O Uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados

SERGIO MARCOS CARVALHO DE ÁVILA NEGRI[1]
Universidade Federal de Juiz de Fora, Minas Gerais, Brasil.

SAMUEL RODRIGUES DE OLIVEIRA[2]
Universidade Federal de Juiz de Fora, Minas Gerais, Brasil.

RAMON SILVA COSTA[3]
Universidade Federal de Juiz de Fora, Minas Gerais, Brasil.

RESUMO: Os recentes avanços na área da inteligência artificial e *big data* possibilitaram o desenvolvimento de tecnologias de reconhecimento facial. Este artigo tem como objetivo investigar como a utilização de tais tecnologias pode gerar violações ao direito à privacidade e à proteção de dados. Conclui-se haver necessidade de desenvolvimento de tecnologias em consonância com os princípios dispostos nas legislações de proteção de dados, a fim de se garantir a salvaguarda de tais direitos.

PALAVRAS-CHAVE: *Big data;* dados pessoais; inteligência artificial; privacidade; vigilância.

ABSTRACT: Recent advances in the field of artificial intelligence and big data have enabled the development of facial recognition technologies. This paper aims to investigate how the use of such technologies can lead to violations of the right to privacy and data protection. We conclude that it is necessary to develop technologies in compliance with the principles established by data protection laws in order to ensure the safeguarding of such rights.

KEYWORDS: artificial intelligence; big data; personal data; privacy; surveillance.

1 Orcid: <http://orcid.org/0000-0003-2156-3518>.
2 Orcid: <http://orcid.org/0000-0002-7059-580X>.
3 Orcid: <http://orcid.org/0000-0003-4183-432X>.

INTRODUÇÃO

Os avanços recentes da ciência de dados e das técnicas de inteligência artificial, somados à suposta demanda por segurança no mundo contemporâneo, fizeram surgir a sociedade da vigilância, que hoje se apresenta como um pan-óptico digital. Nesse contexto, tecnologias de reconhecimento facial destacam-se enquanto ferramentas empregadas para fins de vigilância, cuja onipresença torna-se cada vez mais evidente.

Concomitantemente ao desenvolvimento dessas novas tecnologias, o que foi possibilitado por fatores como a existência de métodos estatísticos e probabilísticos cada vez mais sofisticados e a disponibilidade de *big data* (grandes bases de dados) (Floridi *et al.*, 2017), ocorreram mudanças paradigmáticas das noções de democracia e direitos fundamentais. Isso gerou um aumento de funções estatais, culminando na transformação do próprio Estado, que passou a assumir demandas mais complexas e em maior número, implicando uma tendência mundial de se implementar atividades e serviços públicos, inclusive aqueles de vigilância, alicerçados por sistemas de IA (Eggers, Schatsky e Viechnicki, 2017; Mehr, 2017).

Sobram exemplos, em todo o mundo, do uso de tecnologias de reconhecimento facial para fins de vigilância. Na China, 200 milhões de câmeras compõem um sistema de vigilância capaz de identificar basicamente qualquer um dos 1.4 bilhões de habitantes do país[4]. Em Dubai, capital dos Emirados Árabes Unidos, um gigantesco "túnel-aquário" localizado no principal aeroporto da cidade conta com mais de 80 câmeras de segurança, que capturam e digitalizam, por meio de escâneres, o rosto das pessoas à medida que caminham por ele; por fim, realizada a análise das imagens obtidas, o sistema de segurança ou permite que a pessoa ingresse livremente no país ou emite um alerta, indicando a necessidade de uma análise mais aprofundada acerca da entrada do indivíduo[5]. Nos Estados Unidos da América, no ano de 2016, ao menos 50% dos cidadãos adultos já constavam em bases de dados de reconhecimento facial do governo[6].

No Brasil não é diferente. Na cidade do Rio de Janeiro, o programa "Rio+Seguro" foi apresentado como "um programa pioneiro [...] que

4 Disponível em: <https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html>. Acesso em: 23 set. 2019.

5 Disponível em: <https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium>. Acesso em: 23 set. 2019.

6 Disponível em: <https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/>. Acesso em: 23 set. 2019.

associa planejamento, inteligência e tecnologia na prevenção à desordem urbana e à criminalidade", conforme consta do sítio eletrônico do projeto[7]. A inteligência e tecnologia referidas correspondem, na realidade, ao uso de *software* de reconhecimento facial baseado em IA, a fim de se identificar e, consequentemente, deter suspeitos e foragidos. No estado da Bahia, por sua vez, tem ganhado força um projeto semelhante, intitulado "Vídeo Policiamento". Segundo Rui Costa, Governador do Estado, o projeto "é uma ferramenta que fará o reconhecimento não só de criminosos, mas a meta é colocar todos os 15 milhões de baianos"[8] (*sic*).

Diante desse contexto, o presente artigo objetiva discutir o uso de sistemas de reconhecimento facial baseados em IA para fins de vigilância e segurança pública, analisando a relação dessas tecnologias com o direito à proteção de dados pessoais. Assim, pergunta-se: as tecnologias de reconhecimento facial podem ocasionar violações ao direito à proteção de dados pessoais? A hipótese levantada é que o uso dessas tecnologias pode implicar a mitigação do direito à privacidade e, consequentemente, do direito à proteção de dados.

No que tange à metodologia, trata-se de uma pesquisa exploratória, cujo escopo é proporcionar maior familiaridade com o problema, a fim de torná-lo mais explícito e/ou de construir hipóteses (Gil, 2007). Como aponta Fonseca (2002), a pesquisa científica pode basear-se fundamentalmente na pesquisa bibliográfica, "procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta" (Fonseca, 2002, p. 32). Tendo em vista a relativa novidade do tema aqui abordado, bem como a escassez de estudos e publicações atinentes ao assunto em âmbito nacional, a pesquisa bibliográfica revela-se de grande importância para a concretização dos objetivos pretendidos. Nesse sentido, como a maioria das pesquisas exploratórias vale-se do levantamento bibliográfico como método principal (Gil, 2007), esse será o método majoritariamente adotado no presente trabalho.

