



## O RECONHECIMENTO FACIAL PELA REGIÃO PERIOCLAR E A (IN)CONSTITUCIONALIDADE DO USO DE MÁSCARAS EM MANIFESTAÇÕES PÚBLICAS

**Diogo Dal Magro\***  
**Vinícius Borges Fortes\*\***

Resumo: O objetivo geral do presente estudo é compreender, a partir da tecnologia de reconhecimento facial pela região dos olhos, suas implicações à democracia. Quanto ao problema de pesquisa, este pode ser apresentado pela pergunta: de que maneira as novas possibilidades de reconhecimento facial, a partir da região olhos, podem apresentar riscos de interferência a elementos considerados inerentes à democracia? O método de abordagem utilizado é o indutivo. Como parte das conclusões, registra-se que essa discussão ganhou um novo capítulo com o advento do reconhecimento facial pela região periorcular, o que pode tornar inócua a futura decisão do Supremo Tribunal Federal.

\* Mestrando em Direito pela Faculdade Meridional - IMED, sendo Taxista PROSUP/CAPES (2021/2022). Graduado em Direito pela Faculdade Meridional - IMED (2016-2020). Membro dos Grupos de Pesquisa "Latin America Privacy Hub", "Direito, Novas Tecnologias e Desenvolvimento" e "Ética, Cidadania e Sustentabilidade", vinculados ao Programa de Pós-Graduação Stricto Sensu - Mestrado em Direito - da Faculdade Meridional - IMED. Bolsista MITACS (2019), tendo desenvolvido pesquisas no projeto "Démocratie digitale (digital democracy) en contexte de rapports linguistiques complexes", na Université de Moncton (Canadá). Membro Fundador do Capítulo Legal Hackers de Passo Fundo-RS. Bolsista PROBIC - FAPERGS/IMED (2018/2019). Bolsista PIBIC - CNPq/IMED (2017/2018). Co-fundador da LawTech Hi ORDER Regulação e Tecnologia. Advogado. E-mail: diogodalmagro@gmail.com.

\*\* Possui Estágio de Pós-Doutorado em Direito pela Vrije Universiteit Brussel, Bélgica (2016), com pesquisa voltada aos Direitos de privacidade na internet e o sistema de proteção de dados. Doutorado em Direito pela Universidade Estácio de Sá - UNESA (2015), com período sanduíche na Universidad de Zaragoza (2014-2015), com financiamento do PDSE/CAPES. Mestrado em Direito pela Universidade de Caxias do Sul (2011). Graduação em Direito pela FAPLAN - Faculdades Planalto (2008). Atualmente, é pesquisador e Bolsista de Produtividade em Pesquisa com dedicação exclusiva ao CETID - Centro de Pesquisa, Tecnologia e Inovação Digital da Fundação Meridional, no Projeto de Pesquisa "Tecnologia, Inovação e Sustentabilidade". Além disso, atua como pesquisador-membro do Projeto de pesquisa "O Distrito Federal e a Governança da Internet: tecnologias e informação", financiado pela Fundação de Amparo à Pesquisa do Distrito Federal. Ainda, é líder do Projeto de Pesquisa Latin America Privacy Hub (LAPH), certificado pela IMED no Diretório de Grupos de Pesquisa do CNPq, financiado pelo CETID/Fundação Meridional. Sua pesquisa está focada nas áreas de Tecnologia, Inovação e Sustentabilidade, com ênfase em Direitos de Privacidade na Internet; Proteção de Dados Pessoais; Regulação e Tecnologia para a Democracia e para a Sustentabilidade. É professor visitante no Law, Science, Technology and Society Research Group (LSTS) da Vrije Universiteit Brussel (VUB), Bélgica, bem como do Brussels Privacy Hub, desde o ano 2016. Mantém parcerias de pesquisa com instituições e pesquisadores brasileiros (UnB, PUCPR, UFSM, Uniritter, UFRGS), e estrangeiros (VUB/Bélgica, Brussels Privacy Hub/Bélgica, LSTS/Bélgica, Universidad de Zaragoza/Espanha). Professor permanente do Programa de Pós-Graduação Stricto Sensu em Direito da IMED - Faculdade Meridional, onde foi coordenador no período 2017-2019. Professor dos cursos de Graduação em Direito e Ciência da Computação da IMED - Faculdade Meridional. Tem experiência profissional como advogado e empreendedor no segmento Lawtech, tendo fundado a Hi ORDER Regulação e Tecnologia, startup focada na oferta de soluções jurídicas e tecnológicas voltadas à elaboração e automação de contratos de tecnologia; blindagem contratual e tecnológica em operações empresariais que envolvam tecnologia; suporte regulatório e tecnológico a provedores de aplicação e conexão à internet; gestão de propriedade intelectual e bancos de dados; aplicação de soluções jurídicas inteligentes na produção de prova processual por blockchain e outras tecnologias. Líder do capítulo Legal Hackers Passo Fundo, atuando como articulador do tema Direito e Tecnologia entre profissionais da área jurídica, TI e mídias digitais. E-mail: vinicius.fortes@imed.edu.br.



