2023

MANUAL DE DIREITO NA ERA DIGITAL

Coordenadora
Anna Carolina Pinho

CIVIL

AUTORES

- Ana Carolina Brochado Teixeira
- Ana Luisa Bastos Ramos
- Bruna Vilanova Machado
- Cíntia Burille
- Fernanda Las Casas
- Filipe Medon
- Gabriel Felipe Nami Inácio
- Guilherme Spillari Costa
- Ian Borba Rapozo
- José Eustáquio de Melo Júnior
- José Luiz de Moura Faleiros Júnior
- Lucas Morelli
- Paula Greco Bandeira
- Paula Mena Barreto
- Rodrigo Gugliara da Silva
- Sérgio Marcos Carvalho de Avila Negri
- Sílvio de Salvo Venosa
- Thiago Ferreira Cardoso Neves
- Victoria Paganella
- Vinicius Reis de Barros
- Vitor Almeida

EDITORA FOCO

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD

M294

Manual de Direito na Era Digital: Civil / Ana Carolina Brochado Teixeira... [et al.] ; coordenado por Anna Pinho. - Indaiatuba, SP : Editora Foco, 2023.

406 p. ; 16cm x 23cm. – (Coletânea de Manuais de Direito Digital)

Inclui bibliografia e índice.

ISBN: 978-65-5515-646-1

1. Direito. 2. Direito digital. 3. Tecnologia. I. Teixeira, Ana Carolina Brochado. II. Ramos, Ana Luísa Bastos. III. Machado, Bruna Vilanova. IV. Burille, Cintia. V. Casas, Fernanda Las. VI. Medon, Filipe. VII. Inácio, Gabriel Felipe Nami. IX. Costa, Guilherme Spillari. X. Rapozo, Ian Borba. XI. Melo Júnior, José Eustáquio de. XII. Faleiros Júnior, José Luiz de Moura. XIII. Morelli, Lucas. XIV. Bandeira, Paula Greco. XV. Barreto, Paula Mena. XVI. Silva, Rodrigo Gugliara da. XVII. Negri, Sergio Marcos Carvalho de Avila. XVIII. Venosa, Sílvio de Salvo. XIX. Neves, Thiago Ferreira Cardoso. XX. Paganella, Victoria. XXI. Barros, Vinicius Reis de. XXII. Almeida, Vitor. XXIII. Pinho, Anna. XXIV. Título. XXV. Série.

2022-3139 CDD 340.0285 CDU 34:004

Elaborado por Odilio Hilario Moreira Junior - CRB-8/9949

Índices para Catálogo Sistemático:

1. Direito digital 340.0285
2. Direito digital 34:004

(CIP) de acordo com ISBD

Teixeira... [et al.] ; coordenado por Anna

tal)

Carolina Brochado. II. Ramos, Ana Luisa
s, Fernanda Las. VI. Medon, Filipe. VII.
apozo, Ian Borba. XI. Melo Júnior, José
, Lucas. XIV. Bandeira, Paula Greco. XV.
Sergio Marcos Carvalho de Avila. XVIII.
Paganella, Victoria. XXI. Barros, Vinicius
V. Série.

CDD 340.0285 CDU 34:004

r - CRB-8/9949

ico:

MANUAL DE DIREITO NA ERA DIGITAL

Coordenadora
Anna Carolina Pinho

CIVIL

AUTORES

- Ana Carolina Brochado Teixeira
- Ana Luisa Bastos Ramos
- Bruna Vilanova Machado
- Cíntia Burille
- Fernanda Las Casas
- Filipe Medon
- Gabriel Felipe Nami Inácio
- Guilherme Spillari Costa
- Ian Borba Rapozo
- José Eustáquio de Melo Júnior
- José Luiz de Moura Faleiros Júnior
- Lucas Morelli
- Paula Greco Bandeira
- Paula Mena Barreto
- Rodrigo Gugliara da Silva
- Sérgio Marcos Carvalho de Avila Negri
- Sílvio de Salvo Venosa
- Thiago Ferreira Cardoso Neves
- Victoria Paganella
- Vinicius Reis de Barros
- Vitor Almeida

Coordenadora: Anna Carolina Pinho
Autores: Ana Carolina Brochado Teixeira, Ana Luisa Bastos Ramos, Bruna Vilanova Machado, Cintia Burille, Fernanda Las Casas, Filipe Medon, Gabriel Felipe Nami Inácio, Guilherme Spillari Costa, Ian Borba Rapozo, José Eustáquio de Melo Júnior, José Luiz de Moura Faleiros Júnior, Lucas Morelli, Paula Greco Bandeira, Paula Mena Barreto, Rodrigo Cugliara da Silva, Sergio Marcos Carvalho de Avila Negri, Sílvio de Salvo Venosa, Thiago Ferreira Cardoso Neves, Victoria Paganella, Vinicius Reis de Barros e Vitor Almeida
Diretor Acadêmico: Leonardo Pereira
Assistente Editorial: Paula Morishita
Revisora Sênior: Georgia Renata Dias
Revisora: Simone Dias
Diagramação: Ladislau Lima e Aparecida Lima
Impressão miolo e capa: DOCUPRINT

NOTAS DA EDITORA:

Atualizações e erratas: A presente obra é vendida como está, atualizada até a data do seu fechamento, informação que consta na página II do livro. Havendo a publicação de legislação de suma relevância, a editora, de forma discricionária, se empenhará em disponibilizar atualização futura.

Erratas: A Editora se compromete a disponibilizar no site www.editorafoco.com.br, na seção Atualizações, eventuais erratas por razões de erros técnicos ou de conteúdo. Solicitamos, outrossim, que o leitor faça a gentileza de colaborar com a perfeição da obra, comunicando eventual erro encontrado por meio de mensagem para contato@editorafoco.com.br. O acesso será disponibilizado durante a vigência da edição da obra.

Impresso no Brasil (10.2022) – Data de Fechamento (10.2022)

Editora Foco Jurídico Ltda.
Avenida Itororó, 348 – Sala 05 – Cidade Nova
CEP 13334-050 – Indaiatuba – SP
E-mail: contato@editorafoco.com.br
www.editorafoco.com.br

SUMÁRIO

SUCESSÕES E HERANÇA DIGITAL. REFLEXÕES

*Sílvio de Salvo Venosa**

Sumário: 1. Direito das sucessões. Noção; 1.1 A compreensão do direito das sucessões; 1.2 Noção de herança. Herança digital; 1.3 Direitos da personalidade; 1.4 Direitos da personalidade. Características e enumeração; 1.5 Do testamento analógico ao testamento digital – Referências

1. DIREITO DAS SUCESSÕES. NOÇÃO

Suceder é substituir, tomar o lugar de outrem ou de algo. No campo do Direito ocorre a substituição de uma pessoa por outra. Esse é o seu conceito amplo no campo jurídico. Assim, quando o conteúdo e o objeto de relação jurídica permanecem os mesmos, mas mudam seus titulares, há uma transmissão do direito ou uma sucessão. Dessa forma o comprador sucede o vendedor com relação ao objeto do negócio jurídico, o donatário sucede o doador e assim por diante.

Desse modo, sempre que uma pessoa, que pode ser natural ou jurídica, tomar o lugar de outra em uma relação jurídica, se está perante uma sucessão. A etimologia do vocábulo, *sub cedere*, possui exatamente esse sentido, qual seja, alguém toma o lugar de outrem.

Em direito a doutrina costuma fazer a sensível diferença entre a sucessão *inter vivos*, como por exemplo nos contratos, e a *causa mortis*, quando os direitos e obrigações de uma pessoa que falece transferem-se a seus herdeiros e legatários.

Contudo, convencionou-se na doutrina jurídica que a referência a *direito das sucessões* consiste no tratamento legal das substituições de titulares por causa de morte.