1 TECNOLOGIAS DE RECONHECIMENTO FACIAL E A CONSOLIDAÇÃO DA SOCIEDADE DA VIGILÂNCIA

Não existe consenso na literatura especializada sobre o conceito de inteligência artificial. Todavia, é possível afirmar, em linhas gerais, que se trata

7 Disponível em: <http://maisseguro.rio>. Acesso em: 23 set. 2019.

8 Disponível em: <http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html>. Acesso em: 23 set. 2019.

da tentativa de reprodução da cognição humana e seus mais variados componentes – como o aprendizado, a memória e o processo de tomada de decisões – mediante o uso de *softwares* computacionais. Não obstante, uma boa definição acerca do conceito de IA é aquela formulada por John McCarthy, considerado o "pai da inteligência artificial". Para o autor, constrói-se uma inteligência artificial (IA) ao se fazer uma máquina comportar-se de maneira que, caso se tratasse de um ser humano, fosse considerada inteligente (McCarthy, 2000).

Desde a última década, tem sido possível observar um exponencial desenvolvimento de tecnologias de inteligência artificial e de *big data*. Segundo Floridi *et al.* (2017), esse movimento foi desencadeado pelos seguintes fatores: a criação de métodos estatísticos e probabilísticos cada vez mais sofisticados; a disponibilidade de ampla e crescente quantidade de dados; a acessibilidade a um enorme, e relativamente barato, poder computacional; e a transformação cada vez maior dos ambientes com as novas tecnologias de informação, como a automação residencial e a criação de cidades inteligentes. Esses fatores, que se retroalimentam, possibilitaram avanços patentes na ciência de dados e nas técnicas de IA.

Fato é que, em uma conjuntura de crescimento populacional em áreas urbanas, o que implica uma maior demanda pela atuação do Estado, a Administração Pública depara-se com uma série de desafios concernentes aos mais diversos setores, inclusive de vigilância e controle social. Marina Barros e Jamila Venturini, discutindo os desafios inerentes às chamadas "cidades inteligentes", apontam que "o uso das tecnologias de informação e comunicação (TIC) e processamento de grandes volumes de dados tem se mostrado atrativo para gestores públicos, dado seu potencial de auxiliar no planejamento urbano" (Barros; Venturini, 2018, p. 32).

Concatenando todos esses elementos, Rodotà discorre sobre como o avanço incontido da internet, com a crescente e intensa coleta de dados pessoais, somada à interconexão entre diversos bancos de dados que realizam o cruzamento de informações, faz surgir uma sociedade pautada pelo controle, pela vigilância e pela classificação. Para o autor, a sociedade da informação "ameaça sombrear o crescimento igualmente intenso dos bancos de dados mais tradicionais, aqueles com finalidade de segurança, que também são modificados pelas tecnologias e pela realidade de um mundo sem fronteiras" (Rodotà, 2008, p. 146). Exemplos do emprego de tais tecnologias, como exposto anteriormente, são cada vez mais comuns, sendo, nas palavras do jurista italiano, "uma tendência que já parece irresistível, comum aos mais diversos países" (Rodotà, 2008, p. 147).

Assim, é interessante para os gestores públicos o uso de novas tecnologias alimentadas pelos *big data*, grandes bases de dados, devido ao potencial que tais tecnologias possuem de auxiliar no planejamento urbano. Esse uso, ao mesmo tempo, é impulsionado pelo setor privado, que busca expandir seus mercados, por exemplo, com a intitulada "internet das coisas" (IoT, do inglês, *internet of things*). Nesse sentido, expõe Caitlin Mulholland que IoT possibilita não apenas a comunicação e realização de funções específicas entre as coisas, como também gera "cada vez mais constante coleta, transmissão, guarda e compartilhamento de dados entre os objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas" (2018, p. 485, 486).

Nessa conjuntura, ocorreu o desenvolvimento e aperfeiçoamento das tecnologias de reconhecimento facial. Segundo Vu (2018), técnicas de reconhecimento facial surgiram como uma tentativa de superar a incapacidade do cérebro humano de processar, memorizar e lembrar-se de milhares de faces com que se depara todos os dias. Porém, na atualidade, e especialmente depois dos ataques terroristas ocorridos em setembro de 2001 nos EUA, agências governamentais têm se utilizado de todos os meios para desenvolver maneiras eficientes e precisas de regular o afluxo de pessoas por meio da identificação dos indivíduos, a fim de garantir que nenhuma ameaça conhecida seja permitida, pois, argumenta-se, isso pode colocar em risco os cidadãos de uma sociedade (Vu, 2018, p. 11-12).

Uma "tecnologia de reconhecimento facial" nada mais é que um *software* programado para reconhecer e identificar rostos humanos específicos a partir de fotos ou vídeos. Utilizando amplas bases de dados, e valendo-se de conexões de internet ultravelozes, as tecnologias de reconhecimento facial identificam e catalogam detalhes de cada indivíduo a fim de processar imagens obtidas em um computador, *smartphone* ou câmera de vigilância; os dados processados podem ser usados, então, para uma extensiva gama de propósitos (Nabeel, 2019).

Em linhas gerais, um sistema de reconhecimento facial opera mediante o uso de biometria para mapear características faciais de uma pessoa presente em uma fotografia ou vídeo, comparando as informações obtidas com um banco de dados de rostos conhecidos para encontrar uma correspondência. Embora as técnicas empregadas variem, os sistemas de reconhecimento facial geralmente operam a partir de etapas comuns, conforme expõe Weschler (2007). Primeiramente, uma foto do rosto da pessoa é capturada a partir de uma foto ou vídeo; em seguida, o *software* de reconhecimento facial analisa a "geometria" do rosto, identificando fatores como a distância

entre os olhos e a distância da testa ao queixo e elaborando uma "assinatura facial" a partir da identificação dos pontos de referência faciais. O terceiro passo consiste na comparação da assinatura facial – que nada mais é que uma fórmula matemática – a um banco de dados de rostos conhecidos, pré-coletados e armazenados. Finalmente, realiza-se a etapa de determinação, em que pode ocorrer a verificação (quando se analisa uma determinada assinatura digital em comparação a uma única outra, já definida) ou identificação (quando se compara determinada assinatura digital a diversas outras constantes do banco de dados) do rosto analisado.

