Revista de Direito, Governança e Novas Tecnologias

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 23.11.2019
Aprovado em: 07.12.2019

O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL EM SISTEMAS DE VIGILÂNCIA E SUAS IMPLICAÇÕES NO DIREITO À PRIVACIDADE

Ramon Silva Costa[*]
Samuel Rodrigues de Oliveira[**]

RESUMO:
O presente trabalho tem como objetivo analisar as implicações do desenvolvimento e da utilização de tecnologias de vigilância facial baseados em inteligência artificial no direito à privacidade. Metodologicamente, trata-se de pesquisa exploratória, realizada por meio de levantamento bibliográfico. Adota-se como principal referencial teórico os conceitos de Stefano Rodotà sobre a sociedade da vigilância e da classificação. Conclui-se haver a necessidade de redefinição do conceito clássico de privacidade, de modo a abarcar as transformações sociais promovidas pela tecnologia bem como a proteção de dados enquanto direito autônomo.

Palavras-chave: pessoa e mercado; privacidade; proteção de dados; reconhecimento facial; vigilância.

THE USE OF FACIAL RECOGNITION TECHNOLOGY IN SURVEILLANCE SYSTEMS AND ITS IMPLICATIONS ON THE RIGHT TO PRIVACY

ABSTRACT:
This paper aims to analyze the implications of the development and use of artificial intelligence-based facial control technology on the right to privacy. Methodologically, it is an exploratory research, conducted through bibliographic survey. We adopt as the main theoretical framework Stefano Rodotà's work on the society of surveillance and social sorting. We support there is a need to redefine the classic concept of privacy to encompass as social transformations promoted by technology and as well as data protection as an autonomous right.

Keywords: data protection; facial recognition; legal entity and market; privacy; surveillance.

1 INTRODUÇÃO

Na sociedade contemporânea, a informação é elemento nuclear para o desenvolvimento humano, configurando nova forma de organização social, sedimentada pela

[*] Graduado em Direito pela Universidade Federal Fluminense (UFF) e mestrando bolsista CAPES em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF).
Endereço eletrônico: ramoncostta@outlook.com. Endereço postal: Rua José Lourenço Kelmer, s/n, Faculdade de Direito- UFJF, São Pedro. CEP: 36036-900- Juiz de Fora-MG
[**] Graduado em Direito e mestrando em Direito e Inovação pela Universidade Federal de Juiz de Fora (UFJF). Endereço eletrônico: samuelrdeoliveira@gmail.com. Endereço postal: Rua José Lourenço Kelmer, s/n – Faculdade de Direito, São Pedro. CEP: 36036-900 - Juiz de Fora- MG.

evolução tecnológica que criou mecanismos capazes de processar e transmitir informações de modo cada vez mais veloz (BIONI, 2018). Se no passado éramos essencialmente uma sociedade presencial, hoje nos tornamos também uma sociedade digital, o que implica sociabilidades amplamente mediadas por tecnologias que fomentam as relações de mercado, pessoais, econômicas, culturais e até mesmo de vigilância, o que se dá por meio da expansão do ciberespaço (LEVY, 2000; RODOTÀ, 2008). Tal expansão possibilitou a comunicação digital, que surge da interconexão mundial dos computadores e que se amplia de forma exponencial a partir dos avanços tecnológicos, gerando uma verdadeira "galáxia da internet" (CASTELLS, 2003).

Nesse cenário, a inteligência artificial (IA) desponta como um nicho tecnológico de indescritível ubiquidade, sendo aplicada nas mais diversas áreas do cotidiano (RICHARDS, 2013), o que faz com que questões éticas atinentes à tecnologia ganhem cada vez mais atenção e importância. Concomitantemente ao desenvolvimento de tecnologias de IA, alicerçado por fatores como a existência de métodos estatísticos e probabilísticos cada vez mais sofisticados e disponibilidade de um número expansivo de dados (FLORIDI et al., 2017), ocorreram mudanças paradigmáticas e substanciais das noções de democracia e direitos fundamentais, o que gerou um aumento de funções estatais, culminando na transformação do próprio Estado, que passou a assumir demandas mais complexas e em maior número, gerando uma tendência mundial de implementar atividades e serviços públicos, inclusive aqueles de vigilância, estruturados por sistemas de IA (EGGERS, SCHATSKY e VIECHNICKI, 2017; MEHR, 2017).

Ao redor do globo, não faltam exemplos de como a IA tem sido aplicada a sistemas de reconhecimento facial. 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. Na capital dos Emirados Árabes Unidos, Dubai, um gigantesco aquário localizado no principal aeroporto da cidade conta com mais de 80 câmeras de segurança, que escaneiam e analisam o rosto das pessoas à medida que caminham por ele; por fim, o sistema ou permite que a pessoa ingresse livremente no país, ou emite um alerta de segurança. Nos EUA, no ano de 2016, ao menos 50% dos cidadãos adultos já constavam em bases de dados de reconhecimento facial do governo.

No Brasil, destaca-se o chamado "RIO+SEGURO", "um programa pioneiro no Brasil que associa planejamento, inteligência e tecnologia na prevenção à desordem urbana e à criminalidade", conforme consta do sítio eletrônico do projeto. A inteligência e tecnologia a que se referem a descrição do programa correspondem, na realidade, ao uso de *software* de reconhecimento facial baseado em IA, a fim de se identificar e, consequentemente, prender suspeitos e foragidos. No estado da Bahia, igualmente, tem ganhado força o projeto intitulado "Vídeo Policiamento", que emprega inteligência artificial às ações de videomonitoramento efetuadas em âmbito estadual. 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".

Diante de tal conjuntura, considerando-se que o mero fato de participarmos da sociedade atual é suficiente para que soframos constante vigilância, através de câmeras, sensores e o monitoramento dos dados que fornecemos diariamente, apresenta-se o seguinte problema: quais são as implicações do desenvolvimento e da utilização de sistemas de vigilância facial baseados em IA no direito à privacidade? Objetiva-se, de forma geral, compreender de que maneiras as novas tecnologias de vigilância afetam aquilo que se compreende por "vida privada". De maneira mais específica, procura-se analisar e entender o funcionamento de tais tecnologias, discutir a conceituação e evolução do direito à privacidade na chamada "sociedade da vigilância", e, por fim, debater a influência e as implicações que o recente avanço tecnológico exerce sobre esse direito.

Metodologicamente, devido à natureza do tema abordado na presente pesquisa, é possível classificá-la, no que tange a seus objetivos, como uma pesquisa exploratória. Segundo Gil (2007), esse tipo de pesquisa objetiva proporcionar maior familiaridade com o problema, a fim de torná-lo mais explícito ou a construir hipóteses. Ainda segundo o autor, a grande maioria dessas pesquisas envolve o levantamento bibliográfico, método que será majoritariamente adotado no presente trabalho. A pesquisa bibliográfica é feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos e páginas de sítios eletrônicos. 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). Diante da relativa novidade do tema aqui abordado, e da 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.

2 A INTELIGÊNCIA ARTIFICIAL E AS TECNOLOGIAS DE RECONHECIMENTO FACIAL E VIGILÂNCIA

Inexiste um consenso na literatura especializada sobre o conceito de inteligência artificial, mas é possível afirmar, em linhas gerais, tratar-se 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 (I.A) ao se fazer com que uma máquina se comporte de maneira que, caso se tratasse de um ser humano, fosse considerada inteligente (MCCARTHY, 2000).

Destaca-se que o atual entusiasmo no que diz respeito à pesquisa e desenvolvimento de tecnologias de inteligência artificial teve início aproximadamente em 2010, e foi movido pelos seguintes fatores: 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 (FLORIDI et al., 2017). Tais fatores, que se retroalimentam, possibilitaram o crescimento exponencial da criação e aperfeiçoamento de sistemas de IA nos últimos anos, não aparentando ser uma tendência passageira.

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).

Nessa lógica, Rodotà (2008) 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 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).

Como se pode observar, é interessante para os gestores públicos o uso de novas tecnologias alimentadas pelo *big data*, processamento de grandes volumes 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"; Nesse sentido, expõe Caitlin Mulholland:

> É no âmbito da tecnologia conhecida como Internet das Coisas – ou *Internet of Things*, ou, ainda, IoT – que se desenvolve o argumento desta perspectiva, revelando um dos principais debates que se realiza neste âmbito e que se refere à proteção da privacidade ou dos dados pessoais que são disponibilizados e coletados por estas "coisas" conectadas. Em poucas palavras, a IoT representa inovação tecnológica que permite a criação de ambiente interligado através de sensores que conectam objetos ou bens por meio da internet possibilitando não só a comunicação e realização de funções específicas entre as coisas, como gerando a 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).

Todo esse contexto permitiu o desenvolvimento ainda mais acelerado de tecnologias de reconhecimento facial. O surgimento dessas tecnologias, aponta Vu (2018), foi inicialmente resultado da incapacidade do cérebro humano de processar, memorizar e lembrar-se de milhares de faces com que se depara todos os dias. Contudo, com o aumento de viajantes internacionais ao redor do globo, e especialmente depois dos eventos do 11 de Setembro nos Estados Unidos da América, agências governamentais têm se utilizado de todos os meios para desenvolver maneiras eficientes e precisas de regular o afluxo de pessoas através 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).

O termo "tecnologia de reconhecimento facial" (comumente abreviado como FRT, do inglês, "*facial recognition technology*") refere-se à habilidade que *softwares* de computador possuem de reconhecer e identificar rostos humanos específicos a partir de fotos ou vídeos. Utilizando-se de amplas bases de dados, e valendo-se de conexões de internet ultra velozes, 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 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 armazeandos. 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)[1] desde o século passado alterou fundalmentamente a natureza da *surveillance*, da vigilância ostensiva, tanto quantitativamente

[1] *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.

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 co-presença; o escopo da vigilâncianão mais se restringe Pas 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).[2]

Norris reconhece ainda que a transição para uma sociedade digital resultou na intensificação da sociedade de vigilância. Tradicionalmente, os sistemas inteligentes de vigilância se valiam da tecnologia de reconhecimento facial apenas para fornecer uma confirmação visual de eventos. 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 é realizado por meio de algoritmos, o potencial de conexão com bancos de dados já existentes é dramaticamente amplicado, e "a ligação de informações extraídas de imagens de CFTV a informações relacionadas a identidade em bases de dados exponicialmente aumenta o seu "efeito pan-óptico" (NORRIS, 2003, p. 269- 270).

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 os problemas da vigilância. Antes de tudo, a

[2] No original, "the surveillance gaze has been expanded to a level unimaginable on the basis of co-presence; the surveillance gaze becomes removed from spatial constraints implicit in face-to-face surveillance; the surveillance gaze becomes freed from the temporal constraints of face-to-face interaction and co-presence; surveillance and authoritative intervention become functionally separate; the act of surveillance becomes more democratic: all become equally subject to the surveillance gaze; the disciplinary project of the panopticon is expanded as inclusionary social control is promoted over exclusion. (NORRIS, 2003, p. 253)

vigilância não é apenas o resultado de uma atividade deliberada e específica, mas também um subproduto do comportamento dos mesmos indivíduos, que cedem voluntariamente muitas informações sobre eles. Segundo: 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. Terceiro: a vigilância não visa controlar indivíduos de forma singular, atividades particulares ou segmentos específicos da sociedade, mas está tornando-se um procedimento universal, envolvendo as pessoas em geral. Quarto: os riscos da vigilância não surgem principalmente das atividades dos órgãos de segurança pública, mas da coleta incessante por entes comerciais privados[3]. (RODOTÀ, 2013)

As implicações dessa nova *surveillance* nas questões referentes à privacidade, que geram, por fim, o que Rodotà (2008) denomina "sociedade da classificação", serão melhor endereçadas no tópico seguinte.

4 OS DESAFIOS À PRIVACIDADE NA SOCIEDADE DA CLASSIFICAÇÃO E DA VIGILÂNCIA

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 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 âmbito privado. Ainda que informações da vida íntima sejam compartilhadas com maior ou

[3] No original: "But it's true data the passing to the Web 2.0 implies a fresh approach to the surveillance issues. And this is more and more true if we look at the Web 3.0, the Internet of things. First of all, surveillance is not only the result of a deliberate and specific activity, but also a by-product of the behaviour of the same individuals, leaving voluntarily a lot of informations (sic) about them. Second: surveillance is not only the result of conscious data treatment, but in an increasing number of cases the result of the place given to algorithms. Third: surveillance is not aimed to controlling single individuals, particular activities or specific segments of the society, but is becoming a universal procedure, involving the people at large. Fourth: the risks of the surveillance do not come out especially from the activities of public security agencies, but from the unrelenting collection by private, commercial bodies." (RODOTÀ, 2013)

menor número de pessoas, se restringem ao controle dos indivíduos e ao seu interesse de mantê-las distantes do público em geral.

Nesse contexto, a privacidade pode ser compreendida como o direito de ser deixado só, ou seja, como uma garantia de não violação ou invasão de seus aspectos privativos, assim como o próprio artigo 5º, X da Constituição Federal e o artigo 21 do Código Civil preceituam, ao disporem sobre a inviolabilidade da vida privada (BIONI, 2018, p. 95-96). A privacidade pode ser encarada, então, como um direito guiado pela liberdade negativa de seu titular, que decide sobre quais aspectos de sua vida estão contidos em sua esfera privada e que, portanto, são tutelados por esse direito (RODOTÀ, 2012, p. 320).

Contudo, o entendimento clássico sobre o direito à privacidade como "*the right to be left alone"* revela-se limitado e insuficiente no cenário atual. A própria definição do termo "privacidade" é incerta, sendo utilizado como um termo "guarda-chuva", de conceituação abstrata (SOLOVE, 2008, p. 44). Desse modo, Rodotà destaca a necessidade de ampliação do conceito de direito à privacidade em uma sociedade altamente digitalizada:

> Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem (RODOTÀ, 2008, p. 25).

Esse 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 se consubstancia 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). 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. Assim, mesmo que a proteção de dados esteja relacionada, em alguns aspectos, à tutela da privacidade dos indivíduos, ela não está restrita a dicotomia do público e do privado. Nesse ponto, diferencia-se essencialmente do direito à privacidade, sendo um equívoco dogmático indicar a proteção de dados pessoais como uma mera evolução do direito à privacidade (BIONI, 2018, p. 98-99). Tal cenário justifica a aprovação da Lei Geral de Proteção de Dados (Lei 13.709 de 2018) no Brasil, que não só tutela o direito à privacidade, mas engloba uma série de direitos da personalidade, que podem ser violados em atividades de tratamento de dados pessoais.

Portanto, em uma sociedade digital, o tratamento de dados tem se tornado cada vez mais expansivo e impacta 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 com a proteção de dados pessoais, que extrapolam os limites de tutela do direito à privacidade, pois este é atrelado à 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,

> recentemente, o desenvolvimento e a implementação de tecnologias de inteligência artificial (IA) proporcionou efeitos que, muitas vezes, não podem mais ser compreendidos em termos meramente quantitativos, e que

> implicam uma mudança na subjetividade das relações entre as pessoas e a tecnologia" (DONEDA et al., 2018, p. 2).

Desse modo, especialmente em relação ao tema aqui tratado, *i.e.*, a utilização de sistemas de reconhecimento facial baseados em IA para fins de *surveillance*, é importante apontar que o simples "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 situações encontramo-nos vigiados, sem que a nós seja dada a oportunidade de consentirmos no que diz respeito a tal vigilância.

Rodotà reconhece que "existem evidentemente 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). No mesmo sentido, Norris aponta que determinados autores argumentam a partir da lógica 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 analise tais argumentos com certa cautela. Há que 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". Isso ocasiona a consolidação da imagem do "homem de vidro",

> o verdadeiro cidadão desse novo mundo. Uma imagem que, não por acaso, provém diretamente do tempo do nazismo e que propõe uma forma de organização social profundamente alterada, uma espécie de transformação

> irrefreável da "sociedade da informação" em "sociedade da vigilância" (RODOTÀ, 2008, p. 113).

Considerando-se, também, que os avanços tecnológicos, principalmente a partir do recente desenvolvimento de técnicas de inteligência artificial, 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. Além disso, permanece controversa, e a ser comprovada, a plena validade científica dos modelos usados para produzir novas informações (perfis ou outras) com base em dados coletados. Chega-se assim a "metaconhecimentos" sobre as pessoas, que dificilmente podem ser verificados pelos interessados, embora até embasem decisões sobre eles. Diante dessa nova situação, parece insuficiente a garantia oferecida por algumas legislações, de proibir que decisões judiciais administrativas, que impliquem uma avaliação de comportamento, se baseiem unicamente em elaborações automáticas de informações que forneçam um perfil da personalidade do interessado. Com efeito, os perfis são utilizados para decisões que, para a maioria dos cidadãos são mais freqüentes (sic) e, no mais das vezes, mais significativas do que as judiciais ou administrativas, e que são aquelas que dizem respeito a cidadão consumidor ou usuário de serviços. (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 ocasiona implicações fundamentais para a base normativa do controle social. Explica-se: o controle que se realiza presencialmente – mediante a vigilância – é negociado, não absoluto, sendo baseado em uma avaliação moral complexa do caráter, que avalia o comportamento, a identidade, a aparência da pessoa através 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, pp. 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 invidíduo previamente classificado como praticante de tal delito. Um sistema de vigilância poderia ser utilziado 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).

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 algoritimos. Isso porque, atualmente, "corpos anônimos podem ser transformados em sujeitos digitais, identificados e relacionados às suas personas virtuais que residem em bases de dados eletrônicas" (NORRIS, 2003, p. 278)[4], o que pode ocasionar violações à privacidade, aqui considerada como o direito da pessoa de escolher aquilo que está disposta a revelar às demais. Ademais, a privacidade, no âmbito da comunicação eletrônica, pode se manifestar como a necessidade de anonimato, como se observa:

> Em uma dimensão que se torna cada vez mais diferenciada e complexa, a demanda por privacidade não se manifesta apenas na sua forma tradicional, como direito de impedir aos outros a coleta e a difusão de informações sobre o interessado. No âmbito da comunicação eletrônica, ela pode se exprimir sobretudo como uma necessidade de anonimato ou, melhor dizendo, como exigência de assumir a identidade preferida, apresentando-se com um nome, um sexo, uma idade que podem ser diferentes daqueles efetivamente correspondentes aos dados do indivíduo. Requer-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)

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. Contudo, esse movimento gera o "assujeitamento" da sociedade, culminando, assim, em uma

> armadilha perigosa para os próprios indivíduos, pois ao consentirem silenciosamente com os dispositivos de vigilância, não vislumbram que, por outro lado, 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).

Finalmente, outro aspecto a ser considerado relaciona-se à transparência na coleta de dados pessoais por meio da vigilância, bem como ao acesso que o indivíduo possui a esses

[4] 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),

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 (2008, p. 60) 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 se deslocando 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 se configura, portanto, como "um instrumento capaz de determinar formas de redistribuição de poder" (RODOTÀ, 2008, p. 73). Importante destacar que este direito

> supera o âmbito das informações pessoais e a sua disciplina tende a se conjugar com a outra, mais geral, de um "direito à informação", também esse encarado em uma versão ativa e dinâmica: não mais, portanto, como simples "direito a ser informado mas como o direito a ter acesso direto a determinadas categorias de informações, em mãos públicas e privadas. Aqui desponta claramente a ligação entre os desenvolvimentos institucionais e as inovações tecnológicas: justamente estes tornam possível propor uma generalização do direito de acesso, no momento em que eliminam os obstáculos de caráter "físico" que, no passado, tornavam impossíveis ou extremamente difíceis os acessos à distância, múltiplos, distribuídos em um arco de tempo mais amplo que aquele do horário ordinário dos escritórios, e assim por diante (RODOTÀ, 2008, p. 69).

Conquanto esse seja o cenário ideal, a realidade demonstra 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)

Referindo-se a pesquisa realizada pela Fundação Getúlio Vargas (FGV) em 2016, cujo objetivo era obter dados da gestão municipal e avaliar o grau de transparência das Prefeituras brasileiras com relação à gestão de dados, a oferta de serviços online e a existência de iniciativas de cidades inteligentes na área de segurança pública, as autoras concluem que "boa parte dos municípios avaliados ainda estão despreparados para enfrentar os novos desafios colocados pelas práticas de *big data* no que diz respeito às suas políticas de gestão da Tecnologia da Informação e de tratamento de dados pessoais" (BARROS; VENTURINI, 2018, p. 42). Aduzem ainda que,

> na prática, isso significa que os interesses comerciais e corporativos encontram um terreno suscetível à discricionariedade do agente, ou seja, as decisões de contratação, da escolha de padrões, tecnologias, proteções entre outros elementos de uma política de informação municipal ficam na mão do gestor e, de acordo com a pesquisa, há pouca ou quase nenhuma transparência sobre isso. (BARROS; VENTURINI, 2018, p. 42)

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 o cidadão conheça 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.

5 CONSIDERAÇÕES FINAIS

Conquanto possibilite a construção de uma esfera privada mais diversa, o desenvolvimento tecnológico, paradoxalmente, torna as pessoas mais vulneráveis a partir do momento em que sua exposição pública passa a ser constante. Isso faz surgir a necessidade crescente de um maior fortalecimento da proteção jurídica da privacidade, sendo relevante refletir sobre as limitações de uma compreensão da privacidade como direito individual.

Importa, igualmente, ponderar-se qual deve ser o limite na interferência da vida privada, por parte do Estado e de instituições privadas, no que tange à vigilância e coleta de dados pessoais em troca de uma suposta segurança.

A noção clássica de privacidade, entendida como o direito de ser deixado só, não mais se sustenta na sociedade de informação, que atualmente se releva como uma sociedade de vigilância e de classificação. Considerando-se que muitas de nossas interpretações do mundo e ações são moldadas pelas tecnologias que utilizamos, se mostram necessárias novas formas de tratamento jurídico da privacidade, que deverá ser entendida também como o direito da pessoa de controlar o uso que se faz das informações que lhe dizem respeito, bem como o direito de se escolher o que se quer revelar aos outros. Ademais, há que se considerar, para além da privacidade, o direito à proteção de dados, o qual, todavia necessite de clareza e especificidade normativa, se estabelece como um direito autônomo.

Em uma conjuntura de crescentes avanços tecnológicos, os sistemas de vigilância que empregam tecnologias de reconhecimento facial tornam-se cada vez mais presentes no cotidiano de diversas sociedades. Alimentados por tecnologias de inteligência artificial e *big data*, tais sistemas potencializam a ocorrência de violações ao direito à privacidade, bem como ao direito à proteção de dados. 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. Contudo, como afirma Rodotà, *surveillance is not a destiny*.

Enquanto cresce a preocupação político-institucional no tocante à privacidade e à proteção de dados e informações pessoais, torna-se uma tarefa cada vez mais árdua o respeito a esta presunção geral, o que se dá por motivos como as constantes exigências de segurança pública, interesses de mercado e reorganização da administração pública. No atual contexto, é imprescindível repensar-se a privacidade e a proteção dados enquanto bens sociais para além da dimensão individual, superando-se a lógica puramente proprietária e integrando-se corretamente os controles individuais, como o direito de acesso, com aqueles que dizem respeito à esfera pública, referentes ao controle normativo.

Não se pode negar que 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 que se assegurem tanto a garantia dos direitos individuais quanto 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.

REFERÊNCIAS BIBLIOGRÁFICAS

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 . Data de acesso: 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. 1ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 31-45.

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

CASTELLS, Mannuel. **A Galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges, revisão Paulo Vaz. Rio de Janeiro: Jorge Zahar, 2003.

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

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

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. et al. AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. **Minds and Machines**. Disponível em: https://www.researchgate.net/publication/329192820_AI4People-

An_Ethical_Framework_for_a_Good_AI_Society_Opportunities_Risks_Principles_and_Recommendations. Acesso em: 23 jun. 2019.

FLORIDI, L.; 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.

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.

FLORIDI, L. et al. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. **Science and Engineering Ethics**. Springer, 2017, p. 1-24.

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

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.

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.

LEVY, Pierre. A conexão planetária: o mercado, o ciberespaço, a consciência. Tradução de Maria Lúcia Homem e Ronaldo Entler. São Paulo: Editora 34, 2001.
LIN, P.; ABNEY, K.; BEKEY, G. A. **Robot ethics:** the ethical and social implications of robotics. MIT press, 2012.

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.

MULHOLLAND, C**.** A TUTELA DA PRIVACIDADE NA INTERNET DAS COISAS (IOT). In: Magrani, Eduardo. (Org.). **Horizonte presente:** Debates de tecnologia e sociedade. 1ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 485-495.

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. p. 247-281.

PREFEITURA DO RIO DE JANEIRO. **RIO+ SEGURO**. Disponível em: http://maisseguro.rio. Acesso em: 20 ago. 2019.

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. 1ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 577-586.

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.

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.

WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review,** 2019(1). Disponível em: https://ssrn.com/abstract=3248829. Acesso em: 23 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.