Palavras-chave: Reconhecimento facial; Máscaras; Manifestações públicas; (In)Constitucionalidade; Repercussão Geral.

## **FACIAL RECOGNITION BY THE PERIOCLAR REGION AND THE (UN)CONSTITUTIONALITY OF THE USE OF MASKS IN PUBLIC MANIFESTATIONS**

**Abstract:** The general objective of the present study is to understand, from the facial recognition technology by the eyes region, its implications for democracy. As for the research problem, it can be presented by the question: how can the new possibilities of facial recognition, from the eyes region, present risks of interference to elements considered inherent to democracy? The approach method used is inductive. As part of the conclusions, it is registered that this discussion gained a new chapter with the advent of facial recognition by the perioocular region, which may render the future decision of the Supreme Court innocuous.

**Key- Words:** Facial recognition; Masks; Public manifestations; (Un)Constitutionality; General Repercussion.

### **INTRODUÇÃO**

A partir da pandemia da Covid-19, a utilização de máscaras se tornou obrigatória, por lei, em grande parte dos países do ocidente. A medida, como sabido, visa evitar a transmissão e o contágio do vírus. No entanto, em países do oriente, a prática de utilizar máscaras, no dia a dia, é já corriqueira. Não demorou para que empresas de tecnologia desenvolvessem técnicas de reconhecimento facial de pessoas, mesmo utilizando máscaras. Embora a tecnologia, a princípio, seja positiva, vez que identifica pessoas que não estão seguindo as determinações sanitárias, por outro lado desperta preocupações sobre sua aplicação, especialmente num cenário pós-pandêmico.

Em 2013, no Brasil, no bojo das manifestações que marcaram o cenário político do ano, o Estado do Rio de Janeiro aprovou legislação que proibia a manifestação pública de pessoas utilizando máscaras. Suscitada a inconstitucionalidade da referida lei, o processo hoje encontra-se no Supremo Tribunal Federal, sem julgamento de mérito proferido e afetado pelo Tema 912 da Repercussão Geral.

Diante das premissas lançadas, propõe-se como problema de pesquisa deste trabalho a seguinte indagação: de que maneira as novas possibilidades de reconhecimento facial, a partir da região olhos, podem apresentar riscos de interferência a elementos considerados inerentes à democracia?





Como objetivo geral destaca-se: compreender, a partir da tecnologia de reconhecimento facial pela região dos olhos, as implicações à democracia, tomando-se como base o pendente julgamento, pelo STF, do Tema 912 da Repercussão Geral.

Como objetivos específicos, registre-se: a) explicar os processos de *surveillance*, a partir das tecnologias de reconhecimento facial; b) analisar o interesse do Brasil nas tecnologias de reconhecimento facial; c) verificar o Tema 912 da Repercussão Geral, pendente de julgamento pelo Supremo Tribunal Federal, e sua obsolescência em face das novas técnicas de reconhecimento facial pela região periorcular.

O método de abordagem utilizado é o indutivo. Esse método consiste em “pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral [...]” (PASOLD, 2008, p. 86). Como premissa específica, analisa-se a utilização de técnicas de reconhecimento facial pela região dos olhos para, adotada durante a pandemia da Covid-19, para, em seguida, analisar o fenômeno sob a ótica da utilização de máscaras como meio de não expor a identidade de pessoas em manifestações públicas, tomando-se como paradigma, o caso das manifestações de 2013 no Brasil.