Assim como mais raramente ocorre na sucessão entre vivos, a sucessão por causa de morte transfere, em princípio, uma universalidade, que consiste na herança,

* Foi juiz no Estado de São Paulo por 25 anos. Aposentou-se como desembargador. Pós-graduado em Direito Civil. Lecionou Direito Civil em várias faculdades do Estado de São Paulo. Formado pela USP (Universidade de São Paulo) com pós-graduação em Direito Civil. Autor de inúmeras obras de Direito Civil, destacando a coleção completa em oito volumes, na 16ª edição (2016). A 17ª edição em 2017 será condensada para 7 volumes. Escreveu também obra de Introdução à Ciência do Direito, Código Civil Interpretado e Lei do Inquilinato Comentada, todas em sucessivas edições. Foi professor em diversas instituições de São Paulo. Consultor de vários escritórios jurídicos, parecerista e palestrante, em entidades no Brasil e no Exterior.

TECNOLOGIA, IMAGEM E PRIVACIDADE: CONVERGÊNCIAS À LUZ DA PROTEÇÃO DOS DADOS PESSOAIS NA SOCIEDADE TECNOLÓGICA

*Vitor Almeida**

*Ian Borba Rapozo***

Sumário: Introdução – 1. A proteção dos dados pessoais no direito brasileiro: informação e vigilância na era tecnológica – 2. Imagem e privacidade em risco: os exemplos da internet das coisas e do reconhecimento facial – 3. Convergências entre os direitos à imagem, privacidade e proteção dos dados pessoais – 5. Considerações finais – Referências.

INTRODUÇÃO

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 tecnológicos.[1] Em especial, os avanços tecnológicos

* 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.

** Mestrando em Direito e Inovação no Programa de Pós-Graduação *Stricto Sensu* da Faculdade de Direito da Universidade Federal de Juiz de Fora - UFJF. Pós-Graduando em Direito Processual pela Pontifícia Universidade Católica de Minas Gerais – PUC-MG. Graduado em Direito pela Universidade Federal Rural do Rio de Janeiro – UFRRJ. Pesquisador do grupo de pesquisa Argumentação, Direito e Inovação (UFJF/CNPq). Pesquisador do Núcleo de Pesquisa em Direitos Fundamentais, Relações Privadas e Políticas Públicas – NUREP (UFRRJ). Advogado.

1. Nesta linha, Caitlin Mulholland 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". MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IOT). In: REIA, Jessica; FRANCISCO, Pedro Augusto P.; BARROS, Marina; MAGRANI, Eduardo (Org.). *Horizonte presente*: tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito, Fundação Getúlio Vargas, 2019, p. 485.

desafiam a proteção dos direitos da personalidade, categoria que nasce no século passado e já reclamam uma reformulação de modo a compatibilizar a proteção integral da pessoa humana em sua dignidade no cenário de intensas modificações sociais provocadas pela tecnologia, notadamente com a popularização e, por conseguinte, facilitação dos recursos advindos com a internet.

A hiperconectividade 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 androides 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".[2]

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

2. MCEWAN, Ian. *Máquinas como eu*: a gente como vocês. Trad. Jorio Dauster. São Paulo: Companhia das Letras, 2019, p. 10 e 12.

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.

Após breve contextualização, pretende-se, com o presente trabalho, apresentar os contornos conceituais do direito à imagem e à privacidade na era tecnológica, bem como explorar alguns desafios que a evolução tecnológica tem o potencial de apresentar, quando analisada a partir da lógica constitucional de tutela dos direitos fundamentais, notadamente a partir da proteção dos dados pessoais. Em um cenário no qual a imagem da pessoa humana é captada e divulgada facilmente e as informações transitam para além dos domínios de cada indivíduo é indispensável refletir sobre a tutela da imagem e da privacidade alinhavada com a garantia constitucional de proteção dos dados pessoais.[3]

1. A PROTEÇÃO DOS DADOS PESSOAIS NO DIREITO BRASILEIRO: INFORMAÇÃO E VIGILÂNCIA NA ERA TECNOLÓGICA

Promulgada em 14 de agosto de 2018, a Lei 13.709 de 2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais, 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.

Reafirmando seu espírito protetivo, 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 europeia na qual foi inspirada,[4] a LGPD traz em seu texto as definições que lhe são essenciais e os princípios que norteiam sua aplicação. Ainda em seu art. 2º, inciso IV, a lei assegura expressamente que a proteção de dados tem como um de seus fundamentos a inviolabilidade da intimidade, da honra e da imagem.

Neste sentido, 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

3. "Art. 5º. [...] LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". (Incluído pela Emenda Constitucional 115, de 2022).
4. 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.

dados de maneira clara e explicita, 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.[5] Igualmente importante para a tutela dos direitos fundamentais em questão 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.

Pode-se afirmar, de fato, que vivemos hoje o momento mais expoente da sociedade da informação, o Estado dá indícios de que sua atuação será no sentido de tutelas o tema com a amplitude necessária. Não obstante, não é a primeira vez que o tema é abordado pela academia, de forma que a cultura de informação e vigilância, ainda que sob outras nomenclaturas, foi objeto de estudo de diversos filósofos desde o século XVIII.

Jeremy Bentham, em 1785, concebia a ideia do que chamou de "dispositivo", em sua obra *O Panóptico*, que consistia num edifício circular, com celas separadas em cada andar, até o topo, com uma torre de vigilância ao centro. Um espaço vazio entre a torre e o edifício, somado ao jogo de luzes e aberturas adequado, tornava possível o rompimento do binômio ver-ser visto, de forma que apenas os vigias da torre teriam a possibilidade de exercer vigilância sobre os presos, que, sem conseguir enxergar o interior da torre, jamais saberiam se estariam de fato sendo vigiados naquele momento, criando a ideia de vigilância constante.[6]

O Panóptico não foi originalmente pensado para ser uma prisão, mas é, na verdade, um princípio básico de construção a ser aplicado nas situações em que haja o que Jeremy Bentham chama de habitantes involuntários, reticentes ou constrangidos, como são os detentos de uma prisão, mas também em outros casos, como escolas ou asilos.[7]

Séculos mais tarde, ao se dedicar ao estudo das instituições disciplinares da sociedade moderna, Michael Foucault retoma o panóptico de Jeremy Bentham e aponta que um de seus efeitos mais relevantes é exatamente o de induzir no detento um estado permanente de visibilidade a partir do qual é assegurado o funcionamento automático do poder. O filósofo francês esclarece que, para se atingir a eficiência de tal efeito, é necessário que o panóptico seja, ao mesmo tempo,

5. MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral do Proteção de Dados (Lei 13.709/18). R. *Dir. Gar. Fund.*, v. 19, n. 3, p. 163-165, Vitória, set./dez. 2018.
6. BENTHAM, Jeremy. *O Panóptico*. 2. ed. Belo Horizonte: Autêntica Editora, 2008, p. 89.
7. Idem, ibidem, p. 89.

a utilização para qualquer outro
pio da não discriminação garante
riminatórios ilícitos ou abusivos,
os em normas expressas quanto
lmente importante para a tutela
ípio do livre acesso, estabelecido
uestão garante ao titular do dado
período do tratamento de seus

e o momento mais expoente da
que sua atuação será no sentido
ão obstante, não é a primeira vez
a que a cultura de informação e
foi objeto de estudo de diversos

do que chamou de "dispositivo",
cio circular, com celas separadas
ncia ao centro. Um espaço vazio
e aberturas adequado, tornava
de forma que apenas os vigias
ncia sobre os presos, que, sem
eriam se estariam de fato sendo
gilância constante.[6]

o para ser uma prisão, mas é,
ser aplicado nas situações em
antes involuntários, reticentes
risão, mas também em outros

as instituições disciplinares da
panóptico de Jeremy Bentham
é exatamente o de induzir no
partir do qual é assegurado o
francês esclarece que, para se
nóptico seja, ao mesmo tempo,

de direitos fundamentais: uma análise à
Gar. Fund., v. 19, n. 3, p. 163-165, Vitória,

ntica Editora, 2008, p. 89.

excessivo e muito pouco. O excesso se dá a partir da imperatividade de que aquele que está sendo vigiado se sinta de fato observado a todo o tempo, ainda que não o esteja sendo realmente. De outro lado, o panóptico é muito pouco por não necessitar realmente da vigilância constante e ininterrupta, bastando a sensação de que assim seja. Para o autor, quanto maior é a quantidade de informações que se tem sobre um indivíduo, maior é a possibilidade de se controlar o seu comportamento.[8]

Tal noção de constância se assemelha à construção do conceito de *Big Other* feita por Shoshana Zuboff, para quem este fenômeno pode ser descrito como o nascimento de uma arquitetura universal inédita, cuja existência se encontra em algum ponto entre o natural e o divino. O *Big Other*, em outros termos, seria um novo regime de fatos independentes e independentemente controlados, criado a partir da análise e tratamento de *Big Data* na sociedade contemporânea, de forma a jogar por terra a necessidade, por exemplo, dos contratos e das diversas formas de governança, ao passo que haveria uma espécie de consciência autônoma, que se originou e se retroalimenta dos mais diversos dados gerados pelos indivíduos.[9]

Entenda-se isso no sentido que os dados, uma vez captados, alimentam um regime que não depende mais da atuação humana direta pra funcionar porque já conta com a fonte (os dados) e com a forma de operacionalizá-los – Inteligência Artificial e Machine learning, por exemplo.

