

OTOFORT
OTOFORT
OTOFORT

OTOFORT
OTOFORT
OTOFORT

OTOFORT
OTOFORT
OTOFORT

Com o advento da "Sociedade de Informação", no final do Século XX, o potencial transformador da Tecnologia multiplicou-se, a ponto de prefigurar-se, num horizonte desenhado pela imaginação e pela ficção, a absorção da primeira natureza humana pela segunda, com a cisão dos mundos "um" e "dois" – o surgimento de andróides sobredotados e virtualmente imortais, irreversivelmente pós-humanos, empenhados no caminho para uma eventual "singularidade tecnológica", ou seja, para um momento em que a Tecnologia se autonomizaria e seguiria, incontrolável, o seu próprio caminho, abrindo-se uma clivagem, pela primeira vez desde a invenção da escrita, entre o determinismo e a liberdade como experiências humanas: o que é assustador como possibilidade, mas é riquíssimo como potencial.

Aquém dessa fronteira, explorando as complexidades de um mundo que, rumo a esse triunfo tecnológico que ao mesmo se deseja e se receia, é liderado por um caudal de inovação que se adensa continuamente, resolvendo velhos problemas e gerando novos, reclamando do Direito – e especificamente da sua cidadela conceptual, o Direito Privado – novas posições, novas compreensões, novas respostas, novos horizontes, é que se situa esta obra colectiva que tenho o gosto de prefaciar, coordenada pelas Professoras Dóris Ghilardi e Liz Beatriz Sass.

Nela passam temas candentes da vanguarda jurídica e jurídico-económica, servidos por alguns dos nomes mais talentosos da jovem geração universitária – alguns já consagrados, à mesma velocidade vertiginosa da tecnologia que estudam.

As quatro vertentes dominantes desses estudos são:

- 1) a propriedade intelectual, um domínio no cerne do mundo cultural, a consumação máxima da extra-cerebralização de que a Cultura se compõe, e ao mesmo tempo uma das áreas mais atingidas pelo triunfo da "Sociedade de Informação";
- 2) a protecção de dados, um tema que surge da própria "Sociedade de Informação" como um risco gerado pela circunstância de o ímpeto inovador ir à frente de toda a possibilidade de balizamento e ponderação;
- 3) a regulação e a responsabilidade civil como formas de reacção a essa "liberdade explosiva" que desafia os pressupostos tradicionais em que assentavam os equilíbrios sociais, e em que decorriam as trocas;
- 4) a família, um primeiro regresso ao "mundo um" da corporalidade e do instinto, que nos religa à condição de animais do planeta e aos próprios benefícios da pré-culturalidade (a família não é um fenómeno exclusivo da espécie humana) – mas que também ela se enredou nas teias do progresso tecnológico, o que gera novos problemas a que o Direito, na sua configuração tradicional – e no entanto não muito antiga – já não sabe dar resposta.

Fernando Araújo

Livro financiado pela PROEX/CAPEX

H
HABITUS
EDITORIA



TEMAS ATUAIS DE DIREITO PRIVADO E SOCIEDADE DA INFORMAÇÃO

H
HABITUS
EDITORIA

TEMAS ATUAIS DE DIREITO PRIVADO E SOCIEDADE DA INFORMAÇÃO

O DIREITO NA ERA DIGITAL



DÓRIS GHILARDI
LIZ BEATRIZ SASS
Coordenadoras

Prefácio: Prof. Fernando Araújo
Autora convidada: Valentina Delich

H
HABITUS
EDITORIA



Copyright © 2020 by Dóris Ghilardi e Liz Beatriz Sass

Produção Editorial: Habitus Editora

Editor Responsável: Israel Vilela

Capa e Diagramação: Carla Boito de Barros

Revisora: Valdirene Bressun Formentin

As ideias e opiniões expressas neste livro são de exclusiva responsabilidade dos Autores, não refletindo, necessariamente, a opinião desta Editora.

CONSELHO EDITORIAL:

Alceu de Oliveira Pinto Junior
UNIVALI

Antonio Carlos Brasil Pinto (in memoriam)
UFSC

Cláudio Macedo de Souza
UFSC

Dirajaia Esse Pruner
UNIVALI-AMATRA XII

Edmundo José de Bastos Júnior
UFSC-ESABSC

Eduardo de Carvalho Rêgo
UFSC

Elias Rocha Gonçalves
IPENED-SPCE Portugal-ADMEE Europa-CREFAL Caribe

Fernando Luz da Gama Lobo D'Eça
IS-FASC

Flaviano Vetter Tauschek
CISUSC-ESA-OABSC

Francisco Bissoli Filho
UFSC

Geyson Gonçalves

CISUSC-ESA-OABSC

Gilsilene Passon P. Francischetto

UC-Phragm-EDVES

Jorge Luis Villada

UCASAL-Argentina

Juan Carlos Vezzulla

ISAP (Portugal)

Juliano Keller do Valle

UNIVALI-ESA-OABSC

Lauro Ballock

UNISUL

Marcelo Gomes Silva

UFSC-ESAPSC

Marcelo Buzagó Dantas

UNIVALI

Nazareno Marcineiro

Faculdade da Polícia Militar de Santa Catarina

Paulo de Tarso Brandão

UNIVALI

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

G424I

Ghilardi, Dóris.

Temas Atuais de Direito Privado e Sociedade da Informação: o direito na era digital / Aires José Rover... [et al.], Coordenadoras: Dóris Ghilardi e Liz Beatriz Sass

1ª ed. - Florianópolis: Habitus, 2020.

272 p.; 15,5x22,5 cm

ISBN 978-65-86381-78-8

1. Direito Civil 2. Propriedade Intelectual 3. Direito Digital 2. Novos Temas - Brasil I. Título

CDU 342.12

É proibida a reprodução total ou parcial, por qualquer meio ou processo, inclusive quanto às características gráficas e/ou editoriais.
A violação de direitos autorais constitui crime (Código Penal, art. 184 e seus §§ 1º, 2º e 3º, Lei nº 10.695, de 01/07/2003), sujeitando-se à busca e apreensão e indenizações diversas (Lei nº 9.610/98).



Todos os direitos desta edição reservados à Habitus Editora
www.habituseditora.com.br - habituseditoria@gmail.com

Impresso no Brasil
Printed in Brazil

Dóris Ghilardi
Liz Beatriz Sass
Coordenadoras

TEMAS ATUAIS DE DIREITO PRIVADO E SOCIEDADE DA INFORMAÇÃO O DIREITO NA ERA DIGITAL

Aires José Rover
Aline Beltrame de Moura
Ângela Kretschmann
Dóris Ghilardi
Fabiano Koff Coulon
Gabriel Borges dos Santos
Gabriel Honorato
Geraldina Magella de Faria Rosseto
Ian Borba Rapozo
Jorge Nunes Rosa Filho
Josiane Rose Petry Veronesi
Leandro Canavarros
Leticia Mulinari Gnoatto

Liz Beatriz Sass
Lucas Silveira Duarte
Manoel Gustavo Neubarth Trindade
Mariana Demetruk Marchioro
Márcio M. Szinvelski
Maurilio Casas Maia
Rafaela Paim Cavalcanti Verdi
Rafael de Freitas Valle Dresch
Rafael Carneiro Arnaud Neto
Renan Boccacio Souza da Silva
Valentina Delich
Vitor Almeida
Wilson Engelmann

Grupos de Pesquisa:

GFAM/UFSC/CNPQ - Grupo de Pesquisa em Direito de Família e Sucessões em Perspectiva
NUPPI/UFSC/CNPQ - Núcleo de Pesquisa em Propriedade Intelectual

Obra Financiada pela PROEX/CAPEX



Florianópolis
2020

consignando em papel, e em meios electrónicos, o seu contributo para a Cultura; interpellando o leitor com os seus questionamentos; e, nestes tempos adversos, fornecendo-lhe o exemplo ético de que não abandonaram o seu posto.