## **1 O RECONHECIMENTO FACIAL PELA REGIÃO DOS OLHOS NA ERA DA SURVEILLANCE**

Tecnologias como *big data*, IoT, inteligência artificial e reconhecimento facial, quando utilizadas por órgãos estatais, podem conceber um panorama de Estado de vigilância. O conceito não é novo, e visa, em sua essência, demonstrar que grandes sistemas político-estatais de controle e opressão social podem ganhar forma quando a utilização dessas tecnologias vem desacompanhada da preocupação de proteção de direitos fundamentais, especialmente, no caso, os correlatos à privacidade e aos dados pessoais.

Países orientais como a China são comumente citados para exemplificar a dimensão de um Estado de vigilância. De certo modo, a conexão não é inócua, vez que o país é sede de um número crescente de empresas de tecnologias que vêm crescendo exponencialmente e inovando cotidianamente no cenário tecnológico. Evidente que o Ocidente rapidamente populariza grande parte das inovações tecnológicas lá produzidas. A diferença, no entanto, é a discussão e a proteção jurídica da privacidade, no Ocidente, já percorreram um considerável



caminho, seja com o clássico artigo *The Right to Privacy*, seja com as normativas da União Europeia e dos Estados Unidos da América sobre o tema.

Durante a pandemia da Covid-19, empresas chinesas de tecnologia realizam aperfeiçoamentos de suas tecnologias, também em vista das novas situações criadas pela própria pandemia. Um desses casos é a SenseTime, uma empresa que desenvolve tecnologias de reconhecimento facial, que anunciou o uso em locais públicos de seus sistemas de reconhecimento facial sendo capazes de realizar o reconhecimento e identificação de pessoas, com alto índice de precisão, mesmo que as pessoas estejam utilizando máscaras (LI, 2020).

A empresa SenseTime também informou que seus sistemas de reconhecimento facial podem ser aliados com câmeras que operam a tecnologias de imagem térmica, o que permite a detecção e identificação de pessoas com uma temperatura elevada, ou seja, um sistema que permite realizar a detecção de febre – um dos sintomas que indica que o indivíduo pode estar com a Covid-19. Trata-se, desse modo, de uma possibilidade de realizar a identificação massiva de potenciais pacientes vítimas do coronavírus, de modo que os usuários da tecnologia – em especial Estados e seus órgãos –, possam receber alertas com os dados de identificação desses pacientes. Além disso, a empresa informou que o software também é capaz de identificar pessoas que não estavam usando máscaras em locais públicos, como forma de exigir que utilizassem a proteção para acessar edifícios públicos, por exemplo (LI, 2020).

Tecnologias de reconhecimento facial de pessoas utilizando máscaras, como a da SenseTime, também já é desenvolvida por empresas como Wisisoft, sediada na Província de Sichuan, que faz a análise facial em 3D e possui precisão de 98% em 1.000 pessoas analisadas (XINHUA, 2020). A empresa Hanwang Technology, com sede em Pequim, também anunciou o desenvolvimento da tecnologia de reconhecimento artificial de pessoas utilizando máscaras, aliada a verificação de temperatura corporal, capaz de reconhecer 30 pessoas em 1 segundo, com uma precisão de 95% (POLLARD, 2020).

A mencionada assimetria entre países do Ocidente e Estados do Oriente, como a China, é verificada em situações concretas como esta. Se, por um lado, a China segue no aperfeiçoamento de tecnologias de reconhecimento facial durante a pandemia da Covid-19, a empresa norte americana IBM (*International Business Machines Corporation*), após as repercussões internacionais envolvendo o assassinato de George Perry Floyd Jr., enviou uma



carta ao *United States Congress*, datada de 8 de junho de 2020, assinada pelo CEO Arvind Krishna, afirmando:

*“Responsible technology policies - technology can increase transparency and help police protect communities but must not promote discrimination or racial injustice. IBM no longer offers general purpose IBM facial recognition or analysis software. IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency. We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies. Artificial Intelligence is a powerful tool that can help law enforcement keep citizens safe. But vendors and users of AI systems have a shared responsibility to ensure that AI is tested for bias, particularly when used in law enforcement, and that such bias testing is audited and reported. Finally, national policy also should encourage and advance uses of technology that bring greater transparency and accountability to policing, such as body cameras and modern data analytics techniques.” (KRISHNA, 2020).<sup>1</sup>*