Em 1999, ao tratar da sociedade em rede, Manuel Castells explica que tais redes seriam, na verdade, como um conjunto de nós interligados e que em cada nó se encontraria o ponto de encontro dos diversos fluxos de informação, em um cenário cujo funcionamento da estrutura social seria dependente das tecnologias digitais de comunicação e informação oriundas, basicamente, da internet. Assim, seria impossível pensar as interações digitais como algo alheio ao mundo real, construindo a noção de que a internet, enquanto espaço de fluxos, não seria uma representação da sociedade, mas sim a própria sociedade.[10]

Com olhar contemporâneo, Zygmun Bauman afirma que a vigilância, no panorama atual, se insinua em estado líquido. O filósofo apresenta a denominação de modernidade líquida para um constante e fluido estado de mudança, que não se conserva em sua forma por muito tempo, reforçando o caráter frágil das relações humanas e sociais. O autor correlaciona as ideias de segurança e discipli-

8. FOUCAULT, Michael. *Vigiar e punir*: o nascimento da prisão. Trad. Raquel Ramalhete, 42. ed. Petrópolis, RJ: Vozes, 2014, p. 195.
9. ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et al (Org.). *Tecnopolíticas da vigilância*: perspectivas da margem. Trad. Heloísa Cardoso Mourão et al. São Paulo: Boitempo, 2018, pp. 17-68; 42-44.
10. SCHNEIDER, Camila Berlim; MIRANDA, Pedro Fauth Manhães. Vigilância e segurança pública: preconceitos e segregação social ampliados pela suposta neutralidade digital. *Emancipação*. v. 20, p. 06, Ponta Grossa, 2020.

na, afirmando que, hodiernamente, a noção de proteção seria concretizada pela implementação de tecnologias de vigilância no cotidiano. Esta concepção seria usualmente aplicada a categorias de pessoas, analisando, a partir do universo digital, quem seria indesejado e quem seria bem-vindo no meio social, modelo comumente encontrado em sistemas de controle de fronteiras, por exemplo.[11]

Assim como no meio filosófico, o desenvolvimento das tecnologias e da sociedade de informação é um grande objeto de estudo e dedicação da ciência jurídica, quer seja a partir da Lei n. 12.965 – o Marco Civil da Internet, promulgada em 2014, quer seja sob a ótica atual da já referida Lei n. 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD)

Fato é que, qualquer que seja a concepção filosófica ou sociológica adotada pata tratar do tema, o cenário de vigilância que se impõe no presente e do qual não há mais como sair, cria uma longa fila de desafios que devem ser enfrentados.

2. IMAGEM E PRIVACIDADE EM RISCO: OS EXEMPLOS DA INTERNET DAS COISAS E DO RECONHECIMENTO FACIAL

Para adentras às considerações necessárias ao estudo da privacidade e da imagem no contexto sob análise, propõe-se tomar como ponto de partida, ainda que de forma superficial, alguns aspectos da Internet das Coisas. 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).[12]

Qualquer objeto imaginável pode, teoricamente, ser inserido 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]

11. Idem, ibidem, p. 5.
12. LEMOS, André; MARQUES, Daniel. *Simposio Internacional LAVITS*, Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias. 29 y 30 de noviembre, 01 de diciembre de 2017. Santiago, Chile, p. 10-31. p. 11.
13. Disponível em: https://www.proof.com.br/blog/internet-das-coisas/. Acesso em: 07 mar. 2020.

e proteção seria concretizada pela
o cotidiano. Esta concepção seria
analisando, a partir do universo
em-vindo no meio social, modelo
ole de fronteiras, por exemplo.[11]

volvimento das tecnologias e da
de estudo e dedicação da ciência
Marco Civil da Internet, promul-
referida Lei n. 13.709, a Lei Geral

filosófica ou sociológica adotada
e se impõe no presente e do qual
afios que devem ser enfrentados.

S EXEMPLOS DA INTERNET
FACIAL

s ao estudo da privacidade e da
ar como ponto de partida, ainda
net das Coisas. O termo "Internet
radução em inglês IoT – *Internet*
dade de objetos cotidianos em
strumentalizados com sensores
izadas a partir de procedimen-
ocessamento de dados em uma

nte, ser inserido no universo da
apazes de se conectar à internet.
e número de vagas disponíveis
ão ou um aviso espontâneo no
o trânsito na cidade e o tempo
á estão presentes no cotidiano
das a partir das agências, por

LAVITS, Vigilancia, Democracia y Pri-
9 y 30 de noviembre, 01 de diciembre de

coisas/. Acesso em: 07 mar. 2020.

O que se vislumbrava 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 indivíduos 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 das pessoas e impõe "um fluxo contínuo de informações e uma massiva produção de dados.[14] 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 informações cada vez mais automatizado".[15]

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.[16]

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*,[17] 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.[18] Um ursinho de pelúcia ou uma boneca podem ser

14. Segundo Eduardo Magrani (Op. cit., 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".
15. Idem, ibidem, p. 19.
16. Disponível em: https://www.samsung.com/br/info/privacy/smarttv/. Acesso em: 30 set. 2020.
17. 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.
18. LEAL, Livia Teixeira. Internet *of toys*: os brinquedos conectados à internet e o direito da criança e do adolescente. *Revista Brasileira de Direito Civil* – RBDCivil, v. 12, p. 178-181, Belo Horizonte, abr./jun. 2017.

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*.

Há, ainda, o exemplo dos dados derivados de transações econômicas mediadas por computador, que representam uma parcela significativa do *big data* existente no mundo hoje. No entanto, como esclarece Shoshana Zuboff,[19] há várias outras fontes de grande importância e, dentre estas, encontram-se as câmeras de segurança públicas e privadas, considerando ainda qualquer espécie de aparelhos com capacidade de gravação, desde *smartphones* até satélites de *Google Street View*.

Tamanha é a ingerência das citadas câmeras de monitoramento na sociedade que já foi forjado o conceito de uma sociedade construída com fundamento no hábito da vigilância, o que Jonathan Finn denomina "ver vigilantemente". Segundo o autor,[20] a vigilância de vídeo vem se apresentando cada vez mais como conceito, tema de anúncios, expressões de arte e formas de entretenimento e aponta que a razão para isso não é somente um reflexo do acentuado aumento da prática de vigilância no meio social, mas sim na sua manifestação como um hábito social. Enquanto a vigilância inicialmente nos remete à força policial e ao monitoramento de grupos e indivíduos por parte do Estado, atualmente é considerada em um contexto contemporâneo que aponta para um elemento verdadeiramente constitutivo da vida social. Não se trata apenas de um aparato material ou técnico, mas de um fenômeno que se tornou um verdadeiro estilo de vida, uma forma de ver, compreender e se envolver com o mundo ao nosso redor.

Para construir o conceito, Jonathan Finn parte de um tríplice pilar que indicam as características principais da vigilância contemporânea: (*i*) como

19. ZUBOFF, Shoshana. Op. cit., p. 27-28.
20. FINN, Jonathan. Seeing Surveillantly: Surveillance as Social Practice. In: DOYLE, Aaron; LIPPERT, Randy and LYON, David (Ed.). *Eyes Everywhere:* The Global Growth of Camera Surveillance. New York: Routledge, 2012, p. 67.

conceito estético, (*ii*) como retórica e (*iii*) como participação na vida pública. Em primeiro lugar, a vigilância como conceito estético é uma característica que deriva do exacerbado quantitativo de imagens criativas projetadas com finalidade comercial, objetivando seu uso como conteúdo visual em uma diversidade de atos comunicativos. É o caso, por exemplo, de grandes bancos de imagens, genéricas e variadas, disponíveis para a compra do usuário para uso em publicações de publicidade na internet, exibição na televisão ou o que mais suprir seu interesse comercial. O ponto central desta característica da vigilância é que os diversos impactos e influências culturais que estes bancos de imagem podem gerar passam imperceptíveis, dando espaço para a percepção destas imagens como uma parte banal da vida cotidiana. As imagens em si são relativamente desprovidas de significado, mas quando somadas a textos, cor e outras formas de formatação, ganham significado específico, normalmente direcionado à disseminação de uma mensagem comercial.[21]

Subsequentemente, há a característica da vigilância como instrumento de retórica. Em contribuição direta ao processo de naturalização do videomonitoramento na sociedade, esta característica faz referência à transformação da vigilância de um fenômeno para um mecanismo de comunicação do entretenimento. Diversos foram os filmes que trataram do tema, mas um exemplo ainda mais notável é o crescimento e sucesso dos programas de *reality show*. *True Beauty*, *The Real World*, *Temptation Island*, *Big Brother*, Casa dos Artistas, A Fazenda, De Férias com o Ex, No Limite, são alguns exemplos de midiatização da vigilância, com o uso do videomonitoramento do cotidiano como linguagem de comunicação, bem como objeto central dos programas. Nesta mesma linha, os meios de comunicação de massa se utilizam da vigilância como instrumento narrativo, atribuindo um peso específico e elevado para as imagens obtidas por câmeras de vigilância, como se seu olhar supostamente automatizado, anônimo e onipresente representasse uma visão neutra e objetiva sobre a verdade dos fatos comunicados.[22]

Finalmente, a característica da vigilância como participação na vida pública vem aumentando exponencialmente ao longo do tempo. No passado, para que fosse possível fazer uma filmagem ou mesmo uma captura de imagem estática era preciso um grande aparato técnico, processos químicos e muito tempo de espera. Ao contrário, atualmente, com câmeras cada vez mais potentes, menores e mais leves, com mais capacidade de memória e resolução da imagem, não é preciso fazer qualquer esforço para que se consiga um registro de vídeo de um fato. Cada agência bancária ou loja conta com câmeras de segurança, assim como rodoviárias, aeroportos, praças e vias públicas e até mesmo o mais simples *smartphone*

21. FINN, Jonathan. Op. cit., p. 72-73.
22. Idem, ibidem, p. 74-76.

vendido hoje em dia conta com ao menos uma câmera fotográfica e de vídeo. A título de ilustração, em 2021, o Brasil registrou o uso de mais de um – 1,6 mais especificamente – *smartphone* por habitante. Mais especificamente, o país conta hoje com 440 milhões de dispositivos digitais e dentre eles, 242 milhões de aparelhos celulares inteligentes ativos.[23]

Vídeos amadores de fatos ocorridos na sociedade não são raros e, somados a dados como os expostos acima, é plausível afirmar a que a vigilância não deve mais ser compreendida somente como uma tecnologia empregada pelos Estados a fim de controlar populações perigosas ou como uma ferramenta da qual as grandes corporações lançam mão para atender aos interesses do capital global. De fato, esses fenômenos acontecem e devem ser objeto de severa investigação e resposta jurídica, mas, combinada com essas formas mais tradicionais, o estado atual da vigilância por câmeras de vídeo na sociedade aponta para uma mudança geral na existência, função e entendimento do monitoramento na vida pública.[24]

É relevante notar, inclusive, que, em várias cidades pelo mundo as políticas de videomonitoramento vêm sendo questionadas e, às vezes, abandonadas, ainda que parcialmente. Em junho de 2020, a empresa IBM anunciou que deixaria de realizar pesquisas, bem como deixaria de desenvolver e oferecer tecnologias de reconhecimento facial, em razão das patentes violações a direitos humanos provenientes do emprego dessas tecnologias.[25] Na mesma linha, três cidades do estado da Califórnia e a cidade de São Francisco, nos Estados Unidos, baniram o uso desse tipo de tecnologia para fins de vigilância.[26]

3. CONVERGÊNCIAS ENTRE OS DIREITOS À IMAGEM, PRIVACIDADE E PROTEÇÃO DOS DADOS PESSOAIS

A imagem recebeu proteção constitucional no art. 5º, inciso X, ao lado da intimidade, vida privada e honra. O próprio comando da Constituição da República de 1988 concedeu autonomia àquele direito, determinando sua inviolabilidade e assegurando a reparação em sede material e moral nas hipóteses de violação. É certo que esta inviolabilidade não é absoluta quer em virtude do confronto com a liberda-

23. Dados obtidos a partir da pesquisa anual do uso de TI realizada em 2021 pela Fundação Getúlio Vargas. Disponível em: https://eaesp.fgv.br/producao-intelectual/pesquisa-anual-uso-ti. Acesso em: 1º jun. 2021.
24. FINN, Jonathan. Op. cit., p. 78.
25. Disponível em: https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software. Acesso em: 1º jun. 2021.
26. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/05/centro-da-revolucao-tecnologica-sao-francisco-bane-o-uso-de-reconhecimento-facial-pelo-governo.html. Acesso em: 1º jun. 2021.

câmera fotográfica e de vídeo. A
o uso de mais de um – 1,6 mais
ais especificamente, o país conta
dentre eles, 242 milhões de apa-

iedade não são raros e, somados
afirmar a que a vigilância não
na tecnologia empregada pelos
osas ou como uma ferramenta
para atender aos interesses do
ecem e devem ser objeto de se-
binada com essas formas mais
câmeras de vídeo na sociedade
ia, função e entendimento do

cidades pelo mundo as políticas
as e, às vezes, abandonadas, ain-
esa IBM anunciou que deixaria
envolver e oferecer tecnologias
s violações a direitos humanos
Na mesma linha, três cidades do
nos Estados Unidos, baniram o
ia.[26]

À IMAGEM, PRIVACIDADE E

o art. 5º, inciso X, ao lado da in-
lo da Constituição da República
rminando sua inviolabilidade e
nas hipóteses de violação. É certo
ude do confronto com a liberda-

da em 2021 pela Fundação Getúlio Vargas.
esquisa-anual-uso-ti. Acesso em: 1º jun.

683/ibm-no-longer-general-purpose-fa-

ia/noticia/2019/05/centro-da-revolucao-
-facial-pelo-governo.html. Acesso em: 1º

de de expressão[27] quer em oposição ao direito à informação,[28] eventos nos quais se impõe a necessária ponderação, com o fito de que se determine o "fiel da balança".

Em sede infraconstitucional, o Código Civil de 2002 foi desastroso ao disciplinar o direito à imagem em seu art. 20. Ao perder a oportunidade de propor critérios razoáveis para os conflitos entre o direito à imagem e a liberdade de expressão e de informação, pecou, gravemente, o legislador ordinário, preterindo uma cláusula geral – mais adequada às hipóteses conflitivas em questão – a um enunciado rígido, fechado e demasiadamente restritivo. Não obstante, o aludido dispositivo não foi capaz de representar legitimamente os interesses constitucionalmente albergados de modo a refletir uma norma segura para os operadores do direito e condizente com a sociedade atual tecnológica.

Indispensável, portanto, reler o dispositivo infraconstitucional à luz da centralidade e supremacia da Constituição, fornecendo critérios hábeis e seguros à composição dos conflitos imanentes ao domínio da proteção da imagem da pessoa, eis que encartado como um dos mais importantes direitos da personalidade – tanto é que merecedor de um dentre os poucos dispositivos reservados à categoria no Código Civil, bem como constitui um aspecto essencial da proteção da pessoa humana.

Por sua vez, o direito à privacidade está previsto na Constituição Federal de 1988, em seu art. 5º, inciso X, que dispõe que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. Por sua vez, o Código Civil de 2002, em seu art. 21, estabelece que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

O lacônico dispositivo dispensado ao direito à privacidade no Código Civil foi objeto da Ação Direita de Inconstitucionalidade n. 4815 que versava sobre a questão das biografias não autorizadas, de relatoria da Min. Carmem Lúcia, que "julgou procedente o pedido formulado na ação direta para dar interpretação conforme à Constituição aos artigos 20 e 21 do Código Civil, sem redução de texto, para, em consonância com os direitos fundamentais à liberdade de pensamento e de sua expressão, de criação artística, produção científica, declarar inexigível o consentimento de pessoa biografada relativamente a obras biográficas literárias ou audiovisuais, sendo por igual desnecessária autorização de pessoas retratadas como coadjuvantes (ou de seus familiares, em caso de pessoas falecidas)".

27. Art. 5º [...] IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença.
28. Art. 5º [...] XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional.

De fato, o solitário dispositivo não corresponda a atual dinâmica da privacidade em tempos atuais, que deixa de ser exclusivamente um direito a ficar sozinho e não ter seu microcosmo domiciliar violado para atualmente alcançar o direito à autodeterminação informativa e à proteção dos dados pessoais. Os dados pessoais hoje são facilmente obtidos com a mera navegação na internet ou o uso dos aplicativos, cada vez mais comuns no cotidiano dos usuários de smartphones.

Por isso, durante muito tempo se reclamou por uma tutela mais enérgica da privacidade diante das novas tecnologias, especialmente com o advento e, após, a democratização da internet. Após longa espera, finalmente foi promulgada a Lei 12.965/2014, conhecida como Marco Civil da Internet (MCI), que dispõe sobre os princípios, garantias, direitos e deveres para o uso da internet no Brasil. Com o Marco Civil da Internet, o legislador se posicionou claramente pela necessidade de regulamentação da internet, mas garantindo a liberdade de expressão, a neutralidade da rede, a privacidade e a criação de novos modelos de negócio, nos termos do art. 3º da Lei.

Resta nítido o balanceamento dos valores constitucionais realizado pelo legislador, 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.

O art. 3º do Marco Civil da Internet estabelece, portanto, que a internet brasileira se encontra alicerçada em um tripé axiológico formado pelos princípios da neutralidade da rede, da privacidade e da liberdade de expressão, que estão ligados entre si. Enquanto a neutralidade da rede reforça a liberdade de expressão, a privacidade representa seu limite. O direito à privacidade foi expressamente assegurado pelo MCI nos arts. 3º, II, 8º e 11. Em outras passagens, o MCI assegurou a proteção aos dados pessoais, a inviolabilidade da intimidade e da vida privada e a inviolabilidade e sigilo do fluxo das comunicações pela Internet.

A Lei n. 12.965/2014 estabelece, ainda, em seu art. 7º uma série de direitos dos usuários de internet, fortalecendo a proteção daqueles que utilizam a internet e garantindo o exercício dos direitos fundamentais na rede. Tal dispositivo se preocupou precipuamente com a proteção da privacidade do usuário e o direito à informação em relação à coleta, armazenamento e uso dos dados pessoais dos usuários.

Como já visto, a Lei n. 13.709, promulgada em 14 de agosto de 2018, dispõe sobre a proteção de dados pessoais e altera a Lei 12.965/14 (Marco Civil da Internet), consolidando-se assim como a Lei Geral de Proteção de Dados brasileira (LGPD). Nos termos do seu art. 1º, a LGPD "dispõe sobre o tratamento de dados

pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". Estabelece ainda no seu art. 2º os fundamentos da disciplina da proteção dos dados pessoais, realçando a importância do respeito à privacidade.

Em seu art. 2º, inciso IV, a Lei de Proteção de Dados Pessoais assegura expressamente que a proteção de dados tem como um de seus fundamentos a inviolabilidade da intimidade, da honra e da imagem. Em setembro de 2020, a entidade Coalizão Direitos na Rede emitiu uma nota assinada por 15 entidades[29] a respeito de um projeto de videomonitoramento a ser implantado no estado do Ceará, na qual afirma que a imagem é um dado biométrico e, portanto, dado sensível aos olhos da LGPD, o que implica em uma maior atenção em seu tratamento. A nota aponta ainda que a imagem de um indivíduo é um dado único e, diferentemente de senhas ou números de telefones, as características físicas da pessoa não são alteradas facilmente.

Com a expansão acelerada e naturalização do monitoramento por vídeo na sociedade contemporânea, não é de causar espanto que a quantidade de imagens capturadas no cotidiano seja igualmente grandiosa. Surgem, assim, questões de várias ordens que são merecedoras de atenção e estudo para melhor compreensão e, dentre elas, está o tratamento dispensado a essas imagens facilmente capturadas quando um indivíduo se dirige à padaria ou mesmo quando entra no elevador de seu condomínio, o que envolve não apenas sua imagem, mas seu direito à privacidade.

A concepção mais contemporânea do direito à imagem é aquela que a relaciona não mais apenas aos aspectos físicos da pessoa retratada, mas também àqueles que são relativos ao seu comportamento no âmbito social, tendo em vista que por mais difícil que seja a definição de alguns elementos como humor ou jeito, eles são essenciais para a identificação de uma pessoa e, portanto, legalmente protegidos. É dizer, qualquer expressão, representação ou identificação da personalidade de um indivíduo é imagem para os fins legais, de onde surge inclusive os desdobramentos de imagem atributo da pessoa, ou seja, atributos positivos ou negativos de uma pessoa apresentados a sociedade e que permitem sua identificação.[30]

Vale mencionar ainda que, como manifestação da dignidade humana e com *status* constitucional, o direito à imagem impõe sempre que a eventual autorização para seu uso e divulgação seja interpretada de forma restritiva – assemelhando-se

29. Disponível em: https://direitosnarede.org.br/2020/09/04/nota-sobre-projeto-de-videomonitoramento-no-ceara-e-em-defesa-de-maior-debate-publico/. Acesso em: 20 mar. 2021.
30. MEDON, Filipe. O direito à imagem na era das *deepfakes*. *Revista Brasileira de Direito Civil – RBDCivil*. v. 27, p. 258, Belo Horizonte, jan./mar. 2021.

ao tratamento dos dados pessoas, de forma geral. E, mais ainda, é imperioso que se tenha em mente que toda a proteção dispensada ao direito à imagem é imposta a todo momento, ou seja, em sua autorização, em sua divulgação, mas também em sua origem: o momento da captura da imagem.[31]

O conceito de privacidade, de igual maneira, evoluiu com o passar dos anos e, atualmente, tratada na Constituição Federal, como um direito fundamental, em seu art. 5º, inciso X e no art. 21 do Código Civil de 2002, 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.[32]

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 europeia 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.[33]

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,[34] 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

31. Idem, ibidem, p. 255.
32. MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: ama análise à luz da Lei Geral do Proteção de Dados (Lei 13.709/18). *R. Dir. Gar. Fund.*, v. 19, n. 3, p. 172, Vitória, set./dez. 2018.
33. PEIXOTO, Erick Lucena Campos, EHRARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 16, p. 43, abr./jun. 2018.
34. MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: ama análise à luz da Lei Geral do Proteção de Dados (Lei 13.709/18). *R. Dir. Gar. Fund.*, v. 19, n. 3, p. 172-173, Vitória, set./dez. 2018.

l. E, mais ainda, é imperioso que
da ao direito à imagem é imposta
em sua divulgação, mas também
em.[31]

, evoluiu com o passar dos anos e,
o um direito fundamental, em seu
02, não está mais associada unica-
mbém as situações concernentes
controle de dados sensíveis pelo
ontemporâneo, que a privacidade
próprias informações.[32]

privacidade encontra suas raízes
o, a concepção europeia aborda
-a com características de direito
das para garantir a proteção de
que a privacidade mostrou seu
eterminação informativa, o que
ade hodierna, em que a própria

le como funciona a dinâmica do
r que o download de aplicativos
gratuito, como aparenta ser. Os
as mais valiosas atualmente e,
líticas de uso desses aplicativos,
m disponíveis para o acesso do

Mulholland,[34] há três concepções
o direito de ser deixado só; (b) o
los pessoais (autodeterminação
olhas de caráter pessoal. No pri-
, quando o controle de acesso diz

ela de direitos fundamentais: ama análise
Dir. Gar. Fund., v. 19, n. 3, p. 172, Vitória,

arcos. Breves notas sobre a ressignificação
, Belo Horizonte, v. 16, p. 43, abr./jun. 2018.
la de direitos fundamentais: ama análise à
r. Gar. Fund., v. 19, n. 3, p. 172-173, Vitória,

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.[35]

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 dos indivíduos acabam sendo convertidos em dados sensíveis, cuja proteção, nestes casos, é imprescindível para a integral tutela dos direitos dos usuários.[36] 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 requisita

A lei estabelece, como regra geral, que qualquer pessoa que pretenda realizar alguma forma de tratamento de dados pessoais somente poderá fazê-lo a partir de uma base legal sólida, condizente com a espírito protetivo da legislação. Essas bases legais podem ser localizadas no art. 7º da LGPD, no que diz respeito aos dados pessoais e, relativamente aos dados pessoais sensíveis,[37] especialmente, em seu art. 11. Apesar do entendimento de que as hipóteses elencadas em ambos os artigos são taxativas, há ainda a existência de algumas hipóteses "coringas", como o caso, por exemplo, do tratamento de dados baseado no legítimo interesse do controlador.[38]

O art. 4º elenca os casos de exclusão, em que o tratamento de dados pessoais não será regido pelos preceitos da LGPD. Dentre tais previsões há, no inciso

35. PEIXOTO, Erick Lucena Campos, EHRARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil – RBDCivil*, v. 16, p. 48, Belo Horizonte, abr./jun. 2018.
36. Idem, ibidem, p. 51.
37. O Art. 5º da Lei Geral de Proteção de Dados Pessoais define de forma objetiva o que a norma em questão entende como dados pessoais e dados pessoais sensíveis, respectivamente, em seus incisos I e II: I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II – dado pessoal sensível: 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.
38. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. In: *Civilistica.com*. a. 9, n. 1, p. 4. Rio de Janeiro, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 11 jan. 2021.

III, alínea "a", a exclusão de aplicação da LGPD quando o tratamento de dados pessoais for direcionado para fins exclusivos de segurança pública, hipótese de especial interesse para o presente estudo, tendo em vista que é no argumento de garantia da segurança pública que muitas vezes se fundamentam as aplicações de vigilância por câmeras de vídeo nos espaços públicos. Há, ainda, no parágrafo primeiro do referido artigo a previsão de que o tratamento de dados pessoais com base nas hipóteses de exclusão do inciso III será regido por legislação especial criada para este fim. Por ato do Presidente da Câmara dos Deputados assinado em 26 de novembro de 2019 instituiu-se a Comissão de Juristas Sobre Segurança Pública, com o objetivo de elaborar a legislação referida.[39]

Apesar das previsões taxativas e "coringas" da LGPD sobre as bases legais para tratamento de dados pessoais, a compreensão geral é de que a interpretação do consentimento, sob a ótica da LGPD, deve sempre ser restritiva, vedado o seu tratamento para qualquer outra finalidade diversa daquela para a qual o titular dos dados consentiu.[40] Percebe-se, então, que o tratamento de dados lastreado no legítimo interesse do controlador é um ponto sensível, por ser hipótese bastante flexível, de forma que "quanto mais invasivo, inesperado ou genérico foi o tratamento, menor será a probabilidade de que seja reconhecido o legítimo interesse".[41] Insta mencionar que a própria lei, quando menciona a base legal do legítimo interesse, cria também o limite para o tratamento de dados a partir deste fundamento em casos nos quais devem prevalecer direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Nesse sentido, apesar de ser um fenômeno intrínseco à vida em comunidade, o que parece ser uma simples captação de imagens do cotidiano pode se desdobrar em práticas potencialmente lesivas. Uma das grandes preocupações levantadas, por exemplo, é a possibilidade de reconhecimento facial por Inteligência Artificial como forma de controle e a confirmação visual de eventos. Com o crescente desenvolvimento tecnológico e a possibilidade de reconhecimento de pessoas a partir de cruzamento de informações com bancos de dados, a imagem capturada se revela como uma robusta fonte das mais diversas

39. "Instituí Comissão de Juristas destinada a elaborar anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito de segurança pública, investigações penais e repressão de infrações penais, conforme o disposto no artigo 4º, inciso III, alíneas 'a' e 'd' da Lei 13.709, de 14 de agosto de 2018". BRASIL. Câmara dos Deputados. Ato do Presidente de 26.11.2019. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/conheca-a-comissao/criacao-e-constituicao/ato-de-criacao. Acesso em: 02 jun. 2021. No mês de julho de 2020 realizou-se de forma remota o Seminário Internacional da Comissão de Juristas – Proteção de dados pessoais e investigação criminal. No entanto, até o momento, não houve apresentação de qualquer projeto de lei sobre o tema.
40. TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Op. cit., p. 6.
41. Idem, ibidem, p. 14.

informações sobre os indivíduos, o que desafia a atenção em sua interpretação de acordo com esta natureza.[42]

Originalmente, as técnicas de reconhecimento facial foram concebidas com a finalidade de tentar superar as capacidades – ou incapacidades – do cérebro humano no que diz respeito à memorização e processamento de milhares de faces pelas quais passa todos os dias. No entanto, atualmente, de forma bastante acentuada após os ataques terroristas de 11 de setembro de 2001, as tecnologias de reconhecimento facial vêm sendo empregadas por órgãos governamentais para regular o fluxo de pessoas a partir da identificação individual, novamente com fundamento na garantia da segurança pública.[43]

Há atuação semelhante no Brasil no que diz respeito à implantação de tecnologias de reconhecimento facial. Cita-se, exemplificativamente, a apresentação do programa "Rio+Seguro", na cidade do Rio de Janeiro, que se justificava na prevenção à desordem urbana e à criminalidade. A tecnologia apresentada era baseada em um *software* de reconhecimento facial com funcionamento por Inteligência Artificial que seria capaz de identificar suspeitos e foragidos do sistema de justiça e, assim, possibilitar sua apreensão.[44]

A expansão das tecnologias de reconhecimento facial mundo afora, em especial sob o manto da segurança pública, preocupa sobremaneira em razão do alto potencial lesivo aos direitos da personalidade, a exemplo do direito à imagem, bem como da infinidade de usos possíveis a partir da captura que pode distorcer seus fins e permitir práticas discriminatórias e, portanto, violadora de direitos fundamentais.

Nesse sentido, Danilo Doneda defende que a proteção dos dados pessoais é um direito fundamental, eis que ancorado na cláusula geral de dignidade da pessoa humana. Cabe esclarecer que, segundo lição do referido autor, o dado deve ser compreendido em um sentido mais primitivo, em estado bruto, uma espécie de informação em potencial, enquanto a própria informação faz referência a algo além do dado puro, é o dado já tratado, alcançando o limiar da cognição. As informações pessoais, por exemplo, são tradicionalmente tratadas na esfera jurídica sempre relacionadas à tutela do direito à privacidade, tendo em vista que é possível traçar uma relação inversa entre quantidade de informação exposta e o grau de privacidade do indivíduo.[45]

42. NEGRI, Sergio; OLIVEIRA, Samuel Rodrigues de; COSTA, Ramon. O Uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. *Revista Direito Público*, v. 17 n. 93, p. 87-88, Brasília, maio/jun., 2020.
43. Idem, ibidem, p. 86.
44. Idem, ibidem, p. 83-84.
45. DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, v. 12, n. 2, p. 94. Joaçaba, jul./dez. 2011.

Para que algo seja caracterizado como informação pessoal, é imperioso que cumpra com determinados requisitos caracterizadores. Acima de tudo, a informação deve ostentar um vínculo objetivo com uma pessoa determinada, de forma a revelar algo específico sobre aquela pessoa.[46] É o caso, por exemplo, do nome, que se refere a um atributo da personalidade que pode ser relacionado diretamente à pessoa. É também o caso da imagem fisionômica de um indivíduo, uma vez que a partir de uma simples representação estática, como uma fotografia, é possível identificar uma pessoa e atribuir a ela uma série de informações pessoais sensíveis, como religião, determinada condição de saúde ou hábitos alimentares. No caso de imagens em movimento, como as que são capturadas desde o estacionamento do supermercado até a entrada do apartamento no corredor do condomínio, o potencial informativo é ainda maior.

Outro ponto a ser considerado é que a extração de dados a partir de câmeras de vídeo, assim como acontece na maioria dos casos de captura de imagem no cotidiano, é um processo unidirecional. "Os processos extrativos que tornam o *big data* possível normalmente ocorrem na ausência de diálogo ou de consentimento, apesar de indicarem tanto fatos quanto subjetividades de vidas individuais".[47] Justamente em razão da unilateralidade do processo de coleta, os indivíduos não têm consciência da frequência com que seus dados, especificamente sua imagem, são capturados rotineiramente. Quer seja por literalmente não notarem a presença massiva de câmeras de segurança na vida cotidiana ou, o que é mais plausível, por terem naturalizado a prática da vigilância de vídeo na sociedade.

Contudo, é importante dispensar atenção também ao direito à imagem como um direito fundamental autônomo, assim reconhecido no art. 5º, inciso X, da Constituição Federal. Os precursores do estudo dos direitos da personalidade não tratavam a imagem, em sua origem, como um direito autônomo, em razão dos equívocos que muitos apontam da redação do at. 20 do Código Civil que vincula a tutela da imagem a uma lesão à honra, boa fama ou a respeitabilidade ou ainda à destinação comercial. Nada disso afasta, porém, a concepção da imagem com uma manifestação da personalidade de seu titular.[48] Justamente em razão dessas características o uso da imagem alheia carece sempre de autorização e, apesar de admitir-se a possibilidade de autorização tácita, sua interpretação deve ser sempre restritiva e seu uso limitado àquilo que foi inequivocamente autorizado.[49]

Um caso recente envolvendo a página do *Facebook* da *Epic Booking* e a Agência de Proteção de Dados Dinamarquesa em janeiro de 2020 pode contribuir com a

46. Idem, ibidem, p. 93.
47. ZUBOFF, Shoshana. Op. cit., p. 33-34.
48. SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. São Paulo: Atlas, 2013, p. 105.
49. Idem, ibidem, p. 119.

ormação pessoal, é imperioso que
adores. Acima de tudo, a informa-
a pessoa determinada, de forma a
caso, por exemplo, do nome, que
de ser relacionado diretamente à
ca de um indivíduo, uma vez que
como uma fotografia, é possível
le informações pessoais sensíveis,
ou hábitos alimentares. No caso
pturadas desde o estacionamento
o no corredor do condomínio, o

ação de dados a partir de câmeras
casos de captura de imagem no
essos extrativos que tornam o *big*
de diálogo ou de consentimento,
ividades de vidas individuais".[47]
esso de coleta, os indivíduos não
os, especificamente sua imagem,
ralmente não notarem a presença
na ou, o que é mais plausível, por
leo na sociedade.

mbém ao direito à imagem como
nhecido no art. 5º, inciso X, da
os direitos da personalidade não
direito autônomo, em razão dos
. 20 do Código Civil que vincula
a ou a respeitabilidade ou ainda
m, a concepção da imagem com
ar.[48] Justamente em razão dessas
empre de autorização e, apesar
cita, sua interpretação deve ser
inequivocamente autorizado.[49]

ebook da *Epic Booking* e a Agência
de 2020 pode contribuir com a

ão Paulo: Atlas, 2013, p. 105.

compreensão da relevância do tema. A *Epic Booking* é uma empresa do setor de fotografia e atua no registro visual de eventos para os quais é contratada, disponibilizando discotecas móveis e máquinas automáticas de *selfie*, por exemplo. O ponto sensível é que as fotos tiradas nos eventos, inclusive de crianças e jovens, eram disponibilizadas na página do *Facebook* da empresa para que qualquer usuário tivesse acesso e, ainda, sem estabelecer previamente um prazo de armazenamento.[50]

A Agência de Proteção de Dados Dinamarquesa concluiu que o consentimento dado pelas pessoas nas fotos não atendia aos requisitos da informação, especificidade e voluntariedade. A Agência concluiu ainda que a empresa não cumpriu as regras sobre o dever de fornecer informações de forma adequada e que era contrário ao princípio da retenção de armazenamento que a empresa responsável não tivesse definido um prazo específico de exclusão das imagens de sua página no *Facebook*. Foi determinado que a *Epic Booking* excluísse de sua página todas as fotos processadas sem o consentimento válido dos titulares dos dados e que fosse estabelecido o prazo de 60 dias para a exclusão das imagens da página da empresa. A justificativa central para a decisão tomada pelo órgão é exatamente o fato de que a publicação de imagens de pessoas identificáveis na internet é considerada um tratamento de dados pessoas, ensejando a tutela das regras de proteção de dados adotadas por aquele país.[51]

O ponto sensível da questão é que o videomonitoramento, combinado com as tecnologias de Inteligência Artificial, apesar dos inegáveis avanços proporcionados, gera também um campo aberto para práticas com grande potencial nocivo para a sociedade, em especial, para os grupos minoritários, uma vez que por mais autônomos e movidos por algoritmos que sejam, estes sistemas são alimentados com os olhares viciados dos humanos que os criam. Este processo consistente em carregar sistemas com os mais diversos dados e atribuir a capacidade de instrumentalização destes é chamado aprendizado de máquinas e, apesar de sua aparente neutralidade, ele pode potencializar os preconceitos, estereótipos e desigualdades já existentes no meio social.[52]

As ferramentas de videovigilância e videomonitoramento, extremamente presentes no cotidiano da vida urbana e social, permitem o reconhecimento facial e redimensiona a relação entre segurança e vigilância. Com efeito, as câmeras de segurança não focalizam exclusivamente grupos ou espaços tidos como perigosos

50. Disponível em: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/mar/ny-afgoerelse-offentliggoerelse-af-festbilleder-af-boern-og-unge. Acesso em: 04 maio 2021.
51. Disponível em: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2021/mar/epic-bookings-behandling-af-personoplysninger. Acesso em: 04 maio 2021.
52. SCHNEIDER, Camila Berlim; MIRANDA, Pedro Fauth Manhães. Op. cit., p. 9.

ou suspeitos, mas com a notável expansão e desenvolvimento dessas tecnologias alcançam o espaço público e privado, envolvendo as mais diversas situações cotidianas. A diversidade de tecnologias de reconhecimento fácil descortina diferentes práticas e propósitos de vigilância. No campo privado, o uso comercial é representado por meio do acesso à aplicativos de bancos e outras plataformas, bem como em portões eletrônicos e computadores. Mais significativo, nos espaços públicos o uso de tecnologia de reconhecimento facial para verificação de identidade e acesso a serviços públicos é ainda mais preocupante.

Por um lado, tais ferramentas promovem a segurança, a eficiência dos serviços e a sua personalização, eis que o acesso fica restrito ao ser usuário, o que evita fraudes e usos indevidos. No entanto, como já alertado, as tecnologias de reconhecimento facial, potencializadas com os algoritmos da Inteligência Artificial, apresentam riscos significativos a partir dos vetores de sua utilização com potenciais malefícios diante da captura da representação fisionômica da pessoa-usuária. A rigor, complexas e diversas são as questões relacionadas à compreensão e aplicação dessas tecnologias, mas os variados fins a que se destinam é importante ponto de partida para os debates a respeito da sua regulamentação, uma vez que os usos para fins de relação de consumo, de segurança pública, de lazer, entre outros, muito se diferenciam entre si e reclamam soluções distintas em razão dos propósitos.

