para o tratamento de dados, nem sempre é efetivamente livre e esclarecido. Muitas vezes, os usuários buscando satisfazer as necessidades imediatas de uso do produto ou serviço digital, não compreendem adequadamente as consequências da autorização para o tratamento de dados.

Nesse contexto, nota-se uma propensão de estender-se a hipervulnerabilidade para abranger os usuários de ambientes digitais como um todo, em razão do déficit informacional.

Dessa forma, o objetivo da pesquisa é analisar se há hipervulnerabilidade dos usuários por limitações à autodeterminação informativa, e como equalizar a relação consumidor-fornecedor em ambientes digitais como o metaverso, reduzindo a assimetria existente.

Por meio de pesquisa teórica-bibliográfica e dedutiva, determinam-se os hipervulneráveis em ambientes digitais e as possibilidades de potencialização da exploração de dados com o uso do metaverso, combinado com mecanismos proativos de redução da assimetria informacional e, consequentemente, a promoção da autodeterminação informativa.

2 DEFINIÇÃO DE HIPERVULNERABILIDADE

A vulnerabilidade é multidisciplinar e não está restrita apenas ao âmbito jurídico. Manifesta-se em diversas áreas do conhecimento, amoldando-se às necessidades teóricas do objeto que cada uma delas pretende compreender ou explicar[1].

Sua origem é devida do termo *vulnus (eris*) correspondente à ferida e, em geral, é utilizada em menção à suscetibilidade de ser ferido (NEVES, 2006, p. 158), lesionado, sofrer dano ou prejuízo, tanto com repercussões físicas ou materiais (p. ex. integridade física ou patrimônio) quanto imaterial (p. ex. direitos da personalidade).

Representa, dessa forma, o estado de fragilidade a que uma pessoa está exposta em determinado contexto desfavorecendo-a nas relações jurídicas, e colocando-a em desigualdade em relação a outra parte ou outro grupo (CABRAL, 2022, p. 179).

Em sentido jurídico, é notada em todo o Ordenamento Jurídico com a finalidade de tutelar os indivíduos que estejam em desigualdade material, ou inferioridade em relação aos demais. Direcionando-se à tutela das pessoas que estão em situação ou condição que as deixem mais suscetíveis a lesões ou violação aos seus interesses, independentemente de resultar em danos ou não.

Ou seja, é um estado da pessoa inerente de risco ou um sinal de confrontação excessiva

[1] Ilustrativamente, no âmbito da assistência social a vulnerabilidade pode ser associada "à precariedade no acesso à garantia de direitos e proteção social, caracterizando a ocorrência de incertezas e inseguranças e o frágil ou nulo acesso a serviços e recursos para a manutenção da vida com qualidade" (CARMO; GUIZARDI, 2018, p. 7).

de interesses, identificado no mercado, que fragiliza e enfraquece o sujeito de direitos, desequilibrando a relação. No entanto, a vulnerabilidade não é o fundamento da tutela a quem está em situação de fragilidade, mas tão somente a explicação para as normas, em uma "noção instrumental que guia e ilumina a aplicação destas normas protetivas e reequilibradoras, à procura do fundamento da Igualdade e da Justiça equitativa" (MARQUES; MIRAGEM, 2014, n.p.).

Em razão das diversas condições de fragilidade, várias legislações têm o objetivo de tutelar os vulneráveis, tais como, o Estatuto da Criança e do Adolescente, Estatuto da Pessoa Idosa, Estatuto da Pessoa com Deficiência, o Código de Defesa do Consumidor.

A Consolidação das Leis do Trabalho, por exemplo, tem por objetivo regular a relação jurídica entre o empregador e o empregado, que é considerado vulnerável em razão da própria exigência de subordinação para formação do vínculo de emprego (BIONI, 2021, p. 158).

A Constituição Federal estabeleceu a dignidade da pessoa humana como fundamento da República (artigo 1º, inciso III), consagrando-a como fim e objetivo de todas as áreas do Direito.

Houve a alteração dos paradigmas dos negócios jurídicos, e "os princípios da autonomia privada e da força obrigatória dos contratos tiveram sua abrangência reduzida pela boa-fé, pela função social do contrato e pela equidade entre as partes" (AMARAL; HATOUM; HORITA, 2017, p. 271). Contemporaneamente, os negócios jurídicos têm como finalidade ser "um instrumento a serviço da pessoa, sua dignidade e desenvolvimento" devendo ser integrado pela solidariedade, erradicação da pobreza e a proteção ao consumidor (NEGREIROS, 2006, p. 106-108).

Nesse contexto, em razão do avanço da tecnologia e a ampliação das contratações em massa, tornou-se evidente a inexistência da suposta igualdade de condições para negociação entre os contratantes (consumidores e fornecedores). Isso porque é o fornecedor que tem o domínio da técnica, e pode utilizar-se de diversas formas de marketing e publicidade para direcionar o consumidor ao consumo (MENDES, 2015, n.p).

Em razão disso, para cumprir o comando constitucional de defesa do consumidor (artigo 5º, inciso XXXII da Constituição Federal), foi elaborado o Código de Defesa do Consumidor (Lei n.º 8.078/1990) que definiu direitos aos consumidores e deveres aos fornecedores e ao Poder Público. Optou-se por considerar que todos os consumidores são vulneráveis como um dos princípios da Política Nacional das Relações de Consumo (artigo 4º, inciso I).

Em razão disso, identificam-se diversas formas de vulnerabilidade dos consumidores, que podem ser agrupadas em técnica, jurídica, fática e informacional.

A vulnerabilidade técnica corresponde à ausência de conhecimentos pelo consumidor

sobre o produto ou serviço, deixando-o mais suscetível a equívocos sobre suas características ou utilidade. A vulnerabilidade jurídica, também denominada de científica, refere-se à ausência de conhecimentos nas áreas jurídicas, contábeis ou econômicas, informações que podem influenciar a relação contratual e a própria fruição do bem pelo consumidor. É dever do fornecedor buscar as informações necessárias para garantir a segurança da contratação. A fática, também designada de socioeconômica, decorre da posição privilegiada do fornecedor em relação ao consumidor, identificada tanto por seu poder econômico quanto pela essencialidade do produto ou serviço. Por sua vez, a vulnerabilidade informacional, que pode ser compreendida como integrante da vulnerabilidade técnica, se refere à assimetria de informações, em um mundo em que a informação é poder. Logo, cabe ao fornecedor atuar de forma a compensar o déficit de informações, já a ausência dessa pode ser considerada um risco para os consumidores (MARQUES; MIRAGEM, 2014, n.p).