No mesmo sentido, a Amazon publicou nota, em 10 de junho de 2020, afirmando:

*“We’re implementing a one-year moratorium on police use of Amazon’s facial recognition technology. We will continue to allow organizations like Thorn, the International Center for Missing and Exploited Children, and Marinus Analytics to use Amazon Rekognition to help rescue human trafficking victims and reunite missing children with their families. We’ve advocated that governments should put in place stronger regulations to govern the ethical use of facial recognition technology, and in recent days, Congress appears ready to take on this challenge. We hope this one-year moratorium might give Congress enough time to implement appropriate rules, and we stand ready to help if requested.” (AMAZON, 2020).<sup>2</sup>*

<sup>1</sup> Tradução livre: “Políticas tecnológicas responsáveis - a tecnologia pode aumentar a transparência e ajudar a polícia a proteger as comunidades, mas não deve promover discriminação ou injustiça racial. A IBM não oferece mais software de análise ou reconhecimento facial IBM de uso geral. A IBM se opõe firmemente e não tolerará o uso de nenhuma tecnologia, incluindo a tecnologia de reconhecimento facial oferecida por outros fornecedores, para vigilância em massa, criação de perfil racial, violações de direitos humanos e liberdades básicas ou qualquer finalidade que não seja consistente com nossos valores e Princípios de Confiança e Transparência. Acreditamos que agora é a hora de iniciar um diálogo nacional sobre onde e como a tecnologia de reconhecimento facial deve ser empregada pelas agências policiais nacionais. A inteligência artificial é uma ferramenta poderosa que pode ajudar a aplicação da lei a manter os cidadãos seguros. Porém, fornecedores e usuários de sistemas de IA têm uma responsabilidade compartilhada de garantir que a IA seja testada quanto a vieses [*human bias*], principalmente quando usada na aplicação da lei, e que esses testes de vieses [*human bias*] sejam auditados e relatados. Por fim, a política nacional também deve incentivar e avançar nos usos de tecnologias que tragam maior transparência e responsabilidade ao policiamento, como câmeras corporais e técnicas modernas de análise de dados.”

<sup>2</sup> Tradução livre: “Estamos implementando uma moratória de um ano no uso policial da tecnologia de reconhecimento facial da Amazon. Continuaremos a permitir que organizações como Thorn, o Centro Internacional para Crianças Desaparecidas e Exploradas e o Marinus Analytics usem o Amazon Rekognition para ajudar a resgatar vítimas de tráfico humano e reunir crianças desaparecidas com suas famílias. Defendemos que os governos implementem regulamentações mais rígidas para governar o uso ético da tecnologia de reconhecimento facial e, nos últimos dias, o Congresso parece pronto para enfrentar esse desafio.”



A identificação pela região dos olhos, frequentemente conhecida como região periocular, traz outras vantagens, além da mera possibilidade de reconhecer uma pessoa mesmo que ela esteja utilizando máscara. Isso porque, por mais que a pessoa envelheça ou tenha significativas mudanças no peso, essa região dificilmente se altera com as transformações do corpo, ou, quando ocorre, a alteração é relativamente baixa, o que possibilita o reconhecimento mesmo comparando imagens da mesma pessoa em épocas com um lapso temporal grande (METZ, 2020).

Mas os riscos da tecnologia também se intensificam, vez que a quantidade de dados biométricos utilizados no reconhecimento pela região periocular é menor se comparado àqueles utilizados no reconhecimento por meio de toda a face. Assim, o risco de identificação aumenta, além dos já mencionados riscos à privacidade dos indivíduos submetidos ao processo de reconhecimento (METZ, 2020).

Evidentemente, quem estiver utilizando máscara e óculos de sol, por exemplo, trará uma dificuldade ainda maior para a tecnologia de reconhecimento. No entanto, reconhecer que técnicas precisas também podem apresentar riscos, é um dos fatores que leva o tema ao debate. E mais: deve-se atentar para o uso que Estados e autoridades públicas vem fazendo de técnicas de reconhecimento facial, bem como as potencialidades de ingerência na democracia, quando utilizadas perversamente.