Os sistemas tecnológicos que permitem o reconhecimento facial descortinam potenciais usos maléficos que, sobretudo, possibilita a sua utilização abusiva e discriminatória, em clara violação aos direitos humanos fundamentais. A fisionomia da pessoa humana constitui atributo da personalidade que individualiza e singulariza. Embora, conforma já visto, a imagem não se restrinja à representação fisionômica, eis que em seu aspecto dinâmico contempla as características essenciais de cada indivíduo, indispensável afirmar que que a projeção da imagem-retrato revela dados como idade, cor, etnia, sexo, origem, entre outras informações sensíveis que permitem a discriminação e a exclusão de determinadas pessoas. A rigor, o uso distorcido de tais tecnologias revela a desumanização de pessoas que integram grupos historicamente marginalizados e segregados, eis que as expressões fisionômicas são estereotipadas e caricaturadas. A rigor, o reconhecimento facial é uma tecnologia biométrica que alinhada aos recentes avanços da Inteligência Artificial tem ampliado suas possibilidades de aplicação e potencializado os riscos de discriminação e ofensa aos direitos fundamentais.

Decerto que há problemas na implementação das tecnologias de videovigilância e videomonitoramento, sobretudo aliadas às ferramentas de reconhecimento social. Em especial, as falhas técnicas e o uso prematuro de certas aplicações potencializadas pela inteligência artificial provocam resultados injustos e discri-

minatórios que atingem notadamente as populações vulneráveis, a exemplo de mulheres, negros, pessoas com deficiência e a comunidade LGBTQIAP+. O uso dos algoritmos no reconhecimento facial impulsiona uma hipervigilância que nem sempre promove a segurança, mas, por vezes, reforça a discriminação e provoca a exclusão de certas pessoas, o que descortina a chamada injustiça algorítmica. Severa crítica sofreu estudo de desenvolvimento de software experimental que buscava identificar e diferencias rostos de pessoas homossexuais e heterossexuais, o que pode criar vieses algorítmicos perigosos.[53] No Brasil, o racismo estrutural tem profundas implicações na segurança pública, o que no campo do reconhecimento facial pode gerar resultados enviesados e preconceituosos graves com efeitos nefastos na liberdade individual e criminalização de pessoas negras. Ilustrativamente, pessoas com deficiência podem sofrer discriminação em aplicativos de relacionamento ou similares, o que inclusive tem levado a criação de aplicativos específicos.[54]

Com a promulgação da Lei Geral de Proteção de Dados Pessoais, é indispensável reconhecer que as imagens-retratos das pessoas humanas revelam dados essenciais sobre as identidades individuais, como sexo, idade, origem, funcionalidades, raça, etnia etc. Tais informações capturadas a partir da representação da fisionomia são indelevelmente sensíveis, o que impõe que a tutela da imagem da pessoa humana seja aliada à proteção dos dados pessoais.[55] Cuidam-se de direitos da personalidade, de índole fundamental, eis que ancorados na cláusula geral de proteção e promoção da dignidade da pessoa humana. Talvez seja o momento de compreender que a estática imagem-retrato, na verdade, releva muitos dos aspectos dinâmicos da personalidade, eis que representa o que somos e como nos apresentamos.

5. CONSIDERAÇÕES FINAIS

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 explicita, 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,

53. Disponível em: https://www.bbc.com/portuguese/geral-41250020. Acesso em: 29. jul. 2021.
54. Disponível em: https://emais.estadao.com.br/noticias/comportamento,brasileiro-cria-aplicativo-de-relacionamento-para-pessoas-com-deficiencia,70002860948. Acesso em: 29. jul. 2021.
55. Cf. ALMEIDA, Vitor; RAPOZO, Ian Borba. Proteção de dados pessoais, vigilância e imagem: notas sobre a discriminação fisionômica. In: EHRHARDT JÚNIOR, Marcos. (Org.). *Direito civil*: futuros possíveis. Belo Horizonte: Fórum, 2021, p. 219-250.

tendo-se por medida tanto os critérios definidos em normas expressas quanto por princípios como o da boa-fé objetiva.

Pretendeu-se neste trabalho analisar as convergências e as interseções entre os direitos à imagem e à privacidade em interação com a proteção dos dados pessoais. Com a captura massiva de imagens no cotidiano e a circulação de dados no meio social, desafia o intérprete a uma análise não apensas a partir do tratamento jurídico sob a ótica clássica dos direitos da personalidade, mas também de acordo com a nova legislação específica de tutela do tratamento de dados pessoais. Por fim, como um dos desdobramentos potencialmente maléficos da vigilância constante e da sociedade da informação, tratou-se brevemente do potencial discriminatório desse dado sensível, tendo em conta os exemplos da Internet das Coisas, do videomonitoramento e do reconhecimento facial.

Os avanços tecnológicos descortinam novas fronteiras na proteção das pessoas humanas, em especial a exigir uma tutela dos direitos da personalidade compatível com o cenário já vivenciado. Ao passo que todos são direitos autônomos indubitavelmente, por outro, uma análise da imagem e da privacidade desacoplada da necessária proteção dos dados pessoais é insuficiente. Em um mundo no qual as tecnologias cada vez mais são articuladas com nossas atividades mais corriqueiras e usuais é urgente refletir sobre uma tutela integrada e efetiva em prol da proteção da dignidade da pessoa humana.

REFERÊNCIAS

ALMEIDA, Vitor; RAPOZO, Ian Borba. Proteção de dados pessoais, vigilância e imagem: notas sobre a discriminação fisionômica. In: EHRHARDT JÚNIOR, Marcos. (Org.). *Direito civil*: futuros possíveis. Belo Horizonte: Fórum, 2021.

ALMEIDA JUNIOR, Vitor de Azevedo. A imagem fora de contexto: o uso de imagens de arquivo. In: SCHREIBER, Anderson (Org.). *Direito e mídia*. São Paulo: Atlas, 2013.

BENTHAM, Jeremy. *O panóptico*. 2. ed. Belo Horizonte: Autêntica Editora, 2008.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*. v. 12, n. 2, p. 91-108, Joaçaba, jul./dez. 2011.

FINN, Jonathan. Seeing Surveillantly: Survaillance as Social Practice. In: DOYLE, Aaron; LIPPERT, Randy and LYON, David. *Eyes everywhere*: the global growth of camera surveillance. Edited by. New York: Routledge, 2012.

FOUCAULT, Michael. *Vigiar e punir*: o nascimento da prisão. Trad. Raquel Ramalhete. 42. ed. Petrópolis, RJ: Vozes, 2014.

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

LEMOS, André; MARQUES, Daniel. *Simposio Internacional LAVITS*. Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias. 29 y 30 de noviembre, 01 de diciembre de 2017. Santiago, Chile.

MEDON, Filipe. O direito à imagem na era das *deepfakes*. *Revista Brasileira de Direito Civil – RBD-Civil*, v. 27, p. 251-277, Belo Horizonte, jan./mar., 2021.

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

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral do Proteção de Dados (Lei 13.709/18). *R. Dir. Gar. Fund.*, v. 19, n. 3, p. 159-180, Vitória, set./dez. 2018.

NEGRI, Sergio; OLIVEIRA, Samuel Rodrigues de; COSTA, Ramon. O uso de tecnologias de reconhecimento facial baseadas em inteligência artificial e o direito à proteção de dados. *Revista Direito Público*, Brasília, v. 17 n. 93, p. 82-103, maio/jun. 2020.

ORWELL, George. *1984*. Trad. Karla Lima. Jandira, São Paulo: Principis, 2021.

PEIXOTO, Erick Lucena Campos, EHRARDT JÚNIOR, Marcos. Breves notas sobre a ressignificação da privacidade. *Revista Brasileira de Direito Civil – RBDCivil*, v. 16, p. 35-36, Belo Horizonte, abr./jun. 2018.

SCHNEIDER, Camila Berlim; MIRANDA, Pedro Fauth Manhães. Vigilância e segurança pública: preconceitos e segregação social ampliados pela suposta neutralidade digital. *Emancipação*, v. 20, p. 1-22, Ponta Grossa, 2020.

SCHREIBER, Anderson. *Direitos da personalidade*. 2. ed. São Paulo: Atlas, 2013.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civilistica.com*. a. 9, n. 1, Rio de Janeiro, 2020.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda et al (Org.). *Tecnopolíticas da vigilância*: perspectivas da margem. Trad. Heloísa Cardoso Mourão et al. São Paulo: Boitempo, 2018.