GZ EDITORA

978-65-5813-034-5

DISCUSSÕES SOBRE
DIREITO
NA **ERA DIGITAL**

Coordenadora
Anna Carolina Pinho

GZ EDITORA

DISCUSSÕES SOBRE DIREITO NA ERA DIGITAL

Coordenadora
Anna Carolina Pinho

Prefaciadores
Nelson Rosenvald
Eduardo Tomasevicius Filho
Mamede Said Maia Filho

Autores

- Amanda Luize Nunes Santos
- Ana Beatriz Nóbrega Barbosa
- Ana Cláudia Redecker
- Ana Júlia Silva Alves Guimarães
- Ana Luiza Maia Nevares
- André Luís Bergamaschi
- Anna Carolina Pinho
- Antônio Pereira Gaio Júnior
- Arthur Pinheiro Basan
- Augusto Jobim do Amaral
- Benedito Cerezzo Pereira Filho
- Caio Ribeiro Pires
- Cíntia Rosa Pereira de Lima
- Cláudio José Franzolin
- Clayton Douglas Pereira Guimarães
- Daniel Bucar
- Daniela Marques de Moraes
- Eduardo Dantas
- Eugênio Facchini Neto
- Evandro Piza Duarte
- Fabrício Dreyer de Ávila Pozzebon
- Felipe da Veiga Dias
- Felipe Dannemann Lundgren
- Felipe Varela Caon
- Fernanda Tartuce
- Filipe Medon
- Flávia Mansur Murad Schaal
- Flaviana Rampazzo Soares
- Gabriel Bez-Batti
- Giovana F. Peluso Lopes
- Glayder Daywerth Pereira Guimarães
- Guilherme de Siqueira Castro
- Humberto Dalla Bernardina de Pinho
- Ian Borba Rapozo
- Igor de Lucena Mascarenhas
- Janaina Lima Penalva da Silva
- João Alexandre Silva Alves Guimarães
- José Luiz de Moura Faleiros Junior
- Kelvin Peroli
- Luane Silva Nascimento
- Luís de Lima Pinheiro
- Marcelo Mazzola
- Michael César Silva
- Paola Cantarini
- Paula Greco Bandeira
- Paula Mena Barreto Pinheiro
- Paulo Nalin
- Pedro Paulo Prudente Pereira
- Pietra Daneluzzi Quinelato
- Rafael de Deus Garcia
- Rafaella Nogaroli
- Regina Linden Ruaro
- Roberta de Amorim Dutra
- Roberto Duque Estrada
- Rodrigo Vinícius de Carvalho
- Rogério Vidal Gandra da Silva Martins
- Rubens Beçak
- Samuel Rodrigues de Oliveira
- Sérgio Marcos Carvalho Ávila Negri
- Solano de Camargo
- Tainá Aguiar Junquilho
- Vitor de Azevedo Almeida Júnior
- Vitor Palmela Fidalgo
- Willis Santiago Guerra Filho
- Wilson Pinheiro Jabur

GZ EDITORA

1ª edição – 2021

Diagramação
Olga Martins

CIP – Brasil. Catalogação-na-fonte.
Sindicato Nacional dos Editores de Livros, RJ.

D639

Discussões sobre direito na era digital / coordenação Anna Carolina Pinho. - 1. ed. - Rio de Janeiro: GZ, 2021.
932 p. ; 24 cm.

Inclui bibliografia e índice
ISBN 978-65-5813-034-5

1. Tecnologia e direito. 2. Internet - Legislação - Brasil. 3. Mídia digital - Legislação - Brasil. I. Pinho, Anna Carolina.

21-72635

CDU: 34:004.738.5(81)

Meri Gleice Rodrigues de Souza - Bibliotecária - CRB-7/6439

e-mail: contato@editoragz.com.br
www.editoragz.com.br
Av. Erasmo Braga, 299 – sala 202 – 2º andar – Centro – Rio de Janeiro – RJ – CEP 20010-170
Tels.: (0XX21) 2240-1406 / 2240-1416 – Fax: (0XX21) 2240-1511

Impresso no Brasil
Printed in Brazil

A Jane, sempre ao meu lado.

Ao grande amigo Guilherme Zincone que acreditou nesse projeto, principalmente em mim.

A todos os ilustres colegas que abraçaram esse desafio!

ma de justiça. São textos que conciliam abordagens inovadoras com diferentes matizes conceituais, oferecendo um panorama amplo e diverso dos problemas enfrentados pelo Direito na era da sociedade do conhecimento.

Parabenizo a Editora GZ e a Dra. Anna Pinho, organizadora desta Obra, pelo desafio de reunir, em um mesmo espaço, um leque tão amplo de juristas e pesquisadores que apresentam reflexões sobre temas jurídicos complexos da realidade atual. O conteúdo da Obra fala por si: contribuirá significativamente para que as comunidades jurídicas brasileira e portuguesa disponham de recursos teóricos e empíricos que envolvem os impactos das transformações digitais no Direito. E contribuirá também, com certeza, para a construção de uma justiça mais célere e, por consequência, de um Direito mais inclusivo, que esteja a serviço do progresso social e da melhoria das condições de vida dos nossos povos.

SUMÁRIO

Telessaúde Como Meio de Garantia do Direito ao Aborto: o Caso Brasileiro

Amanda Luize Nunes Santos[1]
Janaína Lima Penalva da Silva[2]

I. Introdução

Com as restrições de circulação e sobrecarga dos serviços de saúde relacionadas à emergência de saúde pública provocada pela COVID-19, o uso de soluções tecnológicas foi explorado intensamente. Nesse contexto, destaca-se o incremento no uso da telessaúde[3], que, essencialmente, consiste no uso de tecnologias de informação e de comunicação na assistência em saúde via substituição do encontro presencial entre profissionais de saúde e pessoas atendidas pelo encontro online. O uso da ferramenta foi incentivado não só para evitar deslocamentos e contatos físicos entre pessoas, como para gerenciar a baixa disponibilidade de profissionais e de recursos.

A telessaúde é considerada pela comunidade científica uma ferramenta eficiente e segura desde que utilizada de forma criteriosa e em atenção aos princípios bioéticos e da ética médica. Embora tenha surgido no final do século XX, como produto dos grandes avanços tecnológicos desse momento, a ferramenta passou a receber mais atenção com o aumento da demanda pelo acesso à saúde e por pressões relacionadas aos gastos públicos e privados[4]. Uma das potencialidades vislumbradas por estudiosos/as do campo é a democratização dos cuidados de saúde, para que cheguem, por exemplo, a localidades de difícil acesso físico. Trata-se, entretanto, de opção a ser considerada com cuidado, de modo

1 Mestranda em Direito pela UnB. Pesquisadora da Anis – Instituto de Bioética. Advogada da clínica Cravinas – Prática em direitos humanos e direitos sexuais e reprodutivos.

2 Professora Adjunta da Faculdade de Direito da Universidade de Brasília (UnB). Mestra e Doutora pela UnB. Pós-Graduada em Direito e Bioética pela Universidade de Barcelona, Espanha. Membro da Coordenação do Centro de Estudos em Desigualdade e Discriminação da Universidade de Brasília/UnB.

3 O presente artigo adotará o termo "telessaúde", em vez de "telemedicina", em razão de o primeiro ser mais amplo do que o segundo, incluindo a atenção multidisciplinar ao aborto previsto em lei no Brasil.

4 MALDONADO, José Manuel Santos de Varge; MARQUES, Alexandre Barbosa; CRUZ, Antonio. Telemedicina: desafios à sua difusão no Brasil. Cadernos de Saúde Pública, v. 32, nº 14, pp. 1-12, 2016. Disponível em: <https://www.scielo.br/j/csp/a/54bg8d5mfWmCC9w7M4FKFVq/?lang=pt>. Acesso em 13 jun 2021.

DUMOULIN, V.; VISIN, F. **A guide to convolution arithmetic for deep learning**. pp. 1-31, 2018.

EBERS, M. Regulating AI and Robotics: Ethical and Legal Challenges. In: EBERS, M.; NAVARRO, S. N. (Eds.). **Algorithms and Law**. [s.l.] Cambridge University Press, 2019. v. 2019 pp. 1-51.

FLORIDI, L. et al. How to Design AI for Social Good : Seven Essential Factors. **Science and Engineering Ethics**, v. 26, nº 3, pp. 1771-1796, 2020.

GOLDBERG, Y. **Neural Network Methods for Natural Language Processing**. Tortonto: Morgan & Claypool Publishers, 2017.

GRAVES, R. **Os mitos gregos. Trad. Fernando Klabin v. 1 e 2.** Rio de Janeiro: Nova Fronteira, 2018.

HEAWOOD, J. Pseudo-public political speech: **Democratic implications of the Cambridge Analytica scandal**. v. 23, nº June, pp. 429-434, 2018.

KEARNS, M.; ROTH, A. **The Ethical Algorithm: The Science of Socially Aware Algorithm Design**. Oxford: Orford University Press, 2020.

KIETZMANN, J. et al. ScienceDirect Deepfakes : Trick or treat? **Business Horizons**, v. 63, nº 2, pp. 135-146, 2020.

MANHEIM, K.; KAPLAN, L. **Artificial Intelligence**: Risks to Privacy and Democracy. v. 106, pp. 106-188, 2019.

MAGRANI, E. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018.

NIELSEN, M. A. **Neural networks and deep learning**. Determination Press, 2015. Disponível em: <http://neuralnetworksanddeeplearning.com/chap2.html>. Acesso em: 12 jul. 2021.

NECHUSHTAI, E.; LEWIS, S. C. Computers in Human Behavior What kind of news gatekeepers do we want machines to be ? Filter bubbles , fragmentation , and the normative dimensions of algorithmic recommendations. **Computers in Human Behavior**, v. 90, nº June 2018, pp. 298-307, 2019.

PARISER, E. **The Filter Bubble: What the Internet Is Hiding from You**. Nova Iorque: The Penguin Press, 2015.

PIOVESAN, Flávia. **Temas de Direitos Humanos**. 9ª ed. rev., ampl. e atual.. São Paulo: Saraiva, 2017.

RASCHKA, S. **Single-Layer Neural Networks and Gradient Descent**. 2015. Disponível em: <https://sebastianraschka.com/Articles/2015_singlelayer_neurons.html>. Acesso em: 01 jul. 2021.

WOLKMER, Antonio Carlos. Direitos Humanos: Novas Dimensões e Novas Fundamentações. **Doutrina Científica**, Ano X, nº 16/17, jan./jun. 2002, pp. 9-32.

Vigilância, Reconhecimento Facial e Discriminação Fisionômica: uma Análise a Partir da Proteção dos Dados Pessoais e do Direito à Imagem

Vítor de Azevedo Almeida Júnior[1]
Ian Borba Rapozo[2]

> *A teletela recebia e transmitia simultaneamente. Qualquer barulho que Winston fizesse, acima do nível de um sussurro muito baixo, era captado por ela; ademais, enquanto ele permanecesse no campo de visão alcançado pela placa metálica, seria visto e também ouvido. Obviamente, não havia como saber se você estava sendo observado em dado momento nem com que frequência, ou por qual sistema, pois a Polícia do Pensamento se conectava a um cabo específico. Era provável que eles observassem todas as pessoas o tempo todo, já que poderiam se conectar a seu cabo quando quisessem. Você era obrigado a viver (e realmente vivia, pois o hábito se tornara instinto) supondo que cada ruído que fizesse seria ouvido, e todo movimento, rastreado, menos na escuridão.*[3]

Introdução

Inobstante poder-se dizer que vivemos hoje o momento mais expoente da sociedade da informação, assim como se percebe da menção à conhecida obra de George Orwell, não é a primeira vez que o tema é amplamente abordado pela academia. Assim como foi tratado sob a ótica da literatura lúdica, a cultura de 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,

---

1 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 (UFRRJ).

2 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.

3 ORWELL, George. *1984*. Trad. Karla Lima. Jandira, São Paulo: Principis, 2021. pp. 10-11.

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.[4]

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.[5]

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, 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.[6]

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

4 BENTHAM, Jeremy. *O Panóptico*. 2. ed., Belo Horizonte: Autêntica Editora, 2008, p. 89.

5 *Id. Ibid.*, p. 89.

6 FOUCAULT, Michael. *Vigiar e punir*: o nascimento da prisão. Trad. Raquel Ramalhete, 42ª ed., Petrópolis, RJ: Vozes, 2014, p. 195.

se originou e se retroalimenta dos mais diversos dados gerados pelos indivíduos.[7]

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.[8]

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 disciplina, 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.[9]

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 nº 12.965 - o Marco Civil da Internet, promulgada em 2014, quer seja sob a ótica atual da Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD), em vigor desde setembro de 2020, com o objetivo de regulamentar em solo nacional o tratamento de dados e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade.

Fato é que, qualquer que seja a concepção filosófica ou sociológica adotada pata tratar do tema, o cenário de vigilância que se impõe no

7 ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda *et al* (Orgs.). *Tecnopolíticas da vigilância*: perspectivas da margem. Trad. Heloísa Cardoso Mourão *et. al.* São Paulo: Boitempo, 2018, pp. 17-68; 42-44.

8 SCHNEIDER, Camila Berlim; MIRANDA, Pedro Fauth Manhães. Vigilância e segurança pública: preconceitos e segregação social ampliados pela suposta neutralidade digital. In: *Emancipação*, Ponta Grossa, v. 20, pp. 1-22, 2020, p. 6.

9 *Id. Ibid.*, p. 5.

presente e do qual não há mais como sair, cria uma longa fila de desafios que devem ser enfrentados. No presente estudo, pretende-se apontar alguns desses desafios, ainda que de forma embrionária. O objeto central da pesquisa se realiza na análise da imagem enquanto dado sensível e no seu potencial informativo e discriminatório, sem prejuízo das referências necessárias a outros tópicos relacionados, relevantes para a compreensão da questão tratada. Desenvolve-se o presente estudo a partir de ampla pesquisa bibliográfica e interdisciplinar, que se alimenta de conhecimentos clássicos do campo jurídico, bem como de conceituações diversas, provenientes de outras áreas do saber.

Para tanto, dedica-se à compreensão de novas formulações sobre a sociedade de vigilância, não apenas sob a ótica geral da vigilância a partir de dados pessoais, mas a partir do campo específico do videomonitoramento. É introduzida nessa seção a concepção de uma sociedade constituída pelo hábito da vigilância, dividida em três formas distintas de manifestação, como proposto por Jonathan Finn. Na segunda parte são abordadas as bases legais criadas pela Lei Geral de Proteção de Dados Pessoais que se relacionam ao tema em estudo, demonstrando os pontos relevantes da legislação e a pertinência da sua aplicação no trato da questão. É mencionado ainda o fenômeno do reconhecimento facial por Inteligência Artificial, as justificativas que se apresentam para a sua adoção e os perigos que podem advir de sua implementação.

Mais para frente, trata-se de forma mais direta do objeto central da pesquisa, apresentando a imagem humana, constantemente capturada no cotidiano, a partir de uma perspectiva dúplice. Em primeiro lugar a imagem é abordada como um direito da personalidade, uma noção clássica e consolidada da qual não se pode prescindir. Não obstante, em segundo lugar, apresenta-se a concepção da imagem também como um dado pessoal sensível, diante do absoluto potencial informativo que pode carregar. Desse modo, pretende-se apresentar algumas breves notas a respeito da imagem-retrato somada às tecnologias de reconhecimento facial e do nascimento de novos desafios diante da captura da representação fisionômica da pessoa-usuária e do seu potencial discriminatório.