É importante registrar que a ideia de vigilância, que é hoje aperfeiçoada, tem sua origem remontando no projeto desenvolvido pelo pai do utilitarismo: o panóptico. Trata-se de um modelo de prisão<sup>3</sup> projetado pelo irmão de Jeremy Bentham, mas por esse apresentado, que consistia em celas de prisão dispostas em formato de círculo em torno de um posto de guarda. A claridade que entrava pelo lado exterior das celas permitia que todos os

---

Esperamos que esta moratória de um ano dê tempo ao Congresso para implementar regras apropriadas e estamos prontos para ajudar, se solicitado.”

<sup>3</sup> O termo utilizado é “casa de inspeção”. Sem prejuízo disso, nos termos do próprio autor, “para dizer tudo em uma palavra, ver-se-á que ele é aplicável, penso eu, sem exceção, a todos e quaisquer estabelecimentos, nos quais, num espaço não demasiadamente grande para que possa ser controlado ou dirigido a partir de edifícios, queira-se manter sob inspeção um certo número de pessoas. Não importa quão diferentes, ou até mesmo quão opostos, sejam os propósitos: seja o de punir o incorrigível, encerrar o insano, reformar o viciado, confinar o suspeito, empregar o desocupado, manter o desassistido, curar o doente, instruir os que estejam dispostos em qualquer ramo da indústria, ou treinar a raça em ascensão no caminho da educação, em uma palavra, seja ele aplicado aos propósitos das prisões perpétuas na câmara da morte, ou prisões de confinamento antes do julgamento, ou casas penitenciárias, ou casas de correção, ou casas de trabalho, ou manufaturas, ou hospícios, ou hospitais, ou escolas.” (BENTHAM, 2008, p. 19-20).



movimentos de qualquer detento fossem percebidos e monitorados por apenas um guarda, o que dava eficiência ao projeto (BENTHAM, 2008, p. 20-23).

A grande engenhosidade no projeto do panóptico reside na capacidade de poder ver, sem ser visto. O projeto possui mecanismos capazes de impedir que os detentos possam ver a presença do inspetor no posto de inspeção, ao mesmo tempo em que as pessoas passam a sentir-se como estando sempre sob observação ou, ao menos, sob uma grande possibilidade dessa vigilância estar ocorrendo (BENTHAM, 2008, p. 28-30).<sup>4</sup>

É com Michel Foucault, posteriormente, que o panóptico é utilizado como conceito filosófico para apontar e descrever os mecanismos de opressão e controle social que permeiam a sociedade. Assim, para além de um modelo de poder elevado à sua forma ideal, “[...] na verdade, é uma figura de tecnologia política que pode e deve ser distinguido de qualquer uso específico.” (FOUCAULT, 2013, p. 158).

Esse modelo clássico de vigilância foi incrementado a partir das inovações tecnológicas, especialmente por meio de infraestruturas de tecnologias da informação. Esses avanços ocasionam a transformação da vigilância, que além de evoluir quantitativamente, passa a contar também com o elemento qualitativo dos dados, inclusive superando uma simples ideia de vigilância digital, para dar origem ao fenômeno da *surveillance*.<sup>5</sup> Ainda que não completamente dissociadas, *surveillance* apresenta um fenômeno mais amplo e complexo do que a simples vigilância (MENEZES NETO, 2016, p. 93-101).

A literatura especializada também sinaliza um semelhante avanço no sentido de pontuar a diferença entre a “*traditional surveillance*” em contraste com a “*new surveillance*”, de modo que esta se constitui a partir das novas tecnologias que operam por meio de coleta de informações pessoais (MARX, 2004, p. 18). Assim, é partir desse cenário que se desenvolve uma das dimensões da *surveillance*, onde “[...] *governments engage in mass surveillance on*

<sup>4</sup> “Regozijo-me com o fato de que há, agora, pouca dúvida de que o plano possui as vantagens fundamentais que venho atribuindo a ele: quero dizer, a aparente onipresença do inspetor (se os teólogos me permitirem a expressão), combinada com a extrema facilidade de sua real presença.” (BENTHAM, 2008, p. 30-31).