Fernando Araújo

Professor Catedrático da Faculdade de Direito da
Universidade de Lisboa – Portugal

SUMÁRIO

PARTE I – PROPRIEDADE INTELECTUAL NA SOCIEDADE DE INFORMAÇÃO	15
CAPÍTULO 1 - DESAFÍOS (LEGALES) DE LOS MUSEOS EN TORNO AL DERECHO DE AUTOR Y LAS POLÍTICAS CULTURALES Valentina Delich	
CAPÍTULO 2 - IMPACTOS ANTICONCORRENCIAIS DA CONCESSÃO DE MARCAS “GENÉRICAS.COM”: O CASO BOOKING.COM V. USPTO Liz Beatriz Sass Lucas Silveira Duarte	33
CAPÍTULO 3 - A GERAÇÃO APP, O PAPEL DO NEUROMARKETING E DOS DIREITOS AUTORAIS NA CONSTRUÇÃO DA “GERAÇÃO CONSUMO” Ángela Kretschmann Gabriel Borges dos Santos	57
PARTE II – A PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DE INFORMAÇÃO	81
CAPÍTULO 4 - DIREITOS HUMANOS E PROTEÇÃO DOS DADOS PESSOAIS EM TEMPOS DE INTELIGÊNCIA ARTIFICIAL: UMA BIBLIOMETRIA TEMÁTICA Aires José Rover	83
CAPÍTULO 5 - RISCO CIBERNÉTICO NO TRATAMENTO DE DADOS PESSOAIS E AUTODETERMINAÇÃO INFORMATIVA: REFLEXÕES À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI N.º 13.709/2018) Wilson Engelmänn Márton M. Szinvelski	99
CAPÍTULO 6 - BREVES APONTAMENTOS SOBRE A AUTODETERMINAÇÃO INFORMATIVA E O DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS Rafael de Freitas Valle Dresch Renan Boccacio Souza da Silva	119
CAPÍTULO 7 - OS DESAFIOS DA APLICAÇÃO EXTRATERRITORIAL DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS PESSOAIS DA UNIÃO EUROPEIA Aline Beltrame de Moura Leticia Mulinari Gnoatton	129

PARTE III – DIREITOS FUNDAMENTAIS DA CRIANÇA E DA FAMÍLIA NA SOCIEDADE DA INFORMAÇÃO 143

CAPÍTULO 8 - A PROTEÇÃO E O TRATAMENTO DE DADOS DE CRIANÇAS E ADOLESCENTES SOB A PERSPECTIVA DA DOUTRINA DA PROTEÇÃO INTEGRAL 145

Josiane Rose Petry Veronese
Geraldina Magella de Faria Rossetto

CAPÍTULO 9 - DESAFIOS DOS NATIVOS DIGITAIS: PERIGOS DA REDE E PROTEÇÃO DE DADOS PESSOAIS 167

Doris Ghilardi
Mariana Demetruk Marchioro
Leandro Canavarros

CAPÍTULO 10 - AUTORIDADE PARENTAL, INTERNET E OS NOVOS CONFLITOS JURÍDICOS. 187

Gabriel Honorato
Raphael Carneiro Arnaud Neto

CAPÍTULO 11 - O DIREITO DAS SUCESSÕES NA SOCIEDADE DA INFORMAÇÃO: UMA OBSOLESCÊNCIA NÃO PROGRAMADA 201

Doris Ghilardi
Jorge Nunes da Rosa Filho

PARTE IV – REGULAÇÃO, MERCADO E RESPONSABILIDADE CIVIL NA SOCIEDADE DA INFORMAÇÃO 217

CAPÍTULO 12 - OS DILEMAS DA TUTELA DO CONSUMIDOR EM FACE DA INTERNET DAS COISAS (IOT) 219

Vitor Almeida
Ian Borba Rapozo

CAPÍTULO 13 - RESPONSABILIDADE CIVIL EM SAÚDE NA SOCIEDADE 5.0: MELHOR INTERESSE DO PACIENTE E TECNOLOGIA NA “RESPONSABILIDADE CIVIL 5.0” 241

Maurilio Casas Maia

CAPÍTULO 14 - A TEORIA DA PERDA DA CHANCE E SUA APLICAÇÃO À LUZ DA ANÁLISE ECONÔMICA DO DIREITO E DAS NOVAS TECNOLOGIAS POR MEIO DA UTILIZAÇÃO DE *BIG DATA* 255

Fabiano Koff Coulon
Manoel Gustavo Neubarth Trindade
Rafaela Paim Cavalcanti Verdi

PARTE I

PROPRIEDADE INTELECTUAL NA SOCIEDADE DE INFORMAÇÃO

OS DILEMAS DA TUTELA DO CONSUMIDOR EM FACE DA INTERNET DAS COISAS (IOT)

Vitor Almeida

Doutor e Mestre em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Professor Adjunto de Direito Civil da Universidade Federal Rural do Rio de Janeiro (ITR/UFRRJ). Coordenador do Núcleo de Pesquisas em Relações Privadas, Direitos Fundamentais e Políticas Públicas (NUREP). Pós-doutorando em Direito Civil pela Universidade do Estado do Rio de Janeiro (UERJ). Advogado. Endereço eletrônico: almeida.vitor@yahoo.com.br

Ian Borba Rapozo

Mestrando em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF). Pesquisador do Núcleo de Pesquisas em Relações Privadas, Direitos Fundamentais e Políticas Públicas (NUREP). Graduado em Direito pela Universidade Federal Rural do Rio de Janeiro (UFRRJ). Advogado. Endereço eletrônico: iborba06@gmail.com

As we build a digital tomorrow, the choices we make today – about the boundaries between our individual and social selves, between consumers and companies, and between citizens and the state – matter.

Neil Richards

1. INTRODUÇÃO: CONSUMIDOR, TECNOLOGIA E O “ADMIRÁVEL MUNDO NOVO”

O alvorecer do século XXI descortina e potencializa uma antiga questão a respeito do descompasso do Direito com o progresso tecnológico. Em diferentes áreas jurídicas, as tentativas de regulamentação dos impactos dos avanços tecnológicos e seus efeitos carecem da velocidade necessária para solucionar os impasses decorrentes das transformações sociais, culturais e econômicas impulsionadas ou criadas pelos aparatos tecnológicos¹. Tal constatação não arrefece no campo do direito do consumidor, mas é agravada se considerada a intrínseca vulnerabilidade da pessoa-consumidora, seja se analisada sob a ótica do desconhecimento técnico, ou da “compulsoriedade” em utilizar as inovações tecnológicas

¹ Nesta linha, Mulholland (2019, p. 485) defende que: “As inovações tecnológicas potencializam a velhice do Direito. Vivemos num momento em que a tecnologia se desenvolve a largos passos e o Direito não consegue acompanhar o seu ritmo. Não se tratando de ciência preditiva, o Direito sempre fica atrás na corrida com – ou para alguns, contra – a tecnologia. De fato, começam a surgir conflitos e questionamentos que devem ser respondidos ou referidos pelo Direito, sempre depois que eles se apresentam como resultado do uso de novas tecnologias”.

numa sociedade que cada vez mais exclui a pessoa não conectada. A bem da verdade, desde serviços bancários, acesso a bens digitais, agendamento de serviços públicos e até mesmo serviços médicos nos impõe uma conectividade constante². Trata-se de uma questão de pertencimento ao mundo digital ou de exclusão desse “admirável mundo novo”.

Como elo mais fraco de uma relação já desequilibrada, a figura do consumidor torna-se ainda mais vulnerável dentro de um contexto de hiperconectividade. As tradicionais vulnerabilidades imputadas ao consumidor dentro de um mercado de consumo em plena expansão já não são suficientes para tutelar de forma adequada as assimetrias provocadas pelos avanços tecnológicos. Neste cenário, a chamada Internet das Coisas (IoT) “representa inovação tecnológica que permite a criação de ambiente interligado através de sensores que conectam objetos ou bens por meio da internet possibilitando não só a comunicação e realização de funções específicas entre coisas, como gerando a cada vez mais constante a coleta, transmissão, guarda e compartilhamento de dados entre objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas” (MULHOLLAND, 2019, 486).³

O que se vislumbra como um distante admirável mundo novo, com efeito, já se apresenta como uma realidade cada vez mais próxima e irrefreável. Alguns casos já nos revelam o agravamento da vulnerabilidade dos consumidores diante desse novo universo tecnológico que se descortina. Tal cenário de hiperconectividade que alcança objetos ou bens de uso pessoal conectados à internet desafia a proteção da segurança, dos dados pessoais e da privacidade do consumidor e impõe “um fluxo contínuo de informações e uma massiva produção de dados” (MAGRANI, 2019, p. 20-21)⁴. Indispensável constatar que as informações circulam de forma cada vez mais intensa e volumosa e que não somente as pessoas inserem dados nas redes, mas “coisas e algoritmos dotados de inteligência artificial que trocam dados e informações entre si, formando um espaço de conexões de rede e de infor-

mações cada vez mais automatizado” (MAGRANI, 2019, p. 19).

Em 2015, por exemplo, a *Samsung* alertou seus consumidores sobre a coleta de dados pessoais feita por sua *smart TV*. Segundo a fabricante, a televisão pode “ouvir” assuntos “pessoais ou confidenciais” falados ao seu redor. O aviso se aplica aos telespectadores que controlam sua *smart TV* da *Samsung* utilizando sua funcionalidade de ativação por voz e o documento esclarece que o aparelho irá ouvir o que as pessoas ao redor estão falando para tentar detectar os comandos de voz da televisão.⁵

Na Inglaterra, em 2016, um casal teve sua intimidade violada e exposta na internet e cenas de sexo dos dois foram postadas num site de pornografia. Como as imagens foram capturadas? Através da *webcam* conectada à TV da casa. De acordo com o jornal *Daily Mail*⁶, que noticiou o caso, não houve nenhuma comunicação com o casal, para ameaça de chantagem ou algo do tipo – *hackers* invadiram o sistema do televisor aleatoriamente e registraram o casal.

Recentemente, foi notícia o vazamento de dados, incluindo conversas entre pais e filhos, pela invasão do *software* de brinquedos infantis, como os *CloudPets* ou a boneca *Cayla*, levando inclusive, em relação a esta, à proibição de sua comercialização em alguns países (LEAL, 2017, p. 178-181). Um ursinho de pelúcia ou uma boneca podem ser perigosos? Na era da Internet das Coisas, essa é uma questão que deve ser levada muito a sério pelos pais, no exercício da autoridade parental responsável, e pelos legisladores por meio de leis repressivas.

Um especialista em segurança cibernética revelou em 2017 um caso envolvendo a *CloudPets*, um conjunto de brinquedos fabricados pela empresa americana *Spiral Toys*. Os brinquedos permitem que os pais conversem com os filhos remotamente. As conversas ficam gravadas e armazenadas – juntamente com senhas encriptadas – num servidor com pouca proteção pertencente a uma empresa romena. As senhas eram facilmente decifráveis. O especialista escutou algumas das mensagens – conversas carinhosas entre os filhos e seus pais. Qualquer um com más intenções poderia descobrir como falar com as crianças pelos brinquedos. Aparentemente, a base de dados violada em diferentes ocasiões usando um mecanismo de busca que identifica objetos conectados, e houve tentativas de pedir um “resgate” à fabricante *Spiral Toys*.

2 “Para estar no mundo da tecnologia e usufruir da sua potencialidade de conveniências e utilidades é necessário renunciar à proteção dos dados pessoais, que se tomam, em grande medida, a moeda de troca padrão desses serviços” (MULHOLLAND, 2019, 493).

3 De acordo com Eduardo Magrani (2019, p. 19-20), a Internet das Coisas é a “expressão que busca designar todo o conjunto de novos serviços e dispositivos que reúnem ao menos três pontos elementares: conectividade, uso de sensores e capacidade computacional de processamento e de armazenamento de dados”.

4 Segundo Eduardo Magrani (2019, p. 20-21), o “termo hiperconectividade foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento”, e “encontra-se hoje atrelado às comunicações entre indivíduos (*person-to-person*, P2P), indivíduos e máquinas (*human-to-machine*, H2M) e entre máquinas (*machine-to-machine*, M2M), valendo-se, para tanto, de diferentes meios de comunicação”.

5 Disponível em <https://www.samsung.com/br/info/privacy/smarttv/>. Acesso em 30 set. 2020.

6 Disponível em <https://www.dailymail.co.uk/news/article-3598012/Trolls-sneak-photos-TV-turn-porn-images-lifted-screens-turned-pornography.html>. Acesso em 30 set. 2020.

O presente artigo apresenta os principais dilemas da Internet da Coisas no que concerne à esfera de proteção dos consumidores, de modo a propor uma releitura das normas em prol da efetiva tutela dos vulneráveis nas relações de consumo. Em especial, a segurança, a privacidade e a liberdade de escolha dos consumidores são colocadas em risco, o que demanda a construção de limites e parâmetros para a sua efetiva proteção diante do fenômeno da Internet das Coisas.

2. VULNERABILIDADE DO CONSUMIDOR NA ERA TECNOLÓGICA

A defesa do consumidor no ordenamento jurídico brasileiro é um imperativo que decorre da própria Constituição da República de 1988. O legislador constituinte consagrou a defesa do consumidor como direito fundamental (art. 5º, XXXII) e princípio geral da atividade econômica (art. 170, V). Nítida, portanto, a opção em proteger de forma prioritária a figura do consumidor, em virtude de sua reconhecida vulnerabilidade (art. 4º, I, CDC), e não por disciplinar as relações de consumo como diretriz constitucional. A par disso, estabeleceu que o desenvolvimento econômico deve, necessariamente, observar a proteção do consumidor, não sendo permitido que os direitos básicos dos consumidores sejam violados em prol do livre jogo de mercado e dos interesses econômicos dos fornecedores de produtos e serviços. Nesse sentido, Guilherme Martins Magalhães (2010, p. 2) pontua que “a opção da Constituição de 1988 de albergar a defesa do consumidor se dá pela inegável necessidade de que certas situações de desequilíbrio social sofram incisiva ação terapêutica do Estado, seja esta ação de cunho econômico ou jurídico”.

Desse modo, por força de expressa determinação do constituinte originário (art. 48 do ADCT), foi promulgado o Código de Defesa do Consumidor (CDC) – Lei n. 8.078, de 11 de setembro de 1990, que surge para dispor, em sede infraconstitucional, sobre os princípios e regras voltados à tutela da parte mais vulnerável da relação de consumo. Tal diploma, portanto, estabelece normas de proteção e defesa do consumidor, de ordem pública e interesse social, conforme previsto em seu art. 1º, com base nas diretrizes de índole constitucional.

Sem embargos, a vulnerabilidade é o elemento justificador de uma normativa mais protetiva ao consumidor em relação aos fornecedores, que assumem o risco de sua atividade em razão das vantagens econômicas obtidas nas operações negociais. Busca-se, a partir de uma tutela da

vulnerabilidade do consumidor, reduzir as desigualdades fáticas existentes entre os polos de uma relação de consumo, fundadas em razões socioeconômicas, técnicas, jurídicas e informacionais, de modo a proteger e promover a pessoa do consumidor, sobretudo no que tange ao seu direito à vida, saúde, segurança, informação, liberdade de escolha e igualdade nas contratações. Por ocasião de tal desiderato, indiscutível que tutelar o vulnerável consumidor serve para abrandar o cenário de hiperconsumo na sociedade contemporânea⁷, na medida em que se estabelecem mecanismos inibitórios para o estímulo desenfreado à aquisição de bens e serviços, calcados notadamente nos direitos básicos à educação e à divulgação sobre o consumo adequado dos produtos e serviços.

Decerto que o fundamento nuclear da proteção do consumidor na ordem civil-constitucional é extraído dos princípios da dignidade da pessoa humana e da solidariedade social. Nesse sentido, Guilherme Magalhães Martins (2010, p. 6) leciona que a defesa do consumidor é um direito fundamental que encontra suas raízes na cláusula geral de proteção à dignidade da pessoa humana, razão pela qual defende que o “cidadão-consumidor, ou melhor, a pessoa-consumidor, se projeta na dimensão constitucional, de modo que, na hipótese de conflito entre o respectivo direito fundamental – sobretudo quando traduzido nas situações jurídicas existenciais – e as exigências de mercado livre, sua primazia se mostra fora de discussão”. O fundamento, portanto, da enérgica tutela do consumidor é de inequívoca índole constitucional.

A partir da promulgação do CDC, pelo menos, na órbita do consumo, a proteção legal da parte mais frágil se impôs como indispensável para que o mercado de consumo se tornasse mais solidário e equilibrado. O princípio da solidariedade social é, nessa linha, “o fundamento de um regime jurídico protetivo em relação ao consumidor, na medida em que visa diminuir as escancaradas disparidades existentes, tornando as relações de consumo mais condizentes com a ótica solidária, que deve permear todos os setores do ordenamento brasileiro” (FURTADO; ALMEIDA, 2020, p. 570). A interpretação conforme à Constituição das normas previstas no CDC descortina um marco normativo indispensável à

⁷ O sociólogo Zygmunt Bauman (2007, p. 16-17) observou que “a vida líquida é uma vida de consumo. Projeta o mundo e todos os seus fragmentos animados e inanimados como objetos de consumo, ou seja, objetos que perdem a utilidade (e portanto o visto, a atração, o poder de sedução e valor) enquanto são usados. Molda o julgamento e a avaliação de todos os fragmentos animados e inanimados do mundo segundo o padrão dos objetos de consumo”. Sobre os consumidores na sociedade líquido-moderna, Zygmunt Bauman desenvolve com maior profundidade as reflexões sobre o tema no Capítulo 5 do livro acima indicado, em especial nas páginas 106-151.

promoção dos direitos fundamentais dos consumidores, cujo atual desafio é implementá-lo e expandi-lo a todos os confins onde se verifique a presença da vulnerabilidade do consumidor.

Observa-se que, desde os fins da década de 1990, acentuaram-se as relações de consumo em ambiente virtual no Brasil, a partir do momento que os usuários se tornaram potenciais consumidores de produtos e serviços oferecidos na rede. No entanto, a massiva utilização da internet com a finalidade de consumir não foi acompanhada de uma regulamentação específica que se dispusesse a estabelecer os princípios e as regras atinentes a essas relações travadas em âmbito eletrônico, em especial diante das características da impessoalidade e da velocidade das contratações eletrônicas via internet⁸, o que exige parâmetros de segurança e de confiança dos *ciberconsumidores*⁹. Com maior vigor a proteção do consumidor na seara tecnológica assume especial destaque diante do fenômeno da Internet das Coisas (IoT).

No Brasil, com a promulgação do chamado Marco Civil da Internet – Lei n. 12.965, de 23 de abril de 2014, que dispõe sobre os princípios, garantias, direitos e deveres para o uso da Internet no país, o legislador se posicionou claramente pela necessidade de regulamentação da internet, mas garantiu, em seu art. 3º, como princípios cardiais do uso da internet no Brasil a liberdade de expressão e a proteção da privacidade e dos dados pessoais. Observa-se, portanto, o balanceamento dos valores constitucionais realizado pelo legislador infraconstitucional, eis que, ao mesmo tempo em que se preservou a privacidade, os dados pessoais, e a neutralidade da rede, por outro lado, quis o legislador reafirmar o espaço virtual como um *locus* genuíno para o exercício das liberdades fundamentais, constitucionalmente garantidas, mas desde que sejam exercidas dentro do contexto de solidariedade social.

Nessa diretriz, a Lei n. 12.965/2014 estabelece em seu art. 7º que o acesso à internet é essencial ao exercício da cidadania e elenca um rol de direitos dos usuários, fortalecendo a proteção daqueles que utilizam a internet e garantindo o exercício dos direitos fundamentais na rede. Tal dispositivo se preocupou precipitadamente com a proteção da privacidade do usuário e o direito à informação em relação à coleta, armazenamento e uso dos dados pessoais dos usuários.

⁸ Sobre o assunto, cf. Gabriel Furtado e Vitor Almeida (2020, p. 574-583).

⁹ O termo *ciberconsumidor* tem sido utilizado pela doutrina estrangeira e nacional. Alhures vem sendo empregado em Portugal por Elisa Dias Oliveira (2002) e Thilbaut Verbiest (2002). Na doutrina nacional, o neologismo é amplamente utilizado por Pedro Modenesi (2011, p. 63 ss). Embora o autor ressaltasse que certamente de forma pioneira, foi entre nós mencionado por Cláudia Lima Marques.

Enquanto se aguarda uma posição do legislador infraconstitucional¹⁰, não deve haver dúvidas quanto à incidência das normas de defesa do consumidor albergadas no Código vigente ao comércio eletrônico, mesmo diante de suas peculiaridades e da ausência de regras específicas, mesmo porque sua promulgação é anterior ao desenvolvimento e expansão da internet no país. O caráter historicamente condicionado do Direito descortina a necessidade de uma interpretação vocacionada a superar o imobilismo dos textos legislativos através de uma visão sistêmica e promocional do ordenamento jurídico.¹¹

Além disso, o Marco Civil da Internet assegurou a defesa do consumidor tanto como um dos fundamentos da disciplina do uso da internet no Brasil (art. 2º, V), bem como assegurou a aplicação das normas de proteção e defesa do consumidor nas relações de consumo na internet como um dos direitos dos usuários (art. 7º, XIII). Assim, resta claro que embora o Marco Civil da Internet não discipline especificamente a proteção do usuário-consumidor, ele assegurou a defesa do consumidor como um de seus pilares, deixando para lei específica o tratamento do tema. Por isso, há que se repisar que a alteração dos meios em que as relações de consumo ocorrem – como no comércio eletrônico, por exemplo – não implica no afastamento da incidência das normas protetivas do consumidor. Pelo contrário, há de se preservar o Código de Defesa do Consumidor como normativa geral dessas relações, sendo que qualquer legislação específica vindoura ou atualização no próprio Código não pode contrariar e nem diminuir a proteção atualmente já concedida aos consumidores, sob pena de indevido retrocesso social.

Ademais, o requisito de incidência das normas de defesa do consumidor, a vulnerabilidade deste, encontra-se especialmente agravado no domínio cibernético, notadamente no que concerne à desigualdade informacional constatada entre os polos da relação. As aviltantes disparidades impõem uma tutela voltada à proteção mais veemente da confiança dos consumidores-usuários. A intensidade do princípio da boa-fé objetiva¹² deve ser reforçada para a melhor equalização do desnivelamento de informação existente entre os lados da relação de consumo na internet. É através

¹⁰ Cabe ressaltar que se encontra em tramitação no Congresso Nacional o Projeto de Lei nº 281/12 que trata especificamente da regulamentação do comércio eletrônico. Diz a ementa do projeto: "Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico".

¹¹ Sobre a função promocional do direito recomenda-se Norberto Bobbio (2007).

¹² Ver a respeito da aplicação do princípio da boa-fé objetiva no direito civil e no direito do consumidor Gustavo Tepedino e Anderson Schreiber (2005, p. 29-44).

do fortalecimento dos deveres de confiança e lealdade, estabelecidos através de *standards* de conduta, que o mandamento constitucional de proteção do consumidor se efetivará nas contratações de consumo via internet.

A revolução social gerada pelo advento da internet trouxe em seu bojo a facilitação das comunicações a distância e das transações negociais, revelando-se uma ferramenta extremamente útil e necessária em um mundo globalizado. Isso implica, contudo, no surgimento de novos riscos ao consumidor no ambiente eletrônico, agravando sua condição de vulnerabilidade. E isso faz com que a preocupação com a proteção do consumidor seja ainda mais robusta, tendo-se em conta que a impessoalidade, a distância entre si e os fornecedores e a velocidade dos anúncios e das transações diminuem o poder de análise e reflexão dos consumidores em relação à aquisição de produtos e serviços. Pedro Modenesi (2011, p. 98) afirma que “resta evidenciado que há, de fato, uma nova e especial vulnerabilidade experimentada pelos *ciberconsumidores* nessa contemporânea maneira de contratar”. Daí se falar da passagem do estado de vulnerabilidade do consumidor para a hipervulnerabilidade do *ciberconsumidor*.

Na era da hiperconectividade, os desafios impostos à tutela do consumidor são ainda mais acentuados e de difícil solução. Novas plataformas de negócios surgem rapidamente, e os fenômenos da Internet das Coisas e da inteligência artificial tendem a trazer, por um lado, maiores comodidades aos consumidores, mas, por outro turno, os tornam refém de um perfil previamente moldado com base nos dados coletados, o que afeta a liberdade de escolha, e, sobretudo, devassam a privacidade e os dados pessoais dos consumidores, sem seu consentimento e com finalidade de não compatíveis com a tutela prioritária da pessoa humana.

3. INTERNET DAS COISAS (IOT) E OS EFEITOS SOBRE A TUTELA DO CONSUMIDOR

O termo “Internet das Coisas”, usualmente tratado pela sigla de sua tradução em inglês *IoT – Internet of Things* -, é utilizado para designar a conectividade de objetos cotidianos em uma rede na qual estes, sensíveis à internet, são instrumentalizados com sensores e se tornam capazes de tomar decisões contextualizadas a partir de procedimentalidade algorítmica, desencadeando ações e processamento de dados em uma ampla rede de agências (mediações) (MARQUES; LEMOS, 2017, p. 11).

Com efeito, qualquer objeto imaginável pode, teoricamente, ser in-

serido no universo da Internet das Coisas, desde que sejam eletrônicos e capazes de se conectar à internet. De um simples relógio de pulso, até o indicador de número de vagas disponíveis em um estacionamento e em que direção elas estão ou um aviso espontâneo no painel do carro, informando em tempo real sobre o trânsito na cidade e o tempo que o motorista levará até sua casa. Objetos que já estão presentes no cotidiano se tornam inteligentes e têm suas funções ampliadas a partir das agências, por cruzamento de dados em rede.¹³

Neste universo é relevante compreender ainda o conceito de sensibilidade performativa. A expressão é utilizada para denominar uma forma específica de sensibilidade e performance dos objetos inteligentes a partir do fenômeno da dataficação, ou seja, transformar toda espécie de informação sobre o indivíduo em dados mensuráveis e analisáveis e tomar decisões com base na análise dos dados. Conforme afirmam Daniel Marques e André Lemos (2017, p. 13), tomando a sensibilidade performativa como ponto de partida, é possível compreender os objetos inteligentes como sencientes, “capazes de perceber a si mesmo e o ambiente, comunicando-se de forma autônoma e uma rede digital, gerando agências em outros objetos, instituições e/ou humanos” (MARQUES; LEMOS, 2017, p. 13).

A base de dispositivos inteligentes instalados, que são classificados como “difíceis de proteger” (*hard-to-secure smart things*), como TVs, geladeiras e câmeras de segurança, tinha a expectativa de crescimento de 31% em 2017, o que permitiria atingir 8,4 bilhões de dispositivos, ou cerca de um bilhão a mais que a população total do mundo. Segundo a pesquisa feita pela empresa *Gartner* em janeiro de 2017, a previsão para o ano de 2020 seria de 12.863 milhões de unidades de dispositivos inteligentes da categoria de consumo instalados pelo mundo. Ainda de acordo com a pesquisa, a projeção para 2020 seria no patamar de 1,494,466 bilhões de dólares em relação ao gasto mundial com dispositivos inteligentes na categoria de consumo.¹⁴

A IoT torna-se uma realidade irrefreável e extremamente célere, bem como projeta profundos impactos sociais e econômicos. Cada vez mais dispositivos conectados, sensores coletores de dados, automação de processos e máquinas comunicam-se sem a intervenção humana. Não obstante, essa hiperconectividade crescente pode acarretar uma série de problemas, de diversas ordens, como as vulnerabilidades relacionadas à

¹³ Disponível em <<https://www.proof.com.br/blog/internet-das-coisas/>>. Acesso em 07 mar. 2020.

¹⁴ Pesquisa disponível em <<https://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/>>. Acesso em 07 mar. 2020.

privacidade e à segurança dos usuários consumidores. É de extrema relevância compreender o papel do Estado e das empresas fornecedoras desse tipo de bens e serviços neste contexto (MAGRANI, 2018, p. 91).

A internet das coisas e os riscos do admirável mundo novo retomam de alguma maneira a dificuldade do Direito em lidar com os rápidos avanços tecnológicos. Com efeito, essas inovações tecnológicas desafiam o Direito como um todo. No caso brasileiro, os desafios para as aplicações da tecnologia incluem questões tributárias, de direito da infraestrutura, e, em particular, efeitos sobre a tutela do consumidor.

Nesta seara, os desafios no novo universo vão desde questões relacionadas a direitos fundamentais do consumidor, como segurança e privacidade, até indagações referentes ao regime de responsabilidades. A título de exemplo, o Código de Defesa do Consumidor definiu os objetos da relação de consumo, o produto e o serviço, de maneira extremamente ampla, sendo estes, respectivamente, “qualquer bem, móvel ou imóvel, material ou imaterial” (art. 3º, §1º) e “qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista” (art. 3º, §2º).

A distinção realizada levou à criação de um consistente sistema de imposição de deveres de adequação e segurança ao fornecedor, implicando no regime de responsabilidades por fato ou vício dos produtos ou serviços, conforme previsto nos artigos 12 a 20 do CDC. No contexto da IoT, a qualificação do fato que dá causa aos deveres impostos pelo regime de responsabilidade é conturbada, tendo em vista que ao mesmo tempo em que se tem um produto, há também, por intermédio dele, o mesmo fornecedor ou outro oferecendo a prestação de um serviço (MIRAGEM, 2017). Ou seja, a distinção dos regimes de responsabilidades não se faz tão nítida¹⁵, o que exige do intérprete uma acurada análise a partir das circunstâncias do caso concreto para qualificar a situação à luz da normativa consumerista, o que pode ensejar na incidência das normas de responsabilização pelo fato do produto e do serviço no mesmo caso específico.

Lembre-se ainda que a legislação consumerista brasileira é de ex-

15 Relativamente à tutela dos dados pessoais, questão intimamente ligada ao tema sob estudo, Maria Celina Bodin de Moraes (2019) esclarece que o legislador, ao elaborar o regime de responsabilidade civil na Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018), não optou nem pelo regime subjetivo, nem pelo objetivo, mas sim por um regime baseado na prevenção dos danos, baseado no risco inerente à atividade de tratamento de dados, classificando-o como um regime “proativo” de responsabilidade.

trema clareza ao limitar o fornecedor, exigindo em seu art. 8º que apenas coloque no mercado aqueles produtos cujos riscos sejam normais e previsíveis. Indaga-se então: seriam os riscos dos novos produtos inteligentes normais e previsíveis?

4. OS DESAFIOS DA PROTEÇÃO DO CONSUMIDOR NA ERA DA INTERNET DAS COISAS (IOT)

A noção de Internet das Coisas pode parecer nova e, de fato, traz algumas inovações no campo da tecnologia aplicada ao cotidiano, mas o cenário no qual se desenvolve já vem sendo preparado ao longo do tempo pela junção, principalmente, de três elementos. Em primeiro lugar, como já abordado, tem-se a massificação dos dispositivos eletrônicos conectados presentes na sociedade, que se comunicam uns com os outros e têm sua “inteligência” cada vez mais avançada. Juntamente a isto é preciso considerar o fenômeno do chamado *big data* e a crescente capacidade de processamento de enormes volumes de dados em grandes velocidades. Por último, os aparelhos conectados geram dados que são processados e proporcionam assim, através da inteligência artificial e da sensibilidade performativa, a retirada de conclusões lógicas. Com efeito, estes três elementos compõem o complexo cenário de explosão de dados na sociedade e devem ser considerados quando da análise do fenômeno da Internet das Coisas.

É importante notar, também, que apesar de a Internet das Coisas potencializar alguns problemas relacionados à privacidade, alguns deles já estão presentes na vida dos consumidores há algum tempo, como a possibilidade de identificação, rastreamento e perfilização a partir da análise de dados (MARQUES; LEMOS, 2017, p. 16).

Indispensável afastar qualquer concepção tendente a demonizar o fenômeno da IoT, uma vez que ela acarreta a construção de um novo modelo de sociedade e traz vantagens e eficiência para diversos setores e aspectos da vida cotidiana. Contudo, descortina a ameaça do monitoramento constante e a consequente constatação de que alguns direitos de grande importância podem ser violados a partir disso, de forma que é essencial entender de que maneira a tutela do consumidor é capaz de reprimir essas violações. É absolutamente necessário compreender as vantagens e desvantagens que o avanço tecnológico proporciona, especialmente quando atinge grupos vulneráveis, como os consumidores. Percebe-se que um dos maiores problemas da IoT é a invisibilidade dos processos envolvendo os dados dos usuários (MARQUES; LEMOS, 2017, *passim*).

Outro relevante problema apontado é que os objetos inteligentes têm uma baixa capacidade computacional. Os protocolos de segurança tradicionais e o estágio que a criptografia alcançou nos dias de hoje demandam uma grande quantidade de memória, energia e recursos de computador, dificultando a sua implementação em alguns dispositivos que integram o universo da rede de compartilhamento de dados (MAGRANI, 2018, p. 101).

Isso nos leva ao primeiro desafio relacionado à Internet das Coisas, que se intensifica na seara consumerista: manter a confidencialidade da informação coletada. Em uma sociedade de consumo, tal qual a que vivemos, é imprescindível que o fator mercadológico seja levado em consideração para a análise aqui proposta, pois essa dimensão influencia diretamente no tratamento da rede de dados e na privacidade do usuário. Indissociável do sistema capitalista a busca pelo lucro, logo, não é espantoso que o contínuo lançamento de produtos faça com estes sejam cada vez mais baratos, em busca de competitividade no mercado, de modo a deixar os investimentos em segurança e opções de configuração e privacidade de lado, como algo não primordial. Não obstante, é preciso ter em mente que informações, os dados, são hoje uma espécie de moeda valiosa. O principal modelo de negócio envolvendo dados pessoais é pautado na sua comercialização, troca e análise, o que proporciona, por exemplo, a perfilização de consumidores (MARQUES; LEMOS, 2017, p. 20).

Uma possível solução, neste ponto, remonta ao conceito já tratado de sensibilidade performativa, pois o termo envolve diretamente a proteção da privacidade dos usuários ou as possíveis ameaças a ela. Por exemplo, uma lâmpada que se acende automaticamente ou um aparelho de som que começa a tocar música ambiente quando detectam algum movimento não precisam de identificação facial ou cruzamento de dados do usuário detectado com outros bancos de dados para que tenham sua funcionalidade totalmente aproveitada. Nestes casos há uma sensibilidade performativa construída levando em consideração a proteção da pessoa e de sua privacidade. A diferenciação está na intencionalidade no projeto do produto e/ou serviço em preservar a impessoalidade do dado coletado – nestes casos, o movimento (MARQUES; LEMOS, 2017, p. 13).

Nesse sistema, a preservação da privacidade é um conceito incorporado já à própria estruturação dos processos desenvolvidos, de forma a garantir ao consumidor, através da infraestrutura do serviço prestado, condições ideais para que preserve sua privacidade e gerencie o tratamento de seus dados pessoais.

Esse conceito, denominado privacidade por design (*privacy by design*) foi desenvolvido por Ann Cavoukian na década de 1990, com o objetivo de alterar a maneira como a privacidade era tratada em sistema de *big data* para que a garantia deste direito se tornasse o modo de atuação padrão das empresas da área. O ponto chave é que a privacidade seja levada em conta durante todo o ciclo de vida do sistema inteligente, desde o seu projeto inicial até sua aplicação final frente ao consumidor (MAGRANI, 2018, p. 103).

Apesar disso, a tutela do consumidor não pode depender da boa vontade do mercado, embora cada vez mais a autorregulamentação e as práticas de *compliance* constituam importantes movimentos dos fornecedores na defesa dos consumidores. Ainda assim, o Estado deve agir para proteger os direitos do consumidor vulnerável, assim como estabelecido na Constituição Federal. Esta tutela não implica, no entanto, no refreamento do desenvolvimento tecnológico. O papel do Poder Público é, pelo contrário, fomentar toda forma de desenvolvimento social, sem, contudo, deixar de garantir os direitos fundamentais dos indivíduos e tutelar as vulnerabilidades existentes no corpo social, primando sempre pela isonomia substancial.

Conforme afirma Neil Richards (2015, p. 5), não é preciso abrir mão totalmente da privacidade. É necessário, no entanto, pensá-la de forma mais criativa. Leis de confidencialidade e de proteção ao consumidor, tal qual o Código de Defesa do Consumidor, desempenham um importante papel no que concerne à privacidade no ambiente digital. Contudo, é de suma importância definir e compreender muito bem o direito à privacidade e suas formas, para que se alcance uma proteção eficaz dos dados pessoais.

A privacidade no direito brasileiro é tratada na Constituição Federal, como um direito fundamental, em seu art. 5º, inciso X e no art. 21 do Código Civil de 2002. Seu conceito evoluiu com o passar dos anos e, atualmente, não está mais associada unicamente ao direito de ser deixado só, abarcando também as situações concernentes à liberdade de escolhas de caráter existencial e ao controle de dados sensíveis pelo seu titular. Nesse sentido, afirmar-se, no direito contemporâneo, que a privacidade é diretamente relacionada ao controle sobre suas próprias informações (MULHOLLAND, 2018, p. 172).

Diferentemente dos Estados Unidos, onde a privacidade encontra suas raízes em um direito do indivíduo, de caráter negativo, a concepção europeia aborda o aspecto social da privacidade, desenvolvendo-a com características de direito positivo, de forma que se exige do Estado medidas para garantir a proteção de dados pessoais. Foi a partir da visão

européia que a privacidade mostrou seu novo perfil, desdobrando-se no direito à autodeterminação informativa, o que é extremamente valioso no contexto da sociedade hodierna, em que a própria informação se tornou um bem (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 43).

Para que se tenha uma noção mais prática de como funciona a dinâmica do “mercado” de informações online basta perceber que o download de aplicativos como Facebook, Instagram ou Whatsapp não é gratuito, como aparenta ser. Os dados de usuários se tornaram uma das moedas mais valiosas atualmente e, teoricamente, ao concordar com os termos e políticas de uso desses aplicativos, o usuário autoriza que suas informações estejam disponíveis para o acesso do governo e de outras empresas.

Em suma, como leciona Caitlin Sampaio Mulholland (2018, p. 172-173), há três concepções possíveis a respeito do direito à privacidade: (a) o direito de ser deixado só; (b) o direito de ter controle sobre a circulação dos dados pessoais (autodeterminação informativa) e; (c) o direito à liberdade para escolhas de caráter pessoal. No primeiro ponto, referente ao direito de ser deixado só, quando o controle de acesso diz respeito a algo físico, um ambiente como, por exemplo, a casa do indivíduo, trata-se da dimensão espacial da privacidade. Sob outra perspectiva, quando o controle de acesso concerne a algo intangível, admite-se a divisão em dois tipos: o primeiro, o aspecto decisional da privacidade, é atinente à proteção contra a interferência indesejada em relação às ações e decisões individuais; já o segundo, resume-se na autodeterminação informativa, ou seja, a dimensão informacional da privacidade (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 48).

Interessante notar ainda que no campo da IoT, a dimensão decisional da privacidade terá constantemente um ponto de encontro com a dimensão informacional, ao passo que diversos assuntos que dizem respeito ao modo de viver do consumidor acabam sendo convertidos em dados sensíveis, cuja proteção, nestes casos, é imprescindível para a integral tutela dos direitos do consumidor (PEIXOTO; EHRHARDT JÚNIOR, 2018, p. 51).

Um exemplo de violação da privacidade diretamente relacionado ao universo da IoT ocorreu no ano de 2018, quando as Cortes de diversos estados norte-americanos começaram a enfrentar casos judiciais envolvendo a assistente pessoal da Amazon, a Alexa. Supostamente, o aparelho somente deveria gravar em áudio o que acontece no ambiente em volta após o usuário dizer o nome do aparelho em voz alta ou alguma palavra de ativação previamente selecionada. Apesar disso, diversos usuários

notaram que suas conversas estavam sendo gravadas – e algumas vezes enviadas a contatos aleatórios – sem que isso fosse requisitado.

Outro caso envolvendo diretamente o controle de dados aconteceu na Austrália no ano de 2016. A *Red Cross Blood Service*, responsável pela coleta e doação de sangue no país, foi vítima de uma falha em seu sistema de segurança, o que levou ao vazamento de dados pessoais de mais de 500.000 homens¹⁶. O fato é especialmente problemático tendo em vista a natureza das informações indevidamente divulgadas, que incluíam nome, endereço e questões mais específicas, como o fato de o indivíduo ter ou não comportamento sexual de risco¹⁷, ou seja, dados pessoais sensíveis. Atualmente, no Brasil, o art. 3º, § 3º, inciso II da Lei n. 12.414/19 – a chamada Lei do Cadastro Positivo, caracteriza como informações sensíveis aquelas relativas à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas. Por sua vez, a LGPD (Lei n. 13.708/2018), em seu art. 5º, inciso II, considera sensível todo “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural”, cujo tratamento é disciplina entre os arts. 11 a 13.

Tendo em vista a relevância do direito envolvido e a necessidade da tutela efetiva do consumidor, é de suma importância ter em mente que investigar as questões concernentes à privacidade na IoT demanda a observação de toda a rede de agências entre os objetos inteligentes, considerando desde o sensor presente no produto e suas funcionalidades, passando pelo discurso das empresas que comercializam os dispositivos, até o tratamento dos dados colhidos. O que dasagua no segundo desafio apresentado pelo universo da IoT: manter a integridade e disponibilidade da informação.

Uma vez que empresas e pessoas passam a “depende” de informações que chegam através de sinais de sensores, o que pode acontecer se essas informações chegarem erradas? E se não chegarem? É possível constatar a periculosidade envolvida na questão a partir de um caso recente no Brasil, envolvendo a empresa de comércio eletrônico OLX, cuja sentença foi prolatada em fevereiro de 2020. Na lide em questão o autor teve seu

16 Disponível em <<https://www.oaic.gov.au/updates/news-and-media/australian-red-cross-blood-service-data-breach/>>. Acesso em 10 mar. 2020.

17 Disponível em <www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036>. Acesso em 10 mar. 2020.

pedido julgado parcialmente procedente para perceber a quantia de 20 mil reais a título de danos morais, tendo em vista que seus dados pessoais, como imagem e nome, foram utilizados de forma indevida para a prática de atividades ilícitas através do site. Na sentença a magistrada ressaltou que a responsabilidade da empresa foi determinada com base na ausência de mecanismos de *Compliance* e de checagem da autenticidade do usuário, o que viola o dever de segurança imposto ao fornecedor de serviços pelo art. 14, §1º do Código de Defesa do Consumidor (BRASIL, 2020).

Bruno Magrani (2018, p. 92) aponta que, conforme a pesquisa realizada pela empresa *HO Security Research*, 70% dos dispositivos conectados à internet das coisas apresentam graves falhas de segurança relacionadas principalmente a falta de criptografia e *softwares* de proteção inadequados, de forma que os dados dos consumidores ficam expostos a vazamentos ou ataques de *hackers*.

Com efeito, a cadeia de processamento dos dados dos consumidores é composta por quatro estágios. O primeiro, obviamente, a coleta dos dados pelos aparelhos inteligentes. Em segundo lugar, com o dado devidamente coletado, entra em cheque a questão do armazenamento, envolvendo diretamente a segurança das informações recolhidas. Após o armazenamento, é preciso abordar as formas de acesso ao dado coletado. A questão envolve não apenas a segurança em relação aos indivíduos que não devem ter acesso às informações, mas também à garantia dos próprios titulares de saber quais dados seus estão armazenados e de que forma estão sendo tratados, o que resulta no último ponto, o tratamento, ou seja, a forma como o dado coletado será processado e utilizado.

A coleta de dados no cotidiano é um fenômeno constante e massivo, cuja tendência é aumentar exponencialmente, tendo em vista que cada vez mais há produtos inteligentes no mercado, transformando o indivíduo em uma verdadeira e rica fonte de dados (MARQUES; LEMOS, 2017, p. 17).

A integridade da informação é um ponto de extrema relevância pois, uma vez que os dados são coletados pelos dispositivos interconectados, em uma rede que não conta com a segurança adequada à proteção eficaz da privacidade, o objeto “coletor” não será o único a possuir os dados coletados e processados, o que abre um grande espaço para práticas nocivas e abusivas ao consumidor como a perfilação e a identificação pessoal (MARQUES; LEMOS, 2017, p. 18).

Neste ponto, ressalte-se, mais uma vez, a incapacidade dos dispositi-

vos inteligentes para executar criptografias de maior complexidade e em velocidade rápida o suficiente para garantir a transmissão segura dos dados coletados, o que é essencial para uma abordagem eficaz da privacidade.

Crucial destacar que a boa-fé objetiva é um princípio elencado no art. 4º, inciso III do CDC, ou seja, é um princípio intrínseco à tutela consumerista e deve ser observado em todos os momentos da relação de consumo, seja na fase pré-contratual, contratual ou pós-contratual. Com efeito, tal qual os demais princípios de envergadura constitucional, a boa-fé objetiva, corolário da solidariedade social, atua como a lente através da qual o ordenamento posto deve ser interpretado, inclusive em relação ao direito a informação garantido ao consumidor (art. 6º, III, CDC) (BENJAMIN; MARQUES; BESSA, 2016, p. 68).

Convém repisar que, no Direito brasileiro, foi promulgada a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n.º 13.709, de 14 de agosto de 2018, já em pleno vigor. Embora não trate da privacidade no contexto do fenômeno da IoT, seus princípios são plenamente aplicáveis ao caso, especialmente a tutela dos dados sensíveis e da proteção da criança e do adolescente. A LGPD dispõe sobre o tratamento de dados pessoais, seja por meio físico ou digital, por pessoa natural ou jurídica, inclusive de direito público, com a finalidade de garantir direitos fundamentais como a liberdade de expressão e a privacidade, conforme aponta seu art. 1º. A Lei é enfática ao afirmar a promoção do livre desenvolvimento da personalidade, a partir da tutela dos dados pessoais, bem como o respeito aos direitos humanos (art. 2º, VII).

Assim como a legislação europeia¹⁸, a LGPD traz em seu texto as definições que lhe são essenciais e os princípios que norteiam sua aplicação. Não por outra razão é importante ressaltar que seu art. 2º, inciso VI, elenca a defesa do consumidor como um dos fundamentos da disciplina da proteção de dados pessoais. A seu turno, o Código de Defesa do Consumidor, em seu capítulo III, elenca os direitos básicos do consumidor no Brasil, em reverência à determinação constitucional contida no art. 5º, inciso XXXII, da Carta Magna. No mesmo capítulo da legislação consumerista, o art. 7º assegura a possibilidade de que os direitos dos consumidores estejam localizados em outras leis ou fontes, seja na forma de tratados, leis ordinárias ou portarias administrativas.

18 A Lei 13.709/18 é claramente inspirada no *General Data Protection Regulation*, uma versão atualizada de outra lei de privacidade da União Europeia, chamada “*Data Protection Directive*” que estava em vigência desde 1995, objetivando tutelar o tratamento dos dados pessoais de seus cidadãos.

Efetivamente, como já afirmado, os princípios estabelecidos pela LGPD não são incompatíveis com o que é estabelecido na seara do direito do consumidor, de forma que a nova lei deve ser aplicada de maneira a reforçar a defesa do consumidor no terreno da proteção dos dados pessoais. Patente, portanto, a sinergia entre CDC e LGPD, que devem ser interpretadas e aplicadas de forma coordenada e harmônica, em constante diálogo entre fontes, de modo a extrair a máxima efetividade dos comandos constitucionais.

Os princípios da LGPD que chamam maior atenção são os da finalidade e da não discriminação, devido à sua grande relevância social. De acordo com o primeiro, todos os dados devem ser coletados e tratados para um propósito determinado, previamente estabelecido, e que deve ser informado ao titular dos dados de maneira clara e explícita, vedando sua utilização para qualquer outro fim diverso do informado. Por sua vez, o princípio da não discriminação garante que os dados não serão utilizados para fins discriminatórios ilícitos ou abusivos, tendo-se por medida tanto os critérios definidos em normas expressas quanto por princípios como o da boa-fé objetiva (MULHOLLAND, 2018, p. 163-165). Igualmente importante para a tutela do consumidor é o princípio do livre acesso, estabelecido no art. 5º, inciso IV, da LGPD. O princípio em questão garante ao titular do dado que ele tem direito à consulta sobre a forma e o período do tratamento de seus dados pessoais, de maneira gratuita e facilitada.

Vale mencionar aqui o acerto da legislação ao garantir de forma expressa em seu texto que a consulta aos dados pessoais pelo titular será de forma facilitada, tendo em vista a especificidade da área e levando em consideração, inclusive, a vulnerabilidade técnica do consumidor. Os aparatos tecnológicos, mais ainda no contexto da IoT, envolvem uma série de conhecimentos técnicos, que os usuários na maior parte das vezes não possuem. Termos especiais, inovações tecnológicas e atualizações, práticas de segurança específicas, enfim, trata-se de uma área que facilmente extrapola a *expertise* do consumidor padrão e que nem pode ser exigida dele.

Paralelamente, o Código de Defesa do Consumidor, ao tratar dos seus princípios norteadores, prima, em seu art. 4º, inciso III, pela harmonização e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico. Tramita atualmente no Congresso Nacional o Projeto de Lei nº 3.514/15, que visa modernizar o CDC, de maneira que disponha também sobre o comércio eletrônico. Há duas principais alterações relevantes para o tema em estudo. A primeira

se refere à inclusão do inciso XI ao artigo 6º do CDC, que trata dos direitos básicos do consumidor. Na primeira parte o dispositivo proposto inclui a privacidade e a segurança das informações e dados pessoais no rol de direitos básicos, garantindo, em sua segunda parte, o acesso gratuito do consumidor aos referidos dados e suas fontes, em consonância com o já mencionado princípio do livre acesso. A segunda alteração está na inclusão do art. 45-A, que visa, dentre outros objetivos, preservar a segurança nas transações e a proteção da autodeterminação e da privacidade em relação aos dados pessoais do consumidor.

O referido projeto traz também como um direito básico do consumidor a liberdade de escolha, notadamente em relação às novas tecnologias e redes de dados, vedando a discriminação e o assédio de consumo (art. 6º, inciso XII). Nesse tocante, importante tratar do terceiro desafio aqui apontado: a imposição de limites ao excesso de informação (*big data*) na vida pessoal. A rigor, o tratamento de *big data* é cada vez mais facilitado pelas técnicas computacionais desenvolvidas e tem a capacidade de apresentar análises probabilísticas e resultados que podem, potencialmente, enfraquecer ou mesmo retirar a capacidade de escolha do consumidor.

Note-se ainda que não apenas a coleta direta de dados pessoais vem crescendo, mas os próprios usuários titulares das informações estão criando o hábito de oferecer, voluntariamente, seus dados para terceiros, normalmente grandes empresas, ao utilizar suas redes sociais e aplicativos¹⁹. Uma vez que esses dados são captados, eles proporcionam para os fornecedores de produtos e serviços um grande poder de publicidade baseada na perfilação de consumidores, relacionando cada pessoa a um determinado padrão de comportamento.

Assim, os dispositivos relacionados à IoT presentes do cotidiano do indivíduo poderiam interferir sobre sua vida e suas decisões, sem que ele sequer tenha conhecimento disso. Por exemplo, um dado obtido a partir da medição de batimentos cardíacos feita por um relógio inteligente, quando cruzado com outros sistemas, pode perfeitamente ocasionar o oferecimento de passagens aéreas para uma determinada localidade turística, se aproveitando do estado de estresse do consumidor (MARQUES; LEMOS, 2017, p. 17).

¹⁹ "Ao passo que a tecnologia domina atividades triviais do ser humano, nossa dependência às inovações aumenta e para que tenhamos acesso a uma gama de serviços essenciais, a abdicção da privacidade e dos dados pessoais parece inevitável. O usuário, portanto, torna-se refém do 'consentimento' para a aquisição de produtos e serviços cada vez mais essenciais à vida em sociedade" (BODIN DE MORAES; QUEIROZ, 2019, p. 122).

De fato, um acervo suficientemente amplo de dados viabiliza a criação de um perfil de consumo que pode ser utilizado para personalizar a venda de produtos e serviços de maneira a incrementar a experiência do indivíduo no mercado de consumo. Não obstante, é preciso estar constantemente atendo ao potencial lesivo dessa perfilização, uma vez que aumentar o controle sobre o consumidor, desconsiderando sua autonomia plena, pode ferir diretamente sua participação no processo decisório de compra e interferir na sua capacidade de autodeterminação em relação a seus dados pessoais (BODIN DE MORAES; TEFFÉ, 2017, p. 121). Por isso, fundamental a promoção do direito à autodeterminação informativa do consumidor de maneira a assegurar, por consequência, seu direito à liberdade de escolha sem discriminações ou perfis que aprisionam a figura do consumidor à produtos e serviços previamente selecionados a partir de dados obtidos, na maior parte das vezes, sem seu consentimento.

5. CONCLUSÕES

Em suma, a privacidade, a segurança e a liberdade de escolha do consumidor são especialmente colocadas em risco neste cenário complexo, o que demanda a construção de limites e parâmetros para a sua proteção diante do fenômeno da internet das coisas. Pois, nunca é demais lembrar, o fator principal de inovação do Código de Defesa do Consumidor é identificar o consumidor como um sujeito vulnerável na relação de consumo, fazendo assim jus a direitos especiais e à construção de um sistema de normas e princípios para protegê-lo e garantir a efetivação de seus direitos de caráter fundamental (BENJAMIN; MARQUES; BESSA, 2016, p. 77).

A hiperconectividade, por meio da IoT, revela que não somente as pessoas se comunicam com as máquinas, mas que elas também podem se comunicar. As informações e os dados coletados por meio de produtos aparentemente inofensivos e que oferecem grande comodidade aos consumidores descortina a face perversa da renúncia da privacidade nas atividades mais triviais do cotidiano e tornam a proteção dos dados pessoais uma falácia diante do “consentimento” necessário para o uso de aplicativos e objetos que fazem parte da vida hiperconectada, que exclui e discrimina aqueles que não participam das regras do jogo.

No perturbador romance “Máquinas como eu – E gente como você”, Ian McEwan antecipa os dilemas éticos da convivência entre humanos e andróides numa Londres de 1982. Num cenário que mistura ficção e realidade, o autor narra a relação entre humanos e não humanos numa Grã-

-Bretanha que recém perdeu a Guerra das Malvinas e o matemático Alan Turing vive sua homossexualidade plenamente, sendo suas contribuições essenciais para o avanço da tecnologia, que permitiram não só a disseminação da internet e dos *smartphones*, bem como a criação dos primeiros humanos sintéticos, com aparência e inteligência altamente fidedignas. Adão, o robô da história, era o “primeiro ser humano artificial verdadeiramente viável – com inteligência e aparência plausíveis, movimentos corretos e mudanças de expressão”. “Sua expectativa de vida era de funcional era de vinte anos. Tinha um corpo compacto, ombros quadrados, pele escura, vasta cabeleira preta penteada para trás; o rosto estreito e o nariz ligeiramente adunco sugeriam inteligência viva, combinada com o ar pensativo que provinha das pálpebras um pouco caídas”. Adão simbolizava o “mais sofisticado brinquedo, sonho de todos os tempos, o triunfo do humanismo – ou seu anjo exterminador” (MCEWAN, 2019, p. 10 e 12).

Em antecipação à um futuro que agora vivemos, Ian McEwan narra em sua história que os “programas de reconhecimento de voz, um milagre da década de 1950, tinham se tornado uma tarefa enfadonha, com populações inteiras sacrificando várias horas por dia aos solilóquios solitários. A interface entre cérebros e máquinas, fruto exótico do otimismo da década de 1960, não atraía mais o interesse nem mesmo de uma criança. Aquilo que fazia as pessoas formarem filas durante todo um fim de semana, seis meses depois era tão interessante quanto as meias que elas calçavam”. “O futuro estava sempre chegando”. O enredo de ficção científica, talvez por antevisão, revela que mesmo os avanços tecnológicos mais esperados acabam se tornando ociosos e ultrapassados. No entanto, enquanto a IoT, em interação ou não com a inteligência artificial, continuar a ser objeto de desejo de muitos consumidores, é papel do Direito proteger e promover a integral proteção da dignidade da pessoa humana. Num mundo de objetos conectados e robôs, torna-se mais do que urgente a afirmação da tutela do ser humano.

REFERÊNCIAS

- BAUMAN, Zygmunt. *A vida líquida*. Trad. de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar, 2007.
- BENJAMIN, Antônio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. *Manual de Direito do Consumidor*. 7. ed., rev., atual. e ampl., São Paulo: Revista dos Tribunais, 2016.
- BOBBIO, Norberto. *Da estrutura à função*: novos estudos de teoria do direito. Barueri: Manole, 2007.
- BODIN DE MORAES, Maria Celina; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *Cadernos Adenauer* (São Paulo), v. 3, pp. 1-17, 2019.

_____. LGPD: um novo regime de responsabilização civil dito "proativo". *Civilitica.com* – Revista Eletrônica de Direito Civil, editorial, a. 8, n. 3, 2019.

_____. TEFFÉ, Chiara Spadacini. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. *Revista Pensar*, Fortaleza, v. 22, n. 1, pp. 108-146, jan./abr., 2017.

BRASIL. *Tribunal de Justiça da Paraíba*. 6ª Juízo Especial Cível da comarca de João Pessoa/PB. Processo n.º 0816138-65.2019.8.15.2001, Juíza Priscilla Ribeiro Paulino, julg. 27 fev. 2020.

FURTADO, Gabriel; ALMEIDA, Vítor. A tutela do consumidor e o comércio eletrônico coletivo. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Orgs.). *Direito digital: direito privado e internet*. 3. ed., atual. rev. e ampl., Indaiatuba, SP: Editora Foco, 2020.

LEAL, Livia Teixeira. *Internet of toys: os brinquedos conectados à internet e o direito da criança e do adolescente*. *Revista Brasileira de Direito Civil* – RBDCCivil, Belo Horizonte, vol. 12, p. 175-187, abr./jun. 2017.

MAGRANI, Eduardo. *Entre dados e robôs: ética e privacidade na era da hiperconectividade*. 2. ed., Porto Alegre: Arquipélago Editorial, 2019.

_____. *A internet das coisas*. – Rio de Janeiro: FGV Editora, 2018.

MARTINS, Guilherme Magalhães. A defesa do consumidor como direito fundamental na ordem constitucional. In: MARTINS, Guilherme Magalhães (Org.). *Temas de Direito do Consumidor*. Rio de Janeiro: Lumen Juris, 2010.

MARQUES, Daniel; LEMOS, André. Sensibilidade performativa e privacidade na internet das coisas. 5º Simpósio Internacional LAVITS I *Vigilância, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias*. 29 y 30 de noviembre, 01 de diciembre de 2017. Santiago, Chile, p. 10-31. ISSN 2175-9596.

MCEWAN, Ian. *Máquinas como eu: a gente como vocês*. Trad. Jorio Dauster. São Paulo: Companhia das Letras, 2019.

MIRAGEM, Bruno. *A internet das coisas e os riscos do admirável mundo novo*. Disponível em: <<https://www.conjur.com.br/2017-mar-29/garantias-consumo-internet-coisas-riscos-admiravel-mundo>>. Acesso em: 07 mar. 2020.

MODENESI, Pedro. Comércio eletrônico e tutela do *ciberconsumidor*. *Revista Trimestral de Direito Civil*, ano 12, v. 48, out./dez. 2011.

MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IoT). In: REIA, Jessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo (Orgs.). *Horizonte presente: tecnologia e sociedade em debate*. Belo Horizonte: Casa do Direito, Fundação Getúlio Vargas, 2019.

_____. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*. Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

OLIVEIRA, Elisa Dias. *A proteção dos consumidores nos contratos celebrados através da internet*. Coimbra, Almedina, 2002.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Breves notas sobre a resignificação da privacidade. In: *Revista Brasileira de Direito Civil* – RBDCCivil, Belo Horizonte, v. 16, p. 35-56, abr./jun., 2018.

RICHARDS, Neil. *Intellectual Privacy: rethinking civil liberties in the digital age*. New York: Oxford University Press, 2015.

TEPEDINO, Gustavo; SCHREIBER, Anderson. A boa-fé objetiva no Código de Defesa do Consumidor e no Novo Código Civil. In: TEPEDINO, Gustavo (Coord.). *Obrigações: estudos na perspectiva civil-constitucional*. Rio de Janeiro: Renovar, 2005.

VERBIEST, Thibaut. *La protection juridique du cyber-consumateur*. Paris: Litec, 2002.

CAPÍTULO 13

RESPONSABILIDADE CIVIL EM SAÚDE NA SOCIEDADE 5.0: MELHOR INTERESSE DO PACIENTE E TECNOLOGIA NA "RESPONSABILIDADE CIVIL 5.0"

Maurílio Casas Maia

Doutor em Direito Constitucional e Teoria Política (UNIFOR). Mestre em Ciências Jurídicas (UFPB). Pós-graduado em "Direito Público: Constitucional e Administrativo" e em "Direitos Civil e Processual Civil" (CIESA). Professor da Faculdade de Direito da Universidade Federal do Amazonas (UFAM) e Defensor Público no Amazonas (DPAM). Endereço eletrônico: maurilioaia@gmail.com

1. INTRODUÇÃO

Diante do advento da *Sociedade da Informação* os fatores tecnológicos passaram a impactar – positiva ou negativamente –, cada vez mais a área da saúde e o paciente enquanto vulnerável da relação profissional. Há algum tempo, fala-se em *vulnerabilidade eletrônica* (MAIA, 2013-b) como elemento importante na *telemedicina* e ainda na *proteção da confiança médica informada do paciente* (MAIA, 2012; MAIA, 2013-a). Contudo, há mais a debater.

Com o advento da denominada "Sociedade 5.0", conforme nome dado pelo Governo Japonês, o uso da tecnologia em sociedade passa a ser cada vez mais explorado, falando-se em inteligência artificial, uso de robôs, telemedicina e *big data* no cenário da saúde mundial. Em tal contexto, com o avanço exponencial no uso de novas tecnologias o presente estudo pretende debater a incorporação das novas tecnologias ao "patrimônio jurídico" do paciente com vistas à tutela de seu melhor interesse. Para cumprir tal objetivo, será exposto o conceito de "Sociedade 5.0" para em seguida expor o vetor normativo da tutela do melhor interesse do paciente, assim também a proteção da sua confiança e expectativas legítimas do paciente para, por fim, trazer a lume o tema de seu acesso ao tratamento mais moderno e seus impactos na responsabilidade civil na área da saúde da sociedade 5.0. Longe de esgotar a temática, o presente estudo pretende estimular novas abordagens da Responsabilidade Civil na área da saúde à luz do cenário veloz da Sociedade tecnológica e da Informação em rede e dados.