A vulnerabilidade informacional ocorre, por exemplo, quando o consumidor não dispõe "[...] de uma informação alimentar, de que um determinado produto contém elementos geneticamente modificados, ou de que um determinado produto legal de tabaco causa vício e danos a 50% de seus consumidores, qualquer a quantidade utilizada" (MARQUES; MIRAGEM, 2014, n.p).

Assim, nota-se que, para a configuração da vulnerabilidade prevista no Código de Defesa do Consumidor, basta tão somente que o indivíduo esteja em uma relação de consumo, sem que seja necessária nenhuma verificação *in concreto*. Tutela-se a inferioridade contratual do consumidor frente ao fornecedor (KONDER; KONDER, 2021, p. 57).

A disposição legal de vulnerabilidade indistinta para os consumidores, afastou-se de sua concepção original, de tutela dos indivíduos com características pessoais que os deixam suscetíveis a lesões ou a violações de seus interesses, e que era analisada casuisticamente (KONDER; KONDER, 2021, p. 56). Deixando, de certa forma, aqueles que estão em vulnerabilidade por condições pessoais em uma, aparente, situação de desamparo pela legislação consumerista.

Em razão disso, com a finalidade de designar aquelas situações em que o indivíduo está em uma condição de maior vulnerabilidade se comparado com os demais consumidores, ou com o consumidor "padrão" (KONDER; KONDER, 2021, p. 58), surgiu o conceito de hipervulnerabilidade. Fala-se, inclusive, em sobreposição de vulnerabilidade (BIONI, 2021, p. 162), vulnerabilidade agravada (MARQUES; MIRAGEM, 2014, n.p) ou supervulnerabilidade (GRUNDMANN, 2016, p. 345).

O termo hipervulnerabilidade ganhou notoriedade jurisprudencial ao ser utilizado pelo

Ministro Antônio Herman Benjamin, no Recurso Especial nº 586.316/MG[2], para referir-se à necessidade de tutela daqueles que estão em maior vulnerabilidade em relação aos demais consumidores, citando como exemplo crianças, idosos, pessoas com deficiências, analfabetos, e aqueles sujeitos a manifestar ou agravar doenças em razão do consumo de produtos ou serviços, ainda que esses não representem risco à generalidade dos consumidores (BRASIL, 2007).

A hipervulnerabilidade é, portanto, intrinsicamente vinculada à ideia de vulnerabilidade, e vai além da ordinária, normal ou típica, e enseja a proteção do mais fraco (MARQUES; MIRAGEM, 2014, n.p.). É caso das crianças e adolescentes, que por estarem em desenvolvimento, são mais suscetíveis à publicidade (TEIXEIRA; SABO, 2016, n.p.). Os idosos são mais propensos a contratar empréstimos ou ter problemas com planos de saúde.

Diferenciam-se porque a condição hipervulnerável não é permanente e automática, tão somente pela existência de um consumidor na relação jurídica, mas deve ser analisada casuisticamente, podendo ser "permanente ou temporária, a considerar condições individuais ou coletivas, com potencialidade de gerar a hipervulnerabilidade" (PASQUALOTTO; SOARES, 2017, n.p.). Embora as consequências de ambas no mundo fático sejam semelhantes, na hipervulnerabilidade é mais acentuada (PASQUALOTTO; SOARES, 2017, n.p.) ensejando maior ocorrência de lesões e violações aos interesses dos consumidores.

Em razão disso, exige-se na hipervulnerabilidade um comportamento mais atento do fornecedor, com maior cuidado por saber que, dentre os inúmeros consumidores para quem ofereceu o produto ou serviço para contratação, podem existir contratantes nessa posição. Isso significa que haverá uma análise mais rigorosa da conduta do fornecedor (PASQUALOTTO; SOARES, 2017, n.p.).

Embora, em um primeiro olhar, pareça necessária a elaboração de novas legislações com a finalidade de tutelar os hipervulneráveis, nota-se que a mera edição de leis não garante a efetividade de direitos. Há ainda, a fluidez das relações comerciais e a diversidade de circunstâncias que podem levar o consumidor à posição de hipervulnerável, sendo, portanto, impossível que a legislação tutele todas as hipóteses.

Existem no Código de Defesa do Consumidor normas que indicam a necessidade de

[2] No caso, discutia-se a obrigatoriedade de inclusão nos rótulos de alimentos da informação "Contém glúten: a existência do glúten é prejudicial à saúde dos doentes celíacos". Dentre os pontos debatidos, analisou-se o artigo 31 do Código de Defesa do Consumidor aplica-se aos inconvenientes que afetariam apenas o grupo determinados de pessoas com doença celíaca, ou limita-se tão somente aos riscos a que os consumidores em geral estejam expostos. Concluiu-se que a igualdade material exige além de oportunidades iguais, a garantia de possibilidades das minorias (hipervulneráveis) "se prevenirem contra os riscos à sua saúde e segurança, decorrentes de produtos e serviços colocados no mercado" (BRASIL, 2007).

maior tutela dos que estão em elevada vulnerabilidade (SANTOS; VASCONCELOS, 2018, n.p.). Por exemplo, a vedação dentre as práticas abusivas, de o fornecedor "prevalecer-se da fraqueza ou ignorância do consumiAW323dor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços" (artigo 39, inciso IV).

Embora a tutela dos hipervulneráveis não se distancie da proteção aos vulneráveis, o ideal é que o fornecedor adote uma postura de "endurecimento das regras de fornecimento e um maior rigor na aplicação do próprio CDC, (LGL\1990\40), que assim serviriam à proteção de todo e qualquer consumidor, independentemente da configuração da hipervulnerabilidade" (SANTOS; VASCONCELOS, 2018, n.p.). Dessa forma, a exigência de cautela do fornecedor terá benefícios práticos para todos os consumidores.

Em decorrência da vinculação da hipervulnerabilidade à conduta de cuidado pelo fornecedor questiona-se, ainda, se haveria uma intervenção na autodeterminação do consumidor e se poderia ser ilimitada (PASQUALOTTO; SOARES, 2017, n.p.). No entanto, não se trata de restringir a autodeterminação do contratante hipervulnerável, mas tão somente permitir a "ponderação entre diferentes interesses em jogo, inclusive, quanto à admissão de um critério de preponderância que pode considerar distintas premissas, inclusive a do menor sacrifício por conta de um maior benefício" (PASQUALOTTO; SOARES, 2017, n.p.). Isso é, deve-se ponderar a motivação e as consequências da contratação para verificar se a escolha é justificada.

Dessa forma, somente haveria limitação ou interferência na autodeterminação do consumidor quando indispensável para o reequilibro contratual e com preponderância à vontade do consumidor, quando considerada a finalidade da contratação em comparação com a do produto ou serviço (PASQUALOTTO; SOARES, 2017, n.p.).

Em razão da amplitude do debate sobre a hipervulnerabilidade, Carlos Konder e Cintia Konder (2021, p. 64-65) defendem que esta não é necessária para o Direito Brasileiro e propõem a suficiência tão somente da diferenciação da vulnerabilidade em patrimonial e existencial. A primeira seria aquela prevista no Código de Defesa do Consumidor, com a finalidade de reduzir o desequilíbrio contratual. A segunda, decorre da situação pessoal da pessoa, vinculando-se à necessidade de tutela do indivíduo com a finalidade de promoção de sua dignidade.

Portanto, não haveria necessidade de subcategorização da vulnerabilidade, que poderia resultar em novas e subsequentes reclassificações quando identificadas outras situações que demandem uma proteção diferenciada ao indivíduo. A excessiva categorização pode resultar em limitação da proteção à dignidade da pessoa humana. Logo, seria mais adequada uma diferenciação que tivesse base qualitativa (esfera existencial) e não quantitativa (soma à esfera

patrimonial) (KONDER; KONDER, 2021, p. 63-64).

Semelhantemente, Adriana de Alencar Setubal Santos e Fernando Antônio de Vasconcelos (2018, n.p.), ao abordarem o novo paradigma da vulnerabilidade, definem que além do reequilíbrio contratual entre fornecedor e consumidor próprio da vulnerabilidade, a hipervulnerabilidade é um "adjetivar o estado de fragilidade de grupos de consumidores" que são identificados em razão da "conjugação de características pessoais" (SANTOS; VASCONCELOS, 2018, n.p.).

Em razão disso, propõem a subdivisão da vulnerabilidade em *lato* e *stricto sensu.* Na vulnerabilidade *lato sensu*, estariam contempladas as situações de mero desequilíbrio contratual, e na *stricto sensu*, seriam identificados grupos de consumidores em vulnerabilidade exacerbada decorrentes de particularidades pessoais (SANTOS; VASCONCELOS, 2018, n.p.).

No cenário de discussão da necessidade de desdobramento da vulnerabilidade em hipervulnerabilidade, torna-se necessário verificar a pertinência dessa categoria para tutelar de forma mais adequada os usuários de ambientes digitais.

3 METAVERSO: HIPERVULNERABILIDADE EM AMBIENTES DIGITAIS

Quando se fala em usuários de ambientes digitais, pode-se identificar ao menos quatro formas de relações: usuário – plataforma; usuário – usuário; usuário – fornecedor (que utiliza a plataforma no fomento de sua atividade empresarial); a qual implica diretamente na existência da relação empresarial fornecedor – plataforma.

Tal situação impede, em certa medida, a equiparação indistinta do usuário de ambientes digitais ao consumidor. No entanto, por pertinência temática, o enfoque da exposição é a proteção de dados pessoais. Logo, refere-se às relações usuário – plataforma e usuário – fornecedor.[3]

Esse recorte temático, permite a transposição de todo o arcabouço jurídico de tutela dos consumidores aos usuários de ambientes digitais, e, portanto, de um pressuposto de vulnerabilidade dos usuários indistintamente considerados.

Isso se dá porque, apesar de não ser evidente para a maioria das pessoas, a utilização de plataformas digitais é uma relação de consumo. Caracterizada, porque o usuário está adquirindo ou utilizando um produto ou serviço como destinatário final (artigo 2º do Código de Defesa do

[3] A relação entre usuário-usuário, *prima facie*, é paritária e regida pelo Código Civil e demais legislações pertinentes. Já a relação entre fornecedor-plataforma, em razão de sua característica empresarial será regida por normas de Direito Empresarial e correlatas.

Consumidor) e há um fornecedor, pessoa física ou jurídica, que oferece produtos ou serviços (sites, redes sociais, plataformas, aplicativos, etc) (artigo 3º do Código de Defesa do Consumidor) em ambientes digitais. Exige-se expressamente a remuneração para o serviço.

Embora os usuários não percebam (MENDES, 2015, n.p.), o produto ou serviço digital é remunerado, tanto de forma direta como indireta. Pode-se remunerar pagando determinado valor pecuniário ao fornecedor, ou indiretamente, por qualquer outra forma que, no caso dos ambientes virtuais, é o fornecimento de dados pessoais.

Em outras palavras, ainda que aparentemente o serviço seja gratuito, ele é remunerado por dados pessoais dos usuários (LEMOS; BRANCO, 2021, p. 456).

Existe tal possibilidade porque os dados pessoais na atualidade têm elevado valor, já que uma vez tratados, possibilitam uma infinidade de utilidades às atividades econômicas dos fornecedores. Fala-se assim que os dados são o novo petróleo (FRAZÃO, 2020a, n.p.), e por suas características, são infindáveis, já que a todo momento, novas informações são coletadas e constantemente novos usuários entram nos ambientes digitais.

Ou seja, o consumidor remunera por meio de seus dados pessoais que, após o tratamento pelo fornecedor, poderão oferecer tanto benefícios quanto riscos:

> [...] os algoritmos estão hoje sendo programados para a extração de padrões e inferências a partir dos quais serão tomadas, de forma automatizada, decisões sobre questões objetivas, mas que estão atreladas a importantes dados sensíveis, assim como decisões sobre questões subjetivas e que envolvem complexos juízos de valor, tais como (i) avaliar as características, a personalidade, as inclinações e as propensões de uma pessoa, inclusive no que diz respeito à sua orientação sexual; (ii) analisar o estado de ânimo ou de atenção de uma pessoa; (iii) identificar estados emocionais, pensamentos, intenções e mesmo mentiras; (iv) detectar a capacidade e a habilidade para determinados empregos ou funções; (v) analisar a propensão à criminalidade; (vi) antever sinais de doenças, inclusive depressão, episódios de mania e outros distúrbios, mesmo antes da manifestação de qualquer sintoma (FRAZÃO, 2020a, n.p.).

Merece destaque a advertência de Bruno Bioni (2021, p. 159) de que em razão do "contexto de agregação de dados e de complexidade do fluxo informacional [...], o consumidor não sabe, ao certo, os custos efetivos de tal transação econômica, já que é incerto o alcance do fluxo de seus dados pessoais e, por conseguinte, o que deles se pode extrair".

Partindo-se da premissa de que há uma infinidade de possibilidade de tratamento dos dados pessoais na sociedade da informação (MENDES, 2015, n.p.) e que há um risco ao titular de dados inerente ao tratamento, é oportuno dizer que a utilização do metaverso trará novas possibilidades de exploração de dados pessoais.

O metaverso constitui-se em um ambiente virtual que promete diversas inovações. Apesar de não ser uma novidade, ganhou notoriedade quando Mark Zuckerberg alterou o nome do grupo de empresas do Facebook para Meta, ainda que não seja a única empresa que está

desenvolvendo um metaverso.

Apesar do metaverso estar em construção é possível identificar algumas características que serão comuns a todos os desenvolvedores: persistência, ou seja, continua indefinidamente; síncrono e ao vivo, isso é acontece para todos os usuários ao mesmo tempo; ausência de limitação em relação aos usuários simultâneos, assim todos que quiserem poderão participar da mesma coisa ao mesmo tempo; economia em pleno desenvolvimento, que se refere à capacidade de criação de relações mercadológicas pelos usuários e empresas; experiência entre mundos digital e físico; oferecimento de interoperabilidade sem precedentes de dados e outros itens entre fornecedores e, até mesmo, entre metaversos; preenchimento por "conteúdo" e "experiências" criados e operados por uma ampla gama de colaboradores, vinculados ou não a algum fornecedor ou desenvolvedor (BALL, 2020, n.p.).

Nota-se que muito se fala sobre o metaverso, mas pouco se sabe sobre ele. Há autores, inclusive, que advertem quanto à falácia da incrível inovação do conceito, demonstrando que a "inovação", em verdade, já era utilizada em outros aplicativos, como a interação social com outros usuários que está presente nos jogos multijogadores há muitos anos. Dessa forma, não há uma necessidade inafastável de utilizar-se de aparelhos de realidade aumentada ou de realidade virtual no metaverso (MAGRO; SOUZA, 2022, p. 30-31).

Porém é justamente a utilização das tecnologias vestíveis (uso dos óculos de realidade virtual ou aumentada, por exemplo) que permitirá a fusão entre o mundo real e digital, e a transferência de mais atividades do mundo físico para o virtual, se comparado com a atualidade.

Isso significa que o foco dos desenvolvedores e investidores em metaverso é cativar as pessoas para que fiquem mais tempo online e usem mais tecnologias vestíveis, permitindo a maior coleta de dados pessoais dos usuários.

Nesse sentido, Marcela Ejnisman, Maria Lacerda e Miguel Carneiro (2022, p. 70) explicam que no metaverso haverá um aumento da coleta de dados "observados".

A divisão dos dados em fornecidos, observados e inferidos, é utilizada com frequência na análise da portabilidade de dados pessoais.

Os dados fornecidos, são coletados de forma ativa pelo fornecedor, ou seja, há requerimento de inclusão das informações e o usuário o incluiu ciente de que estava fornecendo dados pessoais. Já os dados observados correspondem àqueles que podem ser coletados de forma passiva pelo fornecedor, em razão do acompanhamento da "fruição ou interação do usuário com a plataforma digital, como *cookies*, histórico de navegação e de busca, dados de tráfego, geolocalização do usuário, número de *likes* etc". Os dados inferidos ou derivados são aqueles gerados pela estruturação e combinação dos fornecidos e observados pelo fornecedor

(NEGRI; KORKMAZ; FERNANDES, 2021, p. 9).

Ou seja, a utilização das tecnologias vestíveis, combinada com o aumento das atividades desenvolvidas virtualmente e do tempo que o usuário está online, aumentará a possibilidade de coleta dos dados observáveis.

A título de exemplo do aumento da capacidade de coleta de dados, verifica-se que com a utilização dos óculos, não apenas as informações sobre o que o usuário acessa, pesquisa e clica poderão passar a compor os bancos de dados, mas também, todas as informações que estejam no campo de "visão" das tecnologias vestíveis, sejam objetos, marcas utilizadas e até informações biométricas do próprio usuário:

> [...] com uso de óculos de realidade virtual, os desenvolvedores do metaverso conseguirão monitorar respostas fisiológicas e dados biométricos dos indivíduos tais como expressões faciais, inflexões vocais e sinais vitais em tempo real, tudo isso enquanto os participantes estão "vivendo" neste meio digital (EJNISMAN; LACERDA; CARNEIRO, 2022, p. 70).

A coleta dos dados observados, e combinados com outros para gerar os dados inferidos, farão com que essas informações passem a integrar a projeção pessoal do usuário ou sua representação no meio virtual, com reflexos diretos, seja para criação de oportunidades ou discriminação do usuário (MENDES, 2015, n.p.), o que gera diretamente implicações em relação à autodeterminação informativa.

Isso, na medida em que se parte da conceituação de autodeterminação informativa como o direito ou o poder do indivíduo sobre seus dados pessoais em todo o fluxo de dados, desde a coleta, tratamento, transferência e eliminação.

É o direito do usuário determinar quais informações a seu respeito estarão disponíveis para conhecimento de terceiros e poderão ser utilizadas pra influenciar sua vida (MENDES, 2015, n.p.). Bem como perpassa por um "consentimento informado (entendido de forma restrita) como maneira de antecipação de riscos de violação à privacidade e busca por um caráter preventivo" (BONNA; CAÑIZO; CALZAVARA, 2021, p.7).

A origem da autodeterminação informativa está na decisão sobre o Censo Alemão em 1983, em que se concluiu pela necessidade de que o tratamento dos dados pessoais se desse de forma transparente, com a finalidade de tutelar a dignidade da pessoa humana e o livre desenvolvimento da personalidade (MARIA; PICOLO, 2021, n.p). Justamente considerando que os dados pessoais constituem à representação da pessoa.

Em decorrência principalmente do avanço tecnológico, tornou-se necessária a edição de legislações com a finalidade de tutelar os dados pessoais dos usuários, concedendo ao titular o controle sobre seus dados pessoais e limitando-se à atuação dos fornecedores.

No Brasil, a regulamentação do tratamento dos dados pessoais se deu por meio da Lei Geral de Proteção de Dados Pessoais - LGPD (Lei n.º 13.709/2018) que possui certas semelhanças com o Código de Defesa do Consumidor. Mas que, ao invés do paternalismo verificado na legislação consumerista, confere a base legal do tratamento de dados pessoais ao consentimento, ou seja, salvo as exceções expressas, deixa a cargo do próprio titular de dados, decidir pelo tratamento ou não de seus dados pessoais.

A opção legislativa, no entanto, é criticada (VERBICARO; CALANDRINI, 2022, n.p.) em razão da vulnerabilidade do usuário que acaba por não cumprir sua finalidade:

> Muito embora se dedique um diploma próprio para tratar dessa situação específica de vulnerabilidade, apostam-se todas as fichas normativas como se a parte mais fraca desse arranjo regulatório fosse um sujeito racional, livre e capaz para fazer valer a proteção de seus dados pessoais (BIONI, 2021, p. 136).

A exigência do consentimento para o tratamento dos dados pessoais, embora, na prática, proporcione uma autodeterminação informativa formal, não a atinge materialmente, já que em sua maioria a arquitetura dos ambientes digitais não possibilitam o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (artigo 5º, inciso XII da LGPD).

Em outros termos, em razão da própria disposição da plataforma ou por falta de informação adequada, os usuários manifestam o consentimento, tão somente para ter acesso ao produto ou serviço oferecido de forma imediata (MENDES; FONSECA, 2021, p. 95).

Assim, verifica-se a existência de obstáculos ao consentimento como paradigma para proteção dos dados pessoais, já que existem:

> [...] limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; [...] as situações em que não há uma real liberdade de escolha do titular, por exemplo, em circunstâncias denominadas "take it or leave it"; [...] as modernas técnicas de tratamento e análise de dados a partir de Big Data que fazem com que a totalidade do valor e a possibilidade de uso desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido (MENDES; FONSECA, 2021, p. 95).

Isso porque, em algumas situações, a opção que se dá ao consumidor é a de consentir com o que o fornecedor propõe em termos de privacidade, coleta e tratamento de dados, ou sair da plataforma. Implicando em restrição ao uso do produto ou serviço digital, que em muitos casos é de utilização compulsória, como e-mail e reuniões virtuais, para atividades profissionais ou educacionais.

Nesse contexto, acaba o consumidor aceitando os termos do fornecedor como mero requisito para usufruir do produto ou serviço, sem pensar nas consequências referentes ao

consentimento para o tratamento de seus dados pessoais. O ser humano, naturalmente, é tendente a priorizar os benefícios, prazeres ou sensações imediatas em detrimento de evitar prejuízos futuros decorrentes da ignorância da repercussão (extensão da utilização e danos gerados) do consentimento para o tratamento dos dados (MENDES; FONSECA, 2021, p. 96).

Portanto, nota-se que é evidente a posição de inferioridade do usuário de ambientes digitais em relação ao fornecedor ou à plataforma, ainda mais acentuada quando da utilização de plataformas como o metaverso.

Retomando as construções doutrinárias expostas no primeiro capítulo, verificam-se duas possibilidades para a caracterização da hipervulnerabilidade dos usuários de ambientes digitais enquanto consumidores, uma de caráter subjetivo e outra de caráter objetivo.

Ambas teriam como marco básico, a inferioridade do consumidor em relação ao fornecedor e à plataforma, por não possuir conhecimento informático básico e estar em assimetria informacional, impossibilitando a efetiva autodeterminação em relação à coleta e tratamento de seus dados. A plataforma ou fornecedor está em posição de vantagem, porque a arquitetura dos ambientes digitais favorece a coleta de dados pessoais e dificulta a compreensão pelo usuário sobre o que efetivamente está permitindo que realizem com seus dados.

Se diferenciam pela suficiência ou não da vulnerabilidade prevista no Código de Defesa do Consumidor combinada com as disposições da LGPD para tutela dos usuários.

Se pensada a hipervulnerabilidade, sob um enfoque subjetivo, ou seja, de maior exposição do usuário ao risco de sofrer uma lesão ou ter seus interesses violados, decorrente de uma condição pessoal, como a idade ou estado de saúde, notar-se-á a adequação tão somente da vulnerabilidade prevista no Código de Defesa do Consumidor para tutelar os usuários consumidores de forma indistinta. E a necessidade da hipervulnerabilidade constatada no caso concreto, para tutelar os usuários em condições pessoais que aumentam sua vulnerabilidade, exigindo, portanto, uma conduta mais diligente do fornecedor quando houver a possibilidade do usuário ser hipervulnerável, e que teria repercussões positivas para todos os usuários.

Essa possibilidade é identificada na disposição legal que diferencia o tratamento de dados pessoais de Crianças e de Adolescentes no artigo 14 da LGPD, exigindo o consentimento específico e em destaque de ao menos um dos pais ou responsável; que os controladores mantenham pública a informação sobre os tipos de dados coletados, a forma de sua utilização, e os procedimentos para o exercício dos direitos previstos na Lei; proíbe-se o condicionamento da participação de crianças e de adolescentes em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade; exige-se que o controlador realize todos os esforços razoáveis para verificar que o

consentimento foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis. Em especial, exige-se que as informações sobre o tratamento de dados sejam fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Ou seja, nota-se que o consentimento para tratar dados pessoais de crianças e de adolescentes é diferenciado, justamente porque estão em situação de maior risco em relação ao tratamento de seus dados pessoais.

Em relação ao idoso, também há disposição especial no artigo 55-J, XIX da LGPD ao estabelecer a competência da Autoridade Nacional de Proteção de Dados para "garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003" (Estatuto da Pessoa Idosa).

Por outro lado, a hipervulnerabilidade, sob um enfoque objetivo, se vincula à ideia de que, por estarem no ambiente virtual, inseridos no mercado informacional, todos os usuários estariam mais expostos ao risco de serem lesionados se comparados com os consumidores fora do ambiente virtual, em decorrência da despersonalização, desmaterialização, desterritorialização e atemporalidade, inerentes à contratação eletrônica e que independem da verificação de alguma condição pessoal para tanto, e exigiriam a sobreposição de regimes legais (BIONI, 2021, p. 161-162).

Ou seja, os usuários de ambiente virtuais estrariam em uma condição de suscetibilidade à lesão tão somente por estarem no ambiente virtual, em decorrência do déficit informacional a que estão submetidos. A hipervulnerabilidade se caracterizaria pelo simples fato de ser um usuário do ambiente virtual, logo de forma objetiva.

4 MECANISMOS PROATIVOS PARA PROTEÇÃO DE DADOS PESSOAIS E O DEVER DE INFORMAÇÃO

Demonstrado que independentemente da nomenclatura utilizada (vulnerável ou hipervunerável) todos os usuários de ambientes virtuais, enquanto consumidores, estão em uma situação de assimetria com o fornecedor, e a insuficiência do consentimento como base legal que possibilite a autodeterminação informativa, torna-se necessário verificar formas de atribuir ao fornecedor, e também ao Poder Público, parte da responsabilidade pela efetivação da

autodeterminação informativa, o que pode ser feito por meio da proação tanto do fornecedor quanto do Estado, resultando em informações necessárias ao usuário.

Não é suficiente apenas oferecer à informação ao consumidor, porque informações em excesso, acabam por prejudicar a compreensão do usuário (MARQUES; MIRAGEM, 2014, n.p). É o caso, por exemplo, dos termos de uso ou de privacidade que são inviáveis de serem lidos (BIONI, 2021, p. 168), seja por sua extensão, termos técnicos utilizados, e até mesmo o tamanho da letra em que é apresentado.

Nesse sentido, partindo-se da consideração de que a informação é direito do consumidor, correspondendo ao dever do fornecedor de prestar informação adequada e um dos princípios da Política Nacional das Relações de Consumo, é necessário que o fornecedor e o Poder Público invistam tanto na arquitetura dos ambientes digitais quanto em Políticas Públicas de favorecimento e suporte ao usuário para exercer sua autodeterminação informativa (BIONI, 2021, p. 164).

Assim, o fornecedor pensando na vulnerabilidade (ou hipervulnerabilidade) dos usuários, deve adotar uma conduta de cuidado, ou seja, projetar a arquitetura dos ambientes digitais efetivamente observando, por exemplo, as concepções de *privacy by design* e *privacy by defaut* (FRAZÃO, 2020b, n.p.).

O *privacy by design* é previsto no artigo 46, §2º da LGPD e no artigo 25 do GDPR (General Data Protection Regulation), e corresponde à proteção de dados pessoais "orientar a concepção de um produto ou serviço, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais" (BIONI, 2021, p. 171). Ou seja, o desenvolvedor deve pensar na privacidade do usuário a cada passo, durante todo o ciclo de tratamento de dados (FRAZÃO, 2020b, n.p.), permitindo o controle sobre os dados pessoais, seja consentindo, revogando o consentimento e, até mesmo, por meio do esclarecimento adequado de como se dá o tratamento dos dados.

Já o *privacy by defaut*, embora não tenha previsão legal na LGPD ou no GDPR, corresponde ao dever do fornecedor ou do desenvolvedor de ter a privacidade dos usuários como regra ao lançar o produto ou serviço (FRAZÃO, 2020b, n.p.). Isso significa que deve "vir de fábrica" com as opções de permissão mínima à coleta de dados. O que corresponde, inclusive, ao dever de coleta mínima necessária dos dados pessoais, decorrente do princípio da necessidade (artigo 6, inciso III da LGPD):

> [...] a configuração de privacidade mais restritiva possível é estabelecida desde o momento zero. Apenas os dados essenciais para prestar o serviço ou entregar o produto devem ser coletados. Ainda assim, o usuário deverá ser informado de quais informações estão sendo coletadas e para qual propósito. Caberá ao usuário, caso

> deseje, desativar uma ou todas essas salvaguardas. A empresa não deve fornecer o produto ou serviço com essas proteções desativadas, dependendo de uma ação do usuário para serem ativadas (OLIVEIRA, 2019, n.p.).

Nesse sentido, iniciativas como a de *privacy by defaut* possibilitarão também que o consentimento seja granular (BIONI, 2021, p. 177). O usuário não consente automaticamente com o tratamento de todos os dados pessoais e com todas as permissões requeridas pelo aplicativo para sua usabilidade plena. Mas a cada nova funcionalidade, se necessário, o usuário dará o seu consentimento para "desbloqueá-la".

Permitindo, assim, a fragmentação das opções de coleta de dados pessoais e garantindo que o consentimento seja livre e personalizado (BONNA; CAÑIZO; CALZAVARA, 2021, p. 14). Ou seja, a arquitetura dos ambientes digitais deve ser pensada de forma a, efetivamente, exigir uma conduta ativa do usuário, consentindo com a coleta dos dados necessários, facilitando a configuração prévia de coleta tão somente dos dados mínimos.

Para tanto, as Tecnologias de Facilitação da Privacidade (*Privacy Enhancing Technologies*/PETs) são "como tecnologias que reforçam-melhoram a privacidade – denota abrangência do termo que, como um guarda-chuva, é capaz de abarcar toda e qualquer tecnologia que seja amigável e facilitadora à privacidade" (BIONI, 2021, p. 171).

Exemplo prático é o "*Not Track/DNT*", que equivale ao "Não me Rastreie", funcionalidade ativada no navegador indicando a opção prévia dos usuários pela não coleta de dados, e que facilita o controle dos dados, servindo como meio de exteriorização da autodeterminação informativa. Bem como a *Platform for Privacy Preferences/P3P*, permitindo ao usuário definir por meio de seu navegador suas preferências de privacidade, quais dados concorda que sejam coletados e se aceita o compartilhamento com terceiros. A partir disso, o próprio navegador faria uma análise automatizada das políticas de privacidade das aplicações acessadas, verificando-se a sua (in)compatibilidade com as preferências de privacidade pré-configuradas (BIONI, 2021, p. 172-178).

No entanto, ambos os exemplos têm dificuldades de serem executados em razão da necessidade de padronização das políticas de privacidade e sua disponibilização de forma legível por meio de inteligência artificial, o que se dá de certa forma em razão da ausência de ações regulatórias para tanto (BIONI, 2021, p. 177).

Porém, a arquitetura dos ambientes digitais não é suficiente, por si só, para garantir a autodeterminação informativa. Assim, considerando que o Código de Defesa do Consumidor tem por finalidade tutelar integralmente o consumidor, as suas disposições devem ser utilizadas para a proteção dos dados pessoais dos usuários e promoção da autodeterminação informativa.

E o Código de Defesa do Consumidor estabelece que a defesa do consumidor, deve-se dar também pelo Poder Público, instituindo a Política Nacional das Relações de Consumo, que além da vulnerabilidade do consumidor tem como princípio, a educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo (artigo 4º, inciso V).

A informação adequada é, portanto, um direito do consumidor, e consequentemente um dever do fornecedor. Assim, cabe tanto ao fornecedor ou desenvolvedor, quanto ao Estado atuar para garantir o exercício da autodeterminação informativa dos usuários, por meio do fornecimento de informação adequada, que possibilite ao consumidor dar seu consentimento de forma efetiva, fomentando a arquitetura mínima que favoreça a autodeterminação informativa (VERBICARO; CALANDRINI, 2022, n.p.).

Os *nudges* atendem a finalidade de capacitar o usuário para um consentimento efetivo (VERBICARO; CALANDRINI, 2022, n.p.). Ou seja, são empurrões ou cutucadas, em tradução literal, para que o consumidor tenha esclarecimentos e possa consentir de forma material, e não como mera formalidade para superar o impedimento de acesso a produtos ou serviços digitais, preservando-se o poder de escolha.

Os incentivos de conscientização dos usuários sobre o significado e as implicações do consentimento ao aceitar os termos de uso, políticas de privacidade ou *cookies* para utilização dos ambientes digitais pode se dar da maneira convencional, ou seja, campanhas educativas.

Mas também pela utilização das políticas públicas específicas ou voltadas para o fomento da inclusão na arquitetura dos ambientes digitais, de formas simplificadas de esclarecimento do usuário sobre o consentimento requisitado, utilizando-se meios ilustrativos como cores, tabelas, figuras, já que o ser humano é mais tendente a adotar as medidas mais simples, tais como escolher pelo que já vem assinalado como “recomendado” (VERBICARO; CALANDRINI, 2022, n.p.).

Dessa forma, alarga-se o alcance da autodeterminação informativa, ao simplificar as políticas de privacidade ou termos de uso, que devem estar junto ao “aceito” de forma clara e acessível, pode-se, ainda, utilizar resumos simplificados, caixas de texto destacadas, permitindo ao usuário personalizar as opções (BONNA; CAÑIZO; CALZAVARA, 2021, p. 15).

A utilização desses mecanismos de atuação prévia do fornecedor e do Poder Público resultam no empoderamento do usuário (BIONI, 2021, p. 108), o que em última análise gera também maior autodeterminação informativa e minimização da vulnerabilidade ou hipervulnerabilidade de todos os usuários.

5 CONCLUSÃO

A doutrina converge em relação à definição da vulnerabilidade quando analisada nas relações de consumo, como uma qualidade inerente ao consumidor em decorrência do desequilíbrio existente entre as posições de consumidor e fornecedor. E que a hipervulnerabilidade está relacionada à uma condição pessoal que expõe o indivíduo à maior suscetibilidade de lesão, demandando do fornecedor um dever maior de atenção e cuidado em razão da possibilidade de ter um hipervulnerável como consumidor. Controverte-se, no entanto, quanto à necessidade de sua caracterização autônoma ou se não passa de mera construção teórica sem efeitos práticos.

Os usuários de ambientes digitais são consumidores, na medida em que a remuneração dos produtos e serviços se dá por meio dos dados pessoais, que possuem grande valor na sociedade da informação.

O metaverso foi apresentado como uma tendência de acesso aos ambientes virtuais, que possibilitará a realização virtual, síncrona e ao vivo de diversas atividades cotidianas, como trabalho, estudo, lazer e integração social. Permitindo uma revolução no modo de fornecimento de produtos ou serviços, em razão de características como a ausência de limitação de usuários simultâneos e grande interoperabilidade.

Assim, considerando a disposição natural do ser humano de priorizar suas necessidades imediatas, o metaverso tem um grande potencial de cativar a atenção dos usuários. Os quais uma vez integrados à plataforma e utilizando as tecnologias disponíveis fornecerão uma quantidade ainda maior de dados pessoais.

Comparado com os ambientes digitais como redes sociais, sites de pesquisas ou compras, o uso do metaverso potencializará a coleta de dados observados, ou seja, aqueles em que o consumidor não tem uma conduta ativa e intencional de fornecimento. O que poderá ocorrer tanto pela utilização de tecnologias vestíveis quanto pelo aumento do tempo online em razão da transferência de atividades cotidianas para o digital em decorrência da fusão do mundo real e virtual possibilitada pelas tecnologias vestíveis.

Portanto, à medida que novas tecnologias ou conceitos são incorporados aos ambientes virtuais, como o metaverso e as tecnologias vestíveis, que tornam sua utilização mais interativa, há uma maior redução da autodeterminação informativa dos usuários. Dessa forma, é possível concluir que todos os usuários já estariam em situação de hipervulnerabilidade objetiva tão somente em razão da relação de consumo se dar no ambiente informático.

No entanto, não parece necessário definir a hipervulnerabilidade dos usuários de

ambientes digitais no aspecto objetivo, ainda que utilizando-se o metaverso. Isso porque, se a consideração em seu caráter objetivo se dá em decorrência do déficit informacional a que estão submetidos, nota-se que a própria noção de vulnerabilidade prevista no Código de Defesa do Consumidor já contempla a inferioridade técnica e informacional, transferindo assim ao fornecedor o dever de agir de forma a minimizar os riscos e os danos aos consumidores, e no caso do tratamento de dados, devem observar a LGPD. Restando assim, à concepção subjetiva de hipervulnerabilidade para a tutela daqueles que estejam em efetiva inferioridade em relação ao usuário "padrão".

Não havendo hipervulnerabilidade do usuário tão somente pela utilização do metaverso, mas sendo necessária a demonstração de que o usuário por uma condição pessoal estava situação de acentuada redução de sua autodeterminação informativa, se comparado com os demais usuários.

Nesse sentido, a concepção subjetiva de hipervulnerabilidade, exige do fornecedor um olhar atento à possibilidade do usuário indeterminado com quem contrata estar em maior vulnerabilidade e, portanto, resulta em um agir mais cauteloso com benefícios a todos os usuários. Esse cuidado especial, não seria exigido ao adotar-se a concepção objetiva da vulnerabilidade, já que estando todos os usuários já nivelados como hipervulneráveis, bastaria ao fornecedor observar minimamente a legislação consumerista e de proteção de dados para cumprir seus deveres legais, e isentar-se de responsabilidade por eventual violação aos direitos dos titulares de dados.

Dessa forma, o aumento da possibilidade de coleta de dados pessoais, inclusive dados observados no metaverso, torna necessário que o Poder Público incentive, e os fornecedores invistam na arquitetura do ambiente virtual, dando efetividade às concepções de *privacy by design* e *privacy by defaut.* Bem como que adotem condutas e Políticas Públicas direcionadas a conscientizar os usuários sobre as implicações do uso de seus dados pessoais, utilizando estímulos para que decidam de forma esclarecida sobre o consentimento ao tratamento como forma de compensação ou remuneração pela fruição dos produtos e serviços virtuais, promovendo-se, assim, a autodeterminação informativa dos usuários sejam vulneráveis ou hipervulneráveis.

REFERÊNCIAS

AMARAL, Ana Claudia C. Z. Mattos do; HATOUM, Nida S.; HORITA, Marcos M. O paradigma pós-moderno do negócio jurídico e a necessidade de uma nova concepção na contemporaneidade. **Scientia Iuris**, Londrina, v. 21, n. 2, p. 261-297, jul. 2017.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 jul. 2022.

BRASIL**. Lei nº. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 15 jul. 2022.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 jul. 2022.

BRASIL. Superior Tribunal de Justiça. Segunda Turma. **Recurso Especial n. 586.316/MG.** Relator Ministro Herman Benjamin. Brasília/DF. Julgado em 17/4/2007, DJe 19 mar. 2009.

BALL, Matthew. **The Metaverse**: What It Is, Where to Find it, and Who Will Build It. 2020. Disponível em: https://www.matthewball.vc/all/themetaverse. Acesso em: 20 de jul. 2022.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** a função e os limites do consentimento. 3 ed. Rio de Janeiro: Forense, 2021.

BONNA, Alexandre Pereira; CAÑIZO, Amanda de Moura; CALZAVARA, Giovana Ferreira. Consentimento e LGPD: desafios diante da hipervulnerabilidade do consumidor. **Revista De Direito E Atualidades**. v. 1 n. 3, 2021. Disponível em: https://www.portaldeperiodicos.idp.edu.br/rda/article/view/6231. Acesso em: 16 jul. 2022.

CABRAL; Hildeliza Lacerda Tinoco Boechat. Mistanásia: aspectos da morte miserável no Brasil. *In:* NOVAIS, Alinne Arquette; CABRAL, Hildeliza Lacerda Tinoco; MOREIRA, Raquel. **Tratado de Bioética Jurídica**. Portugal: Grupo Almedina, 2022.

CARMO, Michelly Eustáquia do; GUIZARDI, Francini Lube. O conceito de vulnerabilidade e seus sentidos para as políticas públicas de saúde e assistência social**. Cad. Saúde Pública, Rio de Janeiro**, v. 34, n. 3, jun. 2017. Disponível em: https://www.scielo.br/j/csp/a/ywYD8gCqRGg6RrNmsYn8WHv/?lang=pt&format=pdf. Acesso em: 30 nov. 2022.

EJNISMAN, Marcela Waksman; LACERDA, Maria Eugênia Geve de M.; CARNEIRO, Miguel Lima. Novas fronteiras da privacidade: os desafios do exercício da autodeterminação informativa. *In:* MARTINS, Patrícia Helena Marta, FONSECA, Victor Cabral (orgs.). SEREC, Fernando Eduardo (coord.). **Metaverso: Aspectos Jurídicos**. São Paulo: Almedina, 2022.

FRAZÃO, Ana. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (orgs.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2 ed. São Paulo: Thomson Reuters Brasil, 2020a.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (orgs.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 2 ed. São Paulo: Thomson Reuters Brasil, 2020b.

GRUNDMANN, Stefan. Entrevista com Stefan Grundmann. Entrevista concedida a RODRIGUES JUNIOR; Otavio Luiz; NUNES-FRITZ, Karina; RODAS, Sérgio. **Revista de Direito Civil Contemporâneo**, v. 9, n. 3. p. 337-350, 2016.

KONDER, Carlos Nelson; KONDER, Cíntia Muniz de Souza. Da vulnerabilidade à hipervulnerabilidade: exame crítico de uma trajetória de generalização. **Interesse Público -IP [Recurso Eletrônico]**, Belo Horizonte, v. 23, n. 127, p. 53-68, 2021. Disponível em: http://konder.adv.br/wp-content/uploads/2021/08/CNK-e-CMSK-Da-vulnerabilidade-a-hipervulnerabilidade-Interesse-Publico.pdf. Acesso em: 20 jun. 2022.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design: conceito, fundamentos e aplicabilidade na LGPD. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otávio Luiz (coords.). **Tratado de proteção de dados**. Rio de Janeiro: Forense, 2021.

MAGRO, Américo Ribeiro; SOUZA, Landolfo Andrade de. **Manual de Direito Digital**. 2 ed. São Paulo: Juspodivm, 2022.

MARIA, Isabela; PICOLO, Cynthia. Autodeterminação informativa: como esse direito surgiu e como ele me afeta? **Laboratório de Pesquisa Direito Privado e Internet - LAPIN**, 27 abr. 2021. Disponível em: https://lapin.org.br/2021/04/27/autodeterminacao-informativa-como-esse-direito-surgiu-e-como-ele-me-afeta/. Acesso em: 12 ago. 2022.

MARQUES, Claudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis**. 2 ed. São Paulo: Revista dos Tribunais, 2014.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de direito do consumidor**. São Paulo, Revista dos Tribunais, v. 24, n. 102, p. 19–43, 2015. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/revista-dos-tribunais-online.html. Acesso em: 09 jun. 2022.

MENDES; Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otávio Luiz (coords.). **Tratado de proteção de dados**. Rio de Janeiro: Forense, 2021.

NEGREIROS, Teresa. **Teoria dos contratos**. Novos paradigmas. 2 ed. Rio de Janeiro: Renovar, 2006.

NEGRI, Sergio Marcos Carvalho de Ávila; KORKMAZ, Maria Regina Detoni Cavalcanti Rigolon; FERNANDES, Elora Raad. Portabilidade e proteção de dados pessoais: tensões entre pessoa e mercado. **Civilistica.com.** Rio de Janeiro, v. 10, n. 1, 2021. Disponível em: http://civilistica.com/portabilidade-e-protecao-de-dados-pessoais/. Acesso em: 15 jul. 2022.

NEVES, Maria do Céu Patrão. Sentidos da vulnerabilidade: característica, condição,

princípio. **Revista Brasileira De Bioética**, v. 2 n. 2, p. 157–172, 2006. Disponível em: https://periodicos.unb.br/index.php/rbb/article/view/7966. Acesso em: 30 nov. 2022.

OLIVEIRA, Samanta. LGPD: as diferenças entre o privacy by design e o privacy by default. **Consumidor Moderno!.** 2019. Disponível em: https://www.consumidormoderno.com.br/2019/05/27/lgpd-diferencas-privacy-design-privacy-default/. Acesso em: 16 jul. 2022.

PASQUALOTTO, Adalberto; SOARES, Flaviana Rampazzo. Consumidor hipervulnerável: análise crítica, substrato axiológico, contornos e abrangência. **Revista de Direito do Consumidor**, v. 113, p. 81 – 109, 2017. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/revista-dos-tribunais-online.html. Acesso em: 08 ago. 2022.

SANTOS, Adrianna de Alencar Setubal; VASCONCELOS, Fernando Antônio de. Novo paradigma da vulnerabilidade: uma releitura a partir da doutrina. **Revista de Direito do Consumidor**, v. 116, p. 19 – 49, 2018. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/revista-dos-tribunais-online.html . Acesso em: 10 jul. 2022.

UNIÃO EUROPEIA. **Regulation (Eu) 2016/679 of the European Parliament and of the Council.** 04 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Acesso em: 23 ago. 2022.

TEIXEIRA, Tarcísio; SABO, Isabela Cristina. O uso da tecnologia da informação e a validade jurídica dos negócios realizados por crianças e adolescentes: uma análise de sua hipervulnerabilidade nas relações de consumo virtuais. **Revista de Direito do Consumidor**, v. 104, p. 257 – 283, 2016. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/revista-dos-tribunais-online.html. Acesso em: 21 jun. 2022.

VERBICARO, Dennis; CALANDRINI, Jorge. *Nudges* na proteção de dados pessoais no ciberespaço: um empurrão para incentivar decisões racionais dos consumidores. **Revista de Direito do Consumidor**, v. 142, p. 185 – 214, 2022. Disponível em: https://www.thomsonreuters.com.br/pt/juridico/revista-dos-tribunais-online.html. Acesso em: 14 ago. 2022.