<sup>5</sup> De imediato, pontua-se que, na língua inglesa, “*surveillance*” e “*vigilance*” são conceitos diferentes, mas que acabam sendo traduzidos como “vigilância”. Ainda, o já popular termo “*dataveillance*”, que expressa a noção de “vigilância de dados”, não é suficiente para expressar o fenômeno aqui em análise. De igual modo, a palavra de “*sousveillance*”, cunhada na língua francesa a partir da substituição do prefixo “*sur*” (acima) por “*sous*” (abaixo), denota a ideia de que enquanto na *surveillance* o governo monitora seus cidadãos (de cima para baixo), a *sousveillance* expressa a vigilância dos cidadãos para com suas autoridades (de baixo para cima) (MANN; NOLAN; WELLMAN, 2002, p. 332-333).



*their own citizens - contradicting basic democratic practice.*”<sup>6</sup> (LYON, 2015, pos. 337). É por isso que a tecnologia não é apenas um fator externo na *surveillance*, mas sim um componente próprio e interno das relações sociais cotidianas (MENEZES NETO, 2016, p. 93). Fato é, que o fenômeno da *surveillance* é permanentemente renovado.

Não é difícil perceber que o reconhecimento facial funciona para além da função de simples olhos do inspetor no projeto do panóptico, indicando a superação do panoptismo. O uso dessas tecnologias permite que o Estado veja sem ser visto; identifique indivíduos com facilidade e rapidez, ainda que com precisão discutível; e controle os comportamentos dos indivíduos por meio do temor de estarem sob observação. Em uma *smart surveillance*, essas formas de coação, ainda que sutis, são reais, apontando para uma limitação à liberdade dos cidadãos, elemento este – liberdade individual – definidor de um Estado como democrático.

As advertências de George Orwell e Aldous Huxley talvez soem hoje como um clichê. Isso porque, os cenários distópicos que foram descritos por eles são hoje uma realidade, talvez, já superada. Levando-se em conta isso, é preciso verificar como o reconhecimento facial opera e como pode acarretar em complicações não só ao direito à privacidade, mas também em elementos característicos de um estado democrático de direito e da própria democracia.

## **2 A TRAJETÓRIA BRASILEIRA DO RECONHECIMENTO FACIAL E A (IN)CONSTITUCIONALIDADE DA UTILIZAÇÃO DE MÁSCARAS EM MANIFESTAÇÕES PÚBLICAS**

O interesse brasileiro por tecnologias como as reconhecimento facial pode ser notado há quase duas décadas. No âmbito legislativo, o Projeto de Lei nº 3.372/2004, propôs a instituição de mecanismos de características biométricas para credenciamento e autenticação de usuários, como requisito para permitir alterações de informações em bancos de dados dos setores de pessoal, pagamentos e arrecadação de tributos, da administração pública direta, indireta e fundacional (BRASIL, 2004).

Entre outros mecanismos citados diretamente pelo projeto, tem-se o reconhecimento facial, além da impressão digital e o reconhecimento de íris. Apesar de arquivado em 2008, o

<sup>6</sup> Tradução livre: “governos se envolvem na vigilância em massa de seus próprios cidadãos - contradizendo a prática democrática básica.”



projeto, que tramitou na Câmara dos Deputados, recebeu aprovação pela Comissão de Trabalho, Administração e Serviço Público (CTASP), além de parecer pela aprovação na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI) (BRASIL, 2004).

Em 2018, a Câmara dos Deputados recebeu outras duas proposições legislativas, que tramitam simultaneamente, a fim de implementar a utilização de reconhecimento facial no âmbito do sistema penitenciário.<sup>7</sup> O Projeto de Lei nº 9.736/2018 propõe que a guia de recolhimento do apenado seja complementada, mediante identificação biométrica por reconhecimento facial (BRASIL, 2018a). Por sua vez, o Projeto de Lei nº 11.140/2018, estabelece que custodiados, servidores públicos, prestadores de serviços e visitantes, deverão realizar identificação biométrica para acesso aos estabelecimentos penais (BRASIL, 2018b).