Clive Norris (2003) argumenta que a introdução de sistemas de vigilância baseados em circuitos fechados de televisão (CFTV/CCTV)[9] desde o século passado alterou fundalmentamente a natureza da *surveillance*, da vigilância ostensiva, tanto quantitativa quanto qualitativamente. Para o autor, simplificadamente, com a introdução da tecnologia de circuitos fechados de televisão,

> o escopo da vigilância foi expandido para um nível inimaginável com base na copresença; o escopo da vigilância não mais se restringe às limitações espaciais inerentes à vigilância presencial; o escopo da vigilância fica livre das restrições temporais da interação face a face e da presença humana; a vigilância e a intervenção autoritária tornam-se funcionalmente separadas; o ato de vigilância se torna mais democrático: todos ficam igualmente sujeitos ao olhar de vigilância; o projeto disciplinar do *panopitcon* é expandido à medida que o controle social inclusivo é promovido sobre a exclusão. (Norris, 2003, p. 253 – tradução nossa)

Norris reconhece ainda que a transição para uma sociedade digital resultou na intensificação da sociedade de vigilância. Isso porque, tradicionalmente, os sistemas inteligentes de vigilância valiam-se da tecnologia de reconhecimento facial apenas para fornecer uma confirmação visual de eventos. Mas agora, com sistemas digitais que possibilitam o reconhecimento de pessoas a partir de cruzamento de informações com enormes bases de dados, a própria imagem de vídeo torna-se a fonte de informação. *Softwares* de reconhecimento facial dotados de IA representam, portanto, um significativo avanço multificional em relação às informações geradas em um circuito fechado de televisão. Explica-se: uma vez que as imagens são dispostas em um banco de dados digital, e o processamento dessas imagens

9 *CCTV*, sigla em inglês para *closed-circuit television*. Em português, utiliza-se o termo "circuito fechado de TV", ou "CFTV". Corresponde a um sistema de TV em que os sinais não são distribuídos de forma pública, mas monitorados, principalmente para fins de vigilância e segurança.

é realizado por meio de algoritmos, o potencial de conexão com bancos de dados já existentes é dramaticamente amplicado (Norris, 2003, p. 269), e "a ligação de informações extraídas de imagens de CFTV a informações relacionadas à identidade em bases de dados exponicialmente aumenta o seu 'efeito pan-óptico'" (Norris, 2003, p. 270).

Byung-Chul Han, filósofo sul-coreano, fala em um "pan-óptico digital", "dominado pela aparência de liberdade e comunicação ilimitadas", no qual "a transparência e a informação substituem a verdade" (Han, 2018b, p. 56). Para o autor, "o novo objetivo do poder não consiste na administração do passado, mas no controle psicopolítico do futuro" (Han, 2018b, p. 56). O pan-óptico digital diferencia-se do Grande Irmão de Bentham, pois, na sociedade digital, as pessoas não se sentem realmente vigiadas ou ameaçadas, mas, pelo contrário, sentem-se livres. Contudo, "é exatamente essa sensação de liberdade, inexistente no Estado de vigilância de Orwell [que desenvolveu a conhecida ideia do *Big Brother*], que constitui um problema" na sociedade digital (Han, 2018b, p. 57).

Han aponta que as próprias coisas, *i.e.*, objetos que utilizamos cotidianamente, tornaram-se emissoras ativas de informações sobre as pessoas. A expansão da internet das pessoas – *web 2.0* – para a internet das coisas – *web 3.0* – "completa a sociedade de controle digital" (Han, 2018b, p. 86), pois a internet das coisas torna possível um registro (quase) total da vida. Nesse mesmo sentido, Rodotà (2013) aponta que o advento da *web 3.0* não só tornou possível a consolidação da internet das coisas, mas também tornou patente a exigência de uma nova abordagem no que concerne aos problemas da vigilância.

Explica-se: antes de tudo, a vigilância não é apenas o resultado de uma atividade deliberada e específica, mas também um subproduto do comportamento das pessoas, que cedem voluntariamente muitas informações sobre si. Em segundo lugar, a vigilância não é apenas o resultado de um tratamento consciente dos dados, mas, em um número crescente de casos, o resultado das funções atribuídas aos algoritmos. Ainda, a vigilância não visa a controlar pessoas individualmente, atividades particulares ou segmentos específicos da sociedade, mas está tornando-se um procedimento universal, envolvendo as pessoas em geral. Por fim, os riscos da vigilância não surgem principalmente das atividades dos órgãos de segurança pública, mas da coleta incessante por entes comerciais privados (Rodotà, 2013).

Sem dúvida, "os *big data* tornam possível uma forma de controle muito eficiente", pois

> o pan-óptico digital oferece uma visão em 360º dos seus internos. O pan-óptico de Bentham está ligado à óptica perspectivista. Desse modo, são inevitáveis pontos cegos nos quais os prisioneiros podem perseguir seus pensamentos e desejos secretos sem serem notados. A vigilância digital é mais eficiente porque é aperspectivista. Ela é livre de limitações perspectivistas que são características da óptica analógica. A óptica digital possibilita a vigilância a partir de qualquer ângulo. Assim, elimina pontos cegos. Em contraste com a óptica analógica e perspectivista, a óptica digital pode espiar até a *psique*. (Han, 2018b, p. 78)

As implicações do pan-óptico digital nas questões referentes à privacidade e à proteção de dados serão mais bem endereçadas no tópico seguinte.

2 A PROTEÇÃO DE DADOS PESSOAIS NO PAN-ÓPTICO DIGITAL

2.1 Privacidade e proteção de dados pessoais no Direito

Conforme aponta Danilo Doneda (2006), a privacidade é historicamente compreendida a partir da dicotomia público-privado. Para o autor, o direito à privacidade sempre partiu de ideias sobre quais atividades deveriam ser exercidas na esfera pública e quais deveriam estar restritas ao espaço privado dos indivíduos, sendo limitado por uma compreensão de que a habitação dos indivíduos seria o local de refúgio do escrutínio público. Assim, há uma seleção entre as informações que podem ser partilhadas publicamente e aquelas que devem ser mantidas no sigilo privado. Ainda que informações da vida íntima sejam compartilhadas com maior ou menor número de pessoas, restringem-se ao controle dos indivíduos e ao seu interesse de mantê-las distantes do público em geral.

Contudo, o entendimento clássico sobre o direito à privacidade como "*the right to be left alone*" revela-se limitado e insuficiente no cenário atual. Rodotà destaca a necessidade de ampliação do conceito de direito à privacidade em uma sociedade altamente digitalizada. Para o autor italiano, o processo evolutivo do conceito de direito à privacidade vai desde a ideia de ser deixado em paz até uma compreensão de direito de controle sobre as informações pessoais e de construção da esfera privada. Assim, a evolução do direito à privacidade envolveria a proteção de dados pessoais (Rodotà, 2008, p. 17), implicando uma transformação do conceito, que passa a abarcar não só o poder de exclusão, ou seja, de impedimento de interferências alheias, mas também compreende a centralidade do controle do indivíduo sobre suas informações pessoais. Enquanto a influência da tecnologia dos

computadores levou à reconceituação da privacidade como o "direito a controlar o uso que os outros façam das informações que me digam respeito", os avanços tecnológicos mais recentes fizeram surgir "um outro tipo de definição, segundo o qual a privacidade consubstancia-se no 'direito do indivíduo de escolher aquilo que está disposto a revelar aos outros'" (Rodotà, 2008, p. 74).

Dessa forma, a privacidade caminhou da sequência "pessoa-informação-sigilo" para "pessoa-informação-circulação-controle" (Rodotà, 2008, p. 93). Atualmente, emergem novos desdobramentos, como aponta Nadezhda Purtova (2018): devem-se discutir os *information-induced harms* (em tradução livre, "danos causados pela informação"), que devem ser entendidos amplamente como qualquer consequência negativa, pública ou individual, do processamento de informações. Portanto, à ideia tradicional de privacidade devem acrescentar-se as novas dimensões contemporâneas que perpassam a esfera privada e as informações pessoais. Isso não significa, porém, que a proteção de dados pessoais é uma simples extensão do processo evolutivo do conceito de privacidade, mas indica que ela se estabelece como um direito autônomo, que necessita de clareza e especificidade normativa. Mesmo que a proteção de dados esteja relacionada, em alguns aspectos, à tutela da privacidade dos indivíduos, não está restrita a dicotomia do público e do privado (Bioni, 2018, p. 98-99), de modo que o direito à proteção de dados passa a ser reconhecido pela doutrina como um direito fundamental autônomo (Mendes, 2014), entendimento seguido pelo STF em importante decisão histórica (Mendes, 2020).

Há de se observar, todavia, como as esferas pública e privada organizam-se em uma sociedade digital. Para Byung-Chul Han, o alicerce da esfera pública é o respeito. Esta pressupõe "um não olhar para a vida privada" (Han, 2018a, p. 12), sendo a tomada de distância elemento constitutivo do espaço público. Hoje, porém, "domina uma falta total de distância, na qual a intimidade é exposta publicamente e o privado se torna público". Tal falta de distância leva à confusão entre o privado e público, alimentada principalmente pela comunicação digital, que "fornece essa exposição pornográfica da intimidade e da esfera privada" (Han, 2018a, p. 13). Ainda segundo o autor, na sociedade de vigilância digital, o *Big Brother* é substituído pelo *big data*. Nesse sentido, partindo-se da premissa de que a privacidade é o *locus* constitucional adequado da proteção de dados (Mulholland; Frajhof, 2019, p. 270), a confusão entre público e privado ocasionada pela expansão tecnológica ocasiona interferências diretas não somente ao direito à privacidade, mas também ao direito à proteção de dados pessoais.

2.2 As implicações das tecnologias de vigilância no desenvolvimento da personalidade humana

Fato é que, em uma sociedade digital, o tratamento de dados tem se tornado cada vez mais expansivo, impactando cada vez mais pessoas e realidades sociais. Nesse contexto, a proteção de dados pessoais ergue-se como a tutela da "própria dimensão relacional da pessoa humana", pois existe um leque vasto de liberdades individuais relacionadas à proteção de dados pessoais, que extrapolam os limites de tutela do direito à privacidade, uma vez que este é atrelado a uma divisão das esferas pública e privada de seus titulares (Bioni, 2018, p. 99). De acordo com Doneda *et al.* (2018), "a estreita relação entre o desenvolvimento mais recente dos mecanismos de inteligência artificial com a maior disponibilidade de informação deixou seus reflexos na regulação que começou a ser concebida em relação à proteção de dados pessoais". Ainda segundo os autores, o desenvolvimento e a implementação de tecnologias de inteligência artificial (IA) proporcionaram efeitos que "implicam uma mudança na subjetividade das relações entre as pessoas e a tecnologia" (Doneda *et al.*, 2018, p. 2).

Nesse contexto, especialmente em relação ao tema aqui tratado, é importante apontar que o "fato de participarmos desta época é suficiente para que soframos constante vigilância, através de câmeras, sensores e o monitoramento dos dados que produzimos diariamente, seja em redes sociais, ou através do uso dos dispositivos conectados à Internet das coisas (IoT)" (Souza, 2018, p. 577). Isso significa que, voluntária ou involuntariamente, vivemos sob o constante monitoramento possibilitado pelo avanço tecnológico. Voluntariamente, pois em diversas ocasiões cedemos "livremente" nossos dados pessoais ao governo e a corporações privadas; involuntariamente, pois em diversas outras encontramo-nos ostensivamente vigiados, sem que a nós seja dada a oportunidade de consentirmos no que diz respeito a tal vigilância.

Para Han, somos "prisioneiros de uma memória total de caráter digital" (2018b, p. 86). Enquanto o pan-óptico vislumbrado por Bentham carecia de um sistema de registro eficiente, pois contava apenas com o livro das punições disciplinares que listava os castigos aplicados e suas causas, e o *Big Brother* de Orwell era incapaz de manter o registro da vida das pessoas, os *big data* possibilitam o armazenamento virtualmente infinito de informações. Assim, "já por esse motivo, o pan-óptico digital é mais eficiente do que o benthamiano" (Han, 2018b, p. 86).

Evidentemente, existem "muitas boas razões que sustentam a necessidade de usar todas as oportunidades oferecidas pelas novas tecnologias para proteger a sociedade dos crimes", devendo-se "buscar o equilíbrio entre a visão individualista da privacidade e a satisfação das demandas da sociedade" (Rodotà, 2008, p. 147). Norris aponta que determinados autores argumentam no sentido de que é a primeira vez na história que temos a oportunidade de experimentar formas de controle que não levam em consideração nenhuma categoria de divisão social, sendo critérios como idade, sexo, raça, beleza e vestuário considerados irrelevantes (Norris, 2003, p. 276). Contudo, é importante que se analisem tais argumentos com certa cautela. Há de se considerar que "os riscos da sociedade da vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos", sendo que o escopo da vigilância torna-se constante em cada momento da vida, apresentando-se como "um traço próprio das relações de mercado, cuja fluidez diz respeito à possibilidade de dispor livremente de um conjunto crescente de informações" (Rodotà, 2008, p. 113).

Considerando-se, também, que os avanços tecnológicos, principalmente a partir do recente desenvolvimento de técnicas de IA, implicam mudanças na subjetividade das relações entre o ser humano e a tecnologia (Doneda *et al.*, 2018) e que, como aponta Rodotà (2008, p. 113), as tecnologias da comunicação e da informação naturalmente entram em conflito com o direito de construir livremente a própria esfera privada (entendida como autodeterminação informativa, como poder de controlar a circulação das próprias informações), é necessário que se reestruture a noção de cidadania, dentro da qual se encontra a ideia de privacidade.

Para tanto, é imprescindível endereçar e analisar os problemas que despontam, inevitavelmente, com a consolidação da sociedade da vigilância e da classificação. Uma das principais questões – como expõem Rodotà (2008), Norris (2003), Lianos e Douglas (2000), entre outros – é a utilização das informações pessoais para a construção de perfis individuais ou de grupo, pois "as informações utilizadas são, de fato, sempre parciais e incompletas, mesmo quando se recorre a uma multiplicidade de bancos de dados" (Rodotà, 2008, p. 115). Ademais, os sistemas de vigilância baseados em reconhecimento facial, inclusive os mais modernos, são profundamente simples, redutivos, pois não utilizam outra lógica senão aquela que houver sido inserida em seu *software* por um programador humano, e o ponto final desse processamento é a criação de um sistema binário de classificação: o acesso é aceito ou negado; a identidade é confirmada ou rejeitada; o comportamento é legítimo ou ilegítimo (Norris, 2003, p. 276).

Isso gera implicações fundamentais para a base normativa do controle social. Explica-se: o controle que se realiza presencialmente não é absoluto, mas sim baseado em uma análise moral complexa de caráter, que avalia o comportamento, a identidade, a aparência e o comportamento da pessoa por meio das lentes de relevância específica do contexto. Mais importante ainda, como argumentam Lianos e Douglas (*apud* Norris, 2003, p. 276), é que tal controle é negociado, sendo que essa negociação tem uma função moral e educativa crucial, pois é por meio da negociação e da aprovação e desaprovação que os valores sociais são aprendidos e reforçados, uma vez que a classificação realizada por sistemas inteligentes de vigilância e controle não se baseia em avaliação moral diferenciada e multifacetada, mas no elemento único de mediação que o sistema reconhece. Em outras palavras, não há indivíduos bons e ruins, honestos e desonestos, pobres ou ricos: existem simplesmente detentores ou não detentores da possibilidade acesso e ingresso a determinados lugares, bens e serviços (Norris, 2003, p. 276-277).

Aqueles favoráveis ao emprego de tecnologias de reconhecimento para fins de vigilância e controle argumentam que o uso de tais tecnologias possibilitaria uma vigilância "democrática", em comparação aos sistemas tradicionais de vigilância, face a face, presenciais. Contudo, como demonstra estudo realizado por Norris e Armstrong (*apud* Norris, 2003, p. 266), os jovens, homens e pessoas negras são alvo de maneira sistemática e desproporcional de sistemas de vigilância, não por causa de seu envolvimento em crimes ou desordens, mas por "nenhuma razão óbvia" e com base apenas em suspeitas categóricas. Essa diferenciação, segundo os autores, não se baseia em critérios objetivos e comportamentais e individualizados, mas apenas no fato de pertencerem a um grupo social específico, o que torna essas práticas discriminatórias.

Além disso, ainda segundo Norris (2003, p. 277), se os sistemas de vigilância não são universais em sua aplicação, existe um risco real de que eles sejam empregados de forma discricionária; nesse caso, comunidades específicas estão sujeitas a um monitoramento intensivo e extensivo centrado na punição, enquanto outras estão sujeitas a uma vigilância mais "favorável". Observe-se, por exemplo que esses sistemas não são projetados para identificar um furto, mas sim para reconhecer um invivíduo previamente classificado como praticante de tal delito. Um sistema de vigilância poderia ser utilizado para solicitar que a equipe de segurança de determinada loja concentre sua vigilância naquele indivíduo especificamente, na esperança de capturá-lo "em ação" (Norris, 2003, p. 278). As tecnologias de reconhe-

cimento facial parecem ser o "estopim de uma demanda regulatória represada em torno de inteligência artificial de uma maneira geral", pois não faltam evidências sobre os altos índices de falso positivos e, principalmente, revelações em torno do reforço de práticas discriminatórias a partir do seu emprego para fins de policiamento preditivo (Bioni; Luciano, 2019).

Todo esse contexto gera implicações diretas não apenas no comportamento de uma pessoa, mas principalmente no que concerne ao respeito a sua identidade, cuja própria construção passa a ser definida por algoritmos. Isso porque, atualmente, "corpos anônimos podem ser transformados em sujeitos digitais, identificados e relacionados às suas personas digitais que residem em bases de dados eletrônicas" (Norris, 2003, p. 278)[10], o que pode ocasionar violações à privacidade, aqui considerada como o direito da pessoa de escolher aquilo que está disposta a revelar às demais, bem como o direito de se prevenir de danos causados pelo processamento de informações. Ademais, a privacidade, no âmbito da comunicação eletrônica, pode manifestar como a necessidade de anonimato, requerendo-se assim "a tutela de uma identidade nova, de uma intimidade construída, como condição necessária para o desenvolver a própria personalidade, para alcançar plenamente a liberdade existencial" (Rodotà, 2008, p. 116).

Sem embargo, a vigilância e o controle são partes inerentes da comunicação digital (Han, 2018a), e a tendência que se observa em grande parte da sociedade é de não apenas aceitar, mas apoiar as tecnologias de vigilância, que se fazem cada vez mais presentes no cotidiano das pessoas, apresentando-se como inquestionáveis devido à suposta segurança que oferecem. Esse movimento, todavia, gera o "assujeitamento" da sociedade, culminando, por fim, em uma armadilha perigosa para os próprios indivíduos, que consentem silenciosamente com os dispositivos de vigilância, sem perceber que "essas invasões constantes em sua esfera de intimidade acabam por desapropriá-los de seu espaço de construção de identidade e, consequentemente, do valor dignidade que lhe é devido" (Baião; Gonçalves, 2014).

Segundo Han (2018a), essa conjuntura implica uma mudança de paradigma, no qual o panóptico digital apresenta-se não como uma sociedade disciplinar biopolítica, tal qual posto por Foucault (1996), mas sim como uma "sociedade da transparência psicopolítica"; no lugar do biopoder,

10 No original: "*Anonymous bodies can be transformed into digital subjects, identified and linked to their digital personae residing in electronic databases*" (Norris, 2003, p. 278).

assume importância o psicopoder. Como aponta o autor, a psicopolítica, somada à vigilância digital, adquire a capacidade de ler e controlar pensamentos, e, consequentemente, influenciar o comportamento das pessoas. Nesse processo, "a vigilância digital toma o lugar da ótica inconfiável, ineficiente e perspectivista do *Big Brother*" (Han, 2018a, p. 130, 131), sendo eficiente justamente por ser aperspectivista, e pelo fato de o psicopoder possuir condições de intervir nos processos psicológicos.

No que tange à coleta e uso de dados, expõe o autor sul-coreano que

> o *data-mining* torna visíveis os modelos coletivos de comportamento dos quis não se está, enquanto indivíduo, nem sequer consciente. Assim, ele torna acessível o inconsciente-coletivo. Em analogia ao inconsciente-ótico, pode-se também chamá-lo de inconsciente-digital. O psicopoder é mais eficiente do que o biopoder na medida em que vigia, controla e influencia o ser humano não de fora, mas sim a partir de dentro. A psicopolítica se empodera do comportamento social das massas ao acessar a sua lógica inconsciente. A sociedade digital de vigilância, que tem acesso ao inconsciente-coletivo, ao comportamento social futuro das massas, desenvolve traços totalitários. Ela nos entrega à programação e ao controle psicopolíticos. A era da biopolítica está, assim, terminada. Dirigimo-nos, hoje, à era da psicopolítica digital. (Han, 2018a, p. 134)

2.3 Vigilância x transparência

Outro aspecto a ser considerado concerne à transparência na coleta de dados pessoais por meio de tecnologias de vigilância, bem como ao acesso que o indivíduo possui a esses dados. A proteção de dados não pode mais se referir a algum aspecto especial, por mais relevante que seja. É imprescindível que sejam postas em operação estratégias integradas, capazes de regular a circulação de informações em seu conjunto (Rodotà, 2008, p. 50), ganhando destaque o "direito de acesso", que é, "antes de tudo, um instrumento diretamente acionável pelos interessados, que podem utilizá-lo não somente com a finalidade de simples conhecimento, mas também para promover propriamente a efetividade" de princípios relacionados à proteção de dados pessoais (Rodotà, 2008, p. 60).

Rodotà defende que deve ser concedido à pessoa o poder de controle direto e contínuo sobre os coletores de informações, independentemente da existência de uma violação a seus direitos, alterando-se assim a técnica de proteção da privacidade e deslocando-se a atenção em direção ao bom funcionamento das regras sobre a circulação de informações. O direito ao acesso tem por objetivo, primeiramente, reforçar a posição dos indivíduos,

para suprir, "no limite do possível, o *gap* de poder entre estes e os 'senhores da informação'" (Rodotà, 2008, p. 68). O direito de acesso configura-se, portanto, como "um instrumento capaz de determinar formas de redistribuição de poder" (Rodotà, 2008, p. 73).

Conquanto esse seja o cenário ideal, a realidade tem demonstrado que os indivíduos têm se tornado cada vez mais "transparentes" – cada vez mais submetidos à vigilância – e que os órgãos públicos possuem cada vez menos controle político e legal no que tange aos dados pessoais dos cidadãos (Rodotà, 2013). Nesse sentido e a título exemplificativo, Barros e Venturini, em análise sobre o município do Rio de Janeiro, expõem que "as atividades do Estado – inclusive na área de segurança pública e vigilância – seguem secretas e pouco sujeitas a escrutínio público, enquanto os cidadãos encontram-se cada vez mais expostos tanto frente ao próprio Estado, quanto a outros agentes privados" (Barros; Venturini, 2018, p. 43)

Ademais, Mulholland e Frajhof questionam os sistemas de IA dotados de *machine learning*[11], apontando que um favor a se levar em consideração em sistemas de autoaprendizagem "é justamente o fato de que a transparência dos métodos utilizados e, consequentemente, dos resultados alcançados fica deslocada, abrindo espaço para uma opacidade típica de sistemas autoritários não regulados" (2019, p. 272, 273). Dessa maneira, reitera-se a importância de um dos principais elementos da proteção de dados: o direito de acesso, que significa o poder incondicional que a pessoa deve ter de saber *quem* possui *quais* dados sobre ela/ele e *como* esses dados são usados (Rodotà, 2013). Permitir que as pessoas conheçam quais tecnologias de informação são empregadas pelo Estado, quais são as práticas de vigilância e como se dá o recolhimento, uso e distribuição de seus dados significa, portanto, "dar ao cidadão a garantia do exercício do controle social sobre a administração pública" (Barros; Venturini, 2018, p. 43), o que, no fim, configura-se como o exercício de tal direito.

Considerando-se que o emprego de tecnologias de reconhecimento facial demanda o processamento de dados pessoais, a tendência é que essas questões sejam endereçadas em leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) brasileira (Lei nº 13.709/2013), que entrará em vigor em agosto de 2020, e a Regulação Geral de Proteção de Dados da

11 *Machine learning* (traduzido como "aprendizado de máquina") é uma área da ciência da computação, no campo da inteligência artificial. *Grosso modo*, é uma modalidade de programação usada nos computadores, formada por regras previamente definidas que permitem que os computadores tomem decisões com base nos dados prévios e em dados gerados e/ou empregados pelo usuário.

União Europeia (GDPR). A título exemplificativo, pode-se mencionar o fato de ambas as legislações preverem a possibilidade do direito à explicação, que se revela, afinal, como concretização do princípio da transparência. A transparência, embora fundamental, não se revela como único princípio a ser observado.

Ressalva-se que a LGPD, em seu art. 4º, III, estipula que seus dispositivos não regulam o tratamento de dados no que tange aos fins exclusivos para segurança pública, defesa nacional, segurança do Estado, ou de atividades de investigação e repressão das infrações penais. O objetivo dessa limitação é a garantia do interesse público de combater infrações penais, crime organizado, fraude digital, ou até mesmo terrorismo. No entanto, a inaplicabilidade da LGPD nesses contextos não é absoluta, visto que o § 1º do mesmo artigo determina que os princípios gerais de proteção ao titular de dados continuarão norteando qualquer esfera de tratamento, até mesmo em contextos de interesse público. Assim, os princípios da finalidade, adequação, necessidade, transparência e não discriminação, assim como os direitos de acesso aos dados, correção, anonimização e eliminação das informações inadequadas (dispostos nos arts. 6º, 17 e 18 da referida lei), continuam servindo como formas de garantia dos direitos fundamentais dos titulares de dados e impedindo tratamentos irregulares de dados por parte do Poder Público.

2.4 A importância do princípio da precaução

Há de se ter em mente, também, que problemas decorrentes de *biased artificial intelligences* – algoritmos enviesados – são mais comuns do que deveriam, o que ocorre por diversas razões, como a falta de regulação, monopólios no setor de IA, assimetrias de poder entre empresas e usuários, a distância cultural entre os responsáveis por pesquisas em tecnologia e a diversidade das populações nas quais essa tecnologia é utilizada (Norris, 2003; Bioni; Luciano, 2019). Isso parece "indicar o abismo entre desenvolvedores desse tipo de tecnologia e aqueles que são impactados por ela" (Bioni; Luciano, 2019, p. 208), o que tem levado à maior demanda social no que tange à transparência e à precaução na utilização de tecnologias de IA (Floridi *et al.*, 2017).

Segundo Bruno R. Bioni e Maria Luciano, "o princípio da precaução fornece um substrato importante para se pensar medidas e estratégias de regulação de IA, notadamente como lidar com situações de riscos de danos ou de desconhecimento dos potenciais malefícios e benefícios desse tipo de tecnologia" (2019, p. 228). O desenvolvimento recente de tecnologias de

informação e comunicação (TICs) tornou ainda mais patentes os potenciais danos e violações a direitos decorrentes do tratamento (indevido) de dados pessoais. Assim, tornou-se mais complexo o processo de cognição, avaliação e gerenciamento dos riscos de uma economia de dados, sendo que os aqueles que detêm os dados passaram a deter também uma "superioridade informacional ainda maior frente aos demais atores cidadãos e órgãos fiscalizadores desse ecossistema" (Bioni; Luciano, 2019, p. 216).

Especialmente em relação à utilização de reconhecimento facial baseado em IA, as incertezas quanto aos benefícios e aos riscos revelam-se mais evidentes, pelos diversos motivos expostos anteriormente. No que concerne às possibilidades de regulamentação de tais tecnologias, é possível apontar três entendimentos distintos, comparáveis e diferenciáveis devido à carga de atribuição de obrigações precaucionárias diante das incertezas e dos benefícios de seu uso. Num extremo, parte do setor privado acredita em uma "tecnorregulação", suprida pelas diretrizes éticas do mercado, que evitaria entraves ao desenvolvimento de tecnologias de reconhecimento facial. Na outra extremidade, busca-se o banimento total das *FRTs*, sob o argumento de que haveria, em seu próprio *design*, um risco desproporcional de opressão e discriminação. "Ao centro desse movimento pendular, encontra-se uma estratégia que visa desenhar uma arquitetura precaucionária de danos", que indica que o emprego de tecnologias de reconhecimento facial deveria ser antecedido de ações por parte do seu próprio proponente, capazes de mitigar seus eventuais malefícios (Bioni; Luciano, 2019, p. 221-222).

Independente de qual caminho seja adotado, é preciso considerar que tecnologias de IA, principalmente aquelas que se baseiam na análise de dados, não são completamente objetivas e neutras. Tais sistemas "carregam escolhas das entidades e pessoas envolvidas na sua construção, sendo modulado pela agenda política e aspectos socioeconômicos, de forma implícita ou explícita, que lhes são subjacentes" (Bioni; Luciano, p. 228). Nesse sentido,

> o princípio da precaução apresenta dois vetores de regulação que merecem atenção: a) a abertura do debate regulatório a todos os atores envolvidos na implementação dessa tecnologia (e nas escolhas que ela impõe), de desenvolvedores àqueles que sofrerão seus possíveis efeitos, o que é um requisito obrigatório de um sistema democrático com históricas dinâmicas de assimetria de poder e informação; b) a atribuição de obrigações que reduzam as incertezas quanto aos benefícios e riscos em questão, de sorte a determinar a adoção ou não de IA. (Bioni; Luciano, p. 228)

CONSIDERAÇÕES FINAIS

Em uma conjuntura de crescentes avanços tecnológicos, característica das sociedades digitais, os sistemas de vigilância que empregam tecnologias de reconhecimento facial tornam-se cada vez mais presentes no cotidiano de bilhões de pessoas, configurando um verdadeiro pan-óptico digital. Alimentados por tecnologias de inteligência artificial, *big data*, e impulsionados pela internet das coisas, tais sistemas potencializam a ocorrência de violações ao direito à privacidade, bem como ao direito à proteção de dados, conforme se buscou demonstrar. Ademais, os sistemas de vigilância não apenas significam uma "ameaça" à privacidade e à proteção de dados de maneira geral, mas também ocasionam a violação ainda mais patente de tais direitos em se tratando de determinadas pessoas e grupos sociais.

Inegavelmente, o progresso tecnológico pode proporcionar benefícios sociais inimagináveis há até pouquíssimo tempo. Tampouco se pode negar a irrefreabilidade de tal progresso, mesmo que este não se apresente com prognósticos somente positivos. Portanto, torna-se crucial uma ponderação acerca dos interesses em jogo, para assegurar a coexistência da garantia dos direitos individuais, com a progressiva abertura da sociedade, sempre em consonância com a participação pública e com debates abertos sobre as garantias e limitações que se mostrarão necessárias para que novas tecnologias sejam implementadas.

Assim, considerando-se que muitas de nossas interpretações do mundo e ações são moldadas pelas tecnologias que utilizamos, mostram-se necessárias novas formas de tratamento jurídico da privacidade e da proteção dos dados pessoais. Enquanto cresce a preocupação político-institucional no tocante à proteção de dados e informações pessoais, torna-se uma tarefa cada vez mais árdua o respeito a essa presunção geral, o que se dá por motivos como as constantes exigências de segurança pública, os interesses de mercado e a reorganização da Administração Pública.

Especialmente no que se refere ao uso de tecnologias de reconhecimento facial baseadas em inteligência artificial, é imprescindível ter-se em mente que seu desenvolvimento e emprego deverão respeitar os princípios elencados nas legislações sobre a proteção de dados pessoais, que hoje se apresentam como um substrato regulatório para tal matéria. Somadas a elas, leis setoriais de dados biométricos e de reconhecimento facial certamente serão desenvolvidas, e apresentar-se-ão como instrumentos precautórios a

serem analisados, tendo-se em vista a preservação do direito à privacidade e do direito à proteção de dados pessoais.

REFERÊNCIAS

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*. Rio de Janeiro, a. 3, n. 2, jul./dez. 2014. Disponível em: <http://civilistica.com/wp-content/uploads/2015/02/Baião-e-Gonçalves-civilistica.com-a.3.n.2.2014.pdf>. Acesso em: 23 jun. 2019.

BARROS, Marina; VENTURINI, Jamila. Os desafios do avanço das iniciativas de cidades inteligentes nos municípios brasileiros. In: MAGRANI, Eduardo (Org.). *Horizonte presente*: debates de tecnologia e sociedade. 1. ed. Rio de Janeiro: Letramento, v. 1, 2019.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

_____; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

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

_____ et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018.

EGGERS, W.; SCHATSKY, D.; VIECHNICKI, P. AI-augmented government: using cognitive technologies to redesign public sector work. [s.l.], 2017. Disponível em: <https://www2.deloitte.com/insights/us/en/focus/cognitive-technologies/artificial-intelligence-government.html>. Acesso em: 5 ago. 2018.

FAULKNER, Wendy. The technology question in feminism: a view from feminist technology studies. *Women's Studies International Forum*, v. 24, n. 1, p. 79-95, 2001.

FLORIDI, L. Soft ethics, the governance of the digital and the General Data Protection Regulation. Philosophical transactions of the royal society a mathematical physical and engineering sciences. Disponível em: <https://www.researchgate.net/publication/328292318_Soft_ethics_the_governance_of_the_digital_and_the_General_Data_Protection_Regulation>. Acesso em: 23 jun. 2019.

_____; TADDEO, M. What is data ethics? Philosophical transactions of the royal society a mathematical physical and engineering sciences. 2016. Disponível em: <https://www.researchgate.net/publication/310393920_What_is_data_ethics>. Acesso em: 23 jun. 2019.

_____ et al. Artificial intelligence and the "Good Society": the US, EU, and UK approach. *Science and Engineering Ethics*, Springer, p. 1-24, 2017.

FONSECA, J. J. S. *Metodologia da pesquisa científica*. Fortaleza: UEC, 2002. Apostila.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. 14. ed. Petrópolis: Vozes, 1996.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2007.

GOVERNO DO ESTADO DA BAHIA. Lançado sistema de videomonitoramento inteligente de segurança. Disponível em: <http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html>. Acesso em: 20 ago. 2019.

HAN, Byung-Chul. *No enxame*: perspectivas do digital. Trad. Lucas Machado. Petrópolis: Vozes, 2018a.

_____. Psicopolítica: o neoliberalismo e as novas técnicas de poder. Trad. Maurício Liesen. Belo Horizonte: Âyiné, 2018b.

LENTINO, Amanda. This Chinese facial recognition start-up can identify a person in seconds. Disponível em: <https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html>. Acesso em: 20 ago. 2019.

MADDEN, Mary. Privacy, security, and digital inequality: how technology experiences and resources vary by socioeconomic status, race, and ethnicity. Disponível em: <https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf>. Acesso em: 23 jun. 2019.

MARX, Gary T. Murky conceptual waters: The public and the private. *Ethics and Information Technology*, v. 3, n. 3, p. 157-169, 2001.

MCCARTHY, J. What is artificial intelligence? Stanford, 2000. Disponível em: <http://www-formal.stanford.edu/jmc/whatisai.pdf>. Acesso em: 5 ago. 2018.

MEHR, H. Artificial intelligence for citizen services and government. [s.l.], 2017. Disponível em: <https://ash.harvard.edu/files/files/artificial_intelligence_for_citizen_services.pdf>. Acesso em: 5 ago. 2018.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

_____. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. *Jota*, [s.l.], 10 maio 2020. Disponível em: <www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020>. Acesso em: 27 jun. 2020.

MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IOT). In: MAGRANI, Eduardo (Org.). *Horizonte presente*: debates de tecnologia e sociedade. 1. ed. Rio de Janeiro: Letramento, v. 1, 2019.

_____; FRAJHOF, Isabella Z. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). *Inteligência artificial e Direito*: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

NABEEL, Fahad. Regulating facial recognition technology in public places. *Centre for Strategic and Contemporary Research*, 2019. Disponível em: <https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places>. Acesso em: 20 jul. 2019.

NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. *Surveillance as social sorting*: privacy, risk, and digital discrimination. Routledge: New York, 2003.

PREFEITURA DO RIO DE JANEIRO. *Rio+Seguro*. Disponível em: <http://maisseguro.rio>. Acesso em: 20 ago. 2019.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018.

RICHARDS, N. M.; SMART, W. D. How should the law think about robots?, 2013. Disponível em: <https://ssrn.com/abstract=2263363>. Acesso em: jan. 2018.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

_____. Some Remarks on Surveillance today. *European Journal of Law and Technology*, Vol. 4, No. 2, 2013. Disponível em: <http://ejlt.org/article/view/277/388>. Acesso em: 20 ago. 2019.

SOUZA, Renato Rocha. Sobre a ética humana e a ética dos algoritmos. In: MAGRANI, Eduardo (Org.). *Horizonte presente*: debates de tecnologia e sociedade. 1. ed. Rio de Janeiro: Letramento, v. 1, 2019.

THUY, Ong. Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints. Disponível em: <https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium>. Acesso em: 20 ago. 2019.

VERBEEK, P. Morality in design: design ethics and the morality of technological artifacts. In: VERMAAS, Pieter E.; KROES, Peter; LIGHT, Andrew; MOORE, Steven A. (Eds.). *Philosophy and Design*: from Engineering to Architecture. Dordrecht: Springer, p. 91-103, 2008.

VU, Brandon. A technological and ethical analysis of facial recognition in the modern era. In: *A Technological and Ethical Analysis of Facial Recognition in the Modern Era*, 2018. Disponível em: <https://www.academia.edu/38066258/A_

Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era>. Acesso em: 20 jun. 2019.

WADDELL, Kaveh. Half of American Adults Are in Police Facial-Recognition Database. Disponível em: <https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/>. Acesso em: 20 ago. 2019.

WEBER, Rolf H. Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, v. 26, n. 1, p. 23-30, 2010.

WECHSLER, H. *Reliable face recognition methods*: system design, implementation and evaluation. Springer, 2007.

Sobre os autores:

Sergio Marcos Carvalho de Ávila Negri | *E-mail*: smcnegri@yahoo.com
Professor Adjunto do Departamento de Direito Privado da Faculdade de Direito da Universidade Federal de Juiz de Fora – UFJF e do Corpo Permanente do Programa de Pós-Graduação *Stricto Sensu* em Direito e Inovação da Faculdade de Direito da UFJF, Especialização em Direito Civil pela Università degli Studi di Camerino – Itália, Mestrado (2006) e Doutorado (2011) em Direito Civil pela Universidade do Estado do Rio de Janeiro.

Samuel Rodrigues de Oliveira | *E-mail:* samuelrdeoliveira@gmail.com
Mestre (2020) e Bacharel (2017) em Direito pela Universidade Federal de Juiz de Fora.

Ramon Silva Costa | *E-mail*: ramoncostta@outlook.com
Mestre em Direito pela Universidade Federal de Juiz de Fora (2020), Bacharel em Direito pela Universidade Federal Fluminense (2017).

Data da submissão: 1º de outubro de 2019.
Data do aceite: 6 de julho de 2020.