1. Um novo olhar sobre o cotidiano a partir da sociedade de vigilância

Há diversas perspectivas de vigilância a partir das quais o vigente modelo social pode ser abordado. Os dados derivados de transações econômicas mediadas por computador, por exemplo, representam uma parcela significativa do *big data* existente no mundo hoje. No entanto,

como esclarece Shoshana Zuboff[10], há 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 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[11], 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 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,

10 ZUBOFF, Shoshana. *Op. Cit.*, pp. 27-28.

11 FINN, Jonathan. Seeing Surveillantly: Surveillance as Social Practice. In: *Eyes Everywhere:* The Global Growth of Camera Surveillance. Edited by Aaron Doyle, Randy Lippert and David Lyon. New York: Routledge, 2012, p. 67.

cor e outras formas de formatação, ganham significado específico, normalmente direcionado à disseminação de uma mensagem comercial.[12]

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.[13]

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* 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.[14]

12 FINN, Jonathan. *Op. Cit.*, pp. 72-73.

13 *Id. Ibid.*, pp. 74-76.

14 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 01 jun. 2021.

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.[15]

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[16]. 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.[17]

2. Tratamento de dados e reconhecimento facial

Para realizar a análise jurídica da questão da vigilância, quer seja sob um aspecto amplo, quer seja sob o enfoque do videomonitoramento, é necessário discorrer sobre a nova Lei Geral de Proteção de Dados Pessoais, em vigor no Brasil há menos de um ano e que se relaciona diretamente com os pontos tratados neste estudo. A LGPD, Lei nº 13.709/18, é inspirada no *General Data Protection Regulation*, uma versão atualizada de outra lei de privacidade da União Europeia chamada *Data Protection Directive*, que estava em vigor desde 1995, com o objetivo de tutelar o tratamento de dados pessoais de seus cidadãos.

A legislação brasileira 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, conforme aponta seu art. 1º. A Lei é enfática também ao afirmar a pro-

15 FINN, Jonathan. *Op. Cit.*, p. 78.

16 Disponível em: https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software. Acesso em 01 jun. 2021.

17 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: 01 jun. 2021.

moção 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, a LGPD traz em seu texto as definições que lhe são essenciais e os princípios que norteiam sua aplicação. Os princípios da Lei nº 13.709/18 que chamam maior atenção são os da finalidade e da não discriminação, em razão de sua destacada relevância para a tutela dos dados pessoais. De acordo com o princípio da finalidade, todos os dados devem ser coletados e tratados para um propósito determinado, previamente estabelecido, e devidamente informado ao titular dos dados de maneira explícita e clara, vedada sua utilização para qualquer outro fim diverso daquele inicialmente informado. A seu turno, o princípio da não discriminação assegura que os dados não serão utilizados para fins discriminatórios ilícitos ou abusivos, tomando por medida tanto aqueles critérios já legalmente definidos em normas expressas quanto por princípios como o da boa-fé objetiva, por exemplo.[18]

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[19], 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.[20]

18 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, pp. 163-165.

19 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;

20 TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. In: *Civilistica.com*. Rio de Janeiro, a. 9, nº 1, 2020, p. 4. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 11 jan. 2021.

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 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.[21]

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[22]. 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"[23]. 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.

21 "Institui 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 nº 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.

22 TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. *Op. Cit.*, p. 6.

23 *Id. Ibid.*, p. 14.

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 informações sobre os indivíduos, o que desafia a atenção em sua interpretação de acordo com esta natureza.[24]

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.[25]

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.[26]

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.

24 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. In: *Revista Direito Público*, Brasília, vol. 17 nº 93, pp. 82-103, maio/jun., 2020, pp. 87-88.

25 *Id. Ibid.*, p. 86.

26 *Id. Ibid.*, pp. 83-84.

3. Direito à imagem em uma perspectiva dúplice

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.

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[27] 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.

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.[28]

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

27 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.

28 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. In: *Espaço Jurídico*, Joaçaba, vol. 12, nº 2, pp. 91-108, jul./dez., 2011, p. 94.

determinada, de forma a revelar algo específico sobre aquela pessoa[29]. 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"[30]. 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[31]. 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.[32]

A concepção mais contemporânea do direito à imagem é aquela que a relaciona não mais apenas aos aspectos físicos da pessoa retratada,

29 *Id. Ibid.*, p. 93.

30 ZUBOFF, Shoshana. *Op. Cit.*, pp. 33-34.

31 SCHREIBER, Anderson. *Direitos da Personalidade*. 2. ed., São Paulo: Atlas, 2013, p. 105.

32 *Id. Ibid.*, p. 119.

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.[33]

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 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.[34]

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 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.[35]

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

33 MEDON, Filipe. O direito à imagem na era das *deepfakes*. In: *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 27, pp. 251-277, jan./mar., 2021, p. 258.

34 *Id. Ibid.*, p. 255.

35 Disponível em: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/mar/ny-afgoerelse-offentliggoerelse-af-festbilleder-af-boern-og-unge. Acesso em: 04 mai. 2021.

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.[36]

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.[37]

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 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 maleífícios diante da captura da representação fisionômica da pessoa-usuária. A rigor, complexas e

36 Disponível em: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2021/mar/epic-bookings-behandling-af-personoplysninger. Acesso em: 04 mai. 2021.

37 SCHNEIDER, Camila Berlim; MIRANDA, Pedro Fauth Manhães. *Op. Cit.*, p. 9.

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 discriminatórios 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[38]. No Brasil, o racismo estrutural tem profundas implicações na segurança pública, o que no campo do reconhecimento facial

38 Disponível em: https://www.bbc.com/portuguese/geral-41250020. Acesso em: 29. jul. 2021.

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[39].

A representação fisionômica, importante atributo da imagem da pessoa humana, revela mais do que aspectos estéticos, mas sobretudo características pessoais que permitem a discriminação, sobretudo de grupos vulneráveis. Compreender as tecnologias de reconhecimento facial depende de uma análise minuciosa sobre as possíveis injustiças que os algoritmos podem provocar, o que gera exclusão e violação de direitos fundamentais. Tais ferramentas propiciam, a partir de usos enviesados e distorcidos, a chamada discriminação fisionômica, ou seja, a partir dos traços da fisionomia de uma determinada pessoa, o que, a rigor, trata de discriminação racial, etária, de gênero, contra pessoas com deficiência, contra a comunidade LGBTQIAP+, entre outros.

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. 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.

Conclusão

É preciso ter apego à realidade e ao pragmatismo e compreender que a sociedade de vigilância já se instalou há muito na vida cotidiana dos indivíduos e os principais esforços não devem ser desgastados em alguma forma de tentativa de escape ou retorno a um estado anterior a este, mesmo porque seria uma tarefa extremamente difícil determinar em que momento a vigilância se instalou definitivamente na vida humana.

39 Disponível em: https://emais.estadao.com.br/noticias/comportamento,brasileiro-cria-aplicativo-de-relacionamento-para-pessoas-com-deficiencia,70002860948. Acesso em: 29. jul. 2021.

Como se demonstrou, o estudo do tema não é inovador por si só e já foi tratado por diversos estudiosos não apenas do direito, mas da filosofia, sociologia e das diversas áreas de saber tecnológico. Os esforços devem centrar-se, portanto, na compreensão adequada do corpo social na forma em que ele se apresenta diante de nós e, mais ainda, nos novos desafios que se colocam diante dessa realidade.

Pretendeu-se neste trabalho chamar a atenção para algumas destas questões, notadamente aquelas provenientes da captura massiva de imagens no cotidiano, ensejando o tratamento jurídico do tema não somente sob a ótica clássica dos direitos da personalidade, mas também de acordo com a nova legislação específica de tutela do tratamento de dados pessoais, tendo por fundamento central a compreensão da imagem enquanto dado sensível. Por fim, como um dos desdobramentos potencialmente maléficos da vigilância constante, tratou-se brevemente do potencial discriminatório desse dado sensível, notadamente em relação à discriminação fisionômica.

O estudo da nova Lei Geral de Proteção de Dados Pessoais abre uma enorme janela de pesquisas para a ciência jurídica. O objetivo do presente artigo é apresentar algumas novas concepções sobre a sociedade de vigilância, somadas à conhecimentos já consolidados, para incentivar o estudo sobre a tutela jurídica do direito à imagem neste novo contexto que se impõe, com especial atenção ao potencial lesivo que o tratamento da imagem cria, especialmente quando se desenvolve em países como o Brasil, nos quais há a expressiva manifestação de diversas formas de preconceito e discriminação.

Referências bibliográficas

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

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. In: *Espaço Jurídico*, Joaçaba, vol. 12, nº 2, pp. 91-108, jul./dez., 2011.

FINN, Jonathan. Seeing Surveillantly: Surveillance as Social Practice. In: *Eyes Everywhere:* The Global Growth of Camera Surveillance. Edited by Aaron Doyle, Randy Lippert and David Lyon. New York: Routledge, 2012.

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

MEDON, Filipe. O direito à imagem na era das *deepfakes*. In: *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 27, pp. 251-277, 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 (Orgs.). *Horizonte presente*: tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito, Fundação Getúlio Vargas, 2019.

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. In: *Revista Direito Público*, Brasília, vol. 17 nº 93, pp. 82-103, maio/jun., 2020.

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

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

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

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. In: *Civilistica.com*. Rio de Janeiro, a. 9, nº 1, 2020.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda *et al* (Orgs.). *Tecnopolíticas da vigilância*: perspectivas da margem. Trad. Heloísa Cardoso Mourão *et. al.* São Paulo: Boitempo, 2018, pp. 17-68.

O Direito à Portabilidade de Dados Pessoais[1]

Vítor Palmela Fidalgo[2]

Sumário: 1. Introdução **2.** Objetivos do direito à portabilidade dos dados pessoais **2.1.** A menorização do efeito *lock-in* **2.2.** O controlo e o reuso dos dados pessoais pelo titular **2.3.** A tentativa de equilibrar a relação entre os titulares dos dados pessoais e as entidades que beneficiam com o tratamento dos mesmos **2.4.** Promoção de uma nova economia digital **3.** O conteúdo do direito à portabilidade de dados pessoais **3.1.** Direito a receber cópia dos dados pessoais **3.2.** Direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento **4.** Requisitos **4.1.** Os dados pessoais alvo de portabilidade **4.2.** A portabilidade de dados pessoais alvo de tratamento com base no consentimento ou num contrato **4.3.** A automatização do tratamento dos dados pessoais **5.** O procedimento para o exercício do direito à portabilidade de dados pessoais **6.** O dever de informação no exercício do direito à portabilidade de dados pessoais **7.** Direito à portabilidade de dados pessoais e direito ao esquecimento **8.** O Direito à portabilidade de dados pessoais e direitos de terceiros **8.1.** Dados de terceiros **8.2.** Direitos de propriedade intelectual **8.3.** Segredos comerciais **9.** Considerações finais

1. Introdução

I. Tendo como objetivos o reforço da proteção dos titulares de dados pessoais e a impulsão da economia digital europeia, o novo Regulamento (UE), nº 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, sobre a proteção de dados pessoais (doravante RGPD), apresenta, como uma das grandes novidades, o direito à portabilidade de dados pessoais ("*right to data portability*" ou "RtDP"), que, de acordo

1 O presente texto corresponde, no essencial, às conferências apresentadas no âmbito do I, II, III e IV Cursos de Pós-Graduação em E-Commerce, organizados pelo Instituto do Direito do Consumo e pelo Centro de Investigação de Direito Privado da Faculdade de Direito da Universidade de Lisboa, sob a coordenação do Professor Doutor Rui Paulo Coutinho Mascarenhas Ataíde e do Professor Doutor António Barreto Menezes Cordeiro. O mesmo foi, igualmente, publicado no nº 1, da Revista de Direito e Tecnologia (2019).

2 Docente da Faculdade de Direito da Universidade de Lisboa. Investigador do Centro de Investigação de Direito Privado (CIDP)