Para além do poder legislativo, o Brasil conta, desde 2011, com a utilização de reconhecimento facial, implantado como projeto piloto em Ilhéus, na Bahia, visando coibir fraudes no transporte público. Nada obstante, o uso dessas tecnologias se tornou popular a partir de 2018. Ao todo, já são mais de quarenta e oito implantações, somente pelo poder público, respectivamente nos setores de transporte, segurança pública, controle de fronteiras, educação, além de outras aplicações (INSTITUTO IGARAPÉ, 2019).<sup>8</sup>

Na Bahia<sup>9</sup>, a Secretaria de Segurança Pública utiliza sistema de reconhecimento facial, desde 2018 (MARAUX, 2020a). Em 2019, o uso da tecnologia na Micareta de Feira de Santana, capturou o rosto de mais de 1,3 milhão de foliões (NASCIMENTO, 2019). Em 2020, o reconhecimento facial no Carnaval de Salvador permitiu a contagem do número de foliões, chegando a 11,7 milhões (MARAUX, 2020b). O número aponta a quantidade de pessoas que foram submetidas à tecnologia, não sendo divulgado nenhuma medida de proteção aos dados pessoais coletados e, ainda, sem o claro conhecimento pelos cidadãos.

<sup>7</sup> Ambos projetos visam alterar a Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal – LEP). O Projeto de Lei nº 9.736/2018 visa acrescentar o “Art. 107-A. As informações constantes da guia de recolhimento serão complementadas pela identificação biométrica por reconhecimento facial, quando o custodiado for recolhido a um estabelecimento penal.” (BRASIL, 2018a). Já o Projeto de Lei nº 11.140/2018 visa inserir o “Art. 109-A. Todos os custodiados, servidores públicos, prestadores de serviços e visitantes deverão ser identificados pelo sistema biométrico para ter acesso aos estabelecimentos penais.” (BRASIL, 2018b). Esse último, apesar de não citar expressamente o reconhecimento facial, entende-se ser essa uma técnica que pode ser utilizada.

<sup>8</sup> As implantações concentram-se em quinze estados da federação, além do Distrito Federal, estando presentes em trinta cidades (INSTITUTO IGARAPÉ, 2019).

<sup>9</sup> O reconhecimento facial utilizado no Estado da Bahia é da empresa chinesa Huawei, sediada em Shenzhen, onde, em 14 de maio de 2019, a empresa convidou o governador Rui Costa a apresentar as experiências citadas, durante o Fórum Smart City. O governador afirmou que: “estamos felizes com o resultado inicial, mas nosso objetivo é avançar e proporcionar mais segurança aos baianos, por isso estamos licitando este serviço para 55 cidades. Também contrataremos softwares para educação e saúde, áreas que considero fundamental o uso da tecnologia para melhorar e ampliar a oferta de serviços à população.” (BAHIA, 2019).

Em 2019, a Companhia do Metropolitano de São Paulo (METRÔ) realizou processo licitatório (Licitação Pública Internacional nº 10014557) a fim de conceber sistema de monitoração eletrônica nas linhas de metrô. O detalhamento técnico que acompanha a licitação evidencia o objetivo de implantação de reconhecimento facial de todos os usuários do metrô (BRASIL, 2020c, p. 89-201).

Em decorrência disso, em fevereiro de 2020, ajuizou-se Ação de Produção Antecipada de Provas, a fim de que fossem demonstrados os detalhes dos procedimentos de segurança a serem adotados em relação ao banco de dados do sistema (BRASIL, 2020c, p. 1-22). A demanda foi deferida a fim de que a Companhia do Metropolitano de São Paulo (METRÔ) apresentasse documentação hábil a comprovar a segurança do banco de dados utilizado para realizar o reconhecimento facial (BRASIL, 2020c, p. 533-537).

A utilização de tecnologias de detecção facial<sup>10</sup> vai além da área de segurança pública. Em abril de 2018, a empresa ViaQuatro (Concessionária da Linha 4 do Metrô de São Paulo S. A.) realizou instalação de portas interativas digitais, em algumas estações do metrô de São Paulo. A tecnologia consiste na implantação de câmeras com sensores capazes de contabilizar a quantidade de pessoas que passam em frente às telas de publicidade. Além da captação da presença humana, há a coleta de dados da face (detecção facial) que, após processados pelo software, interpretam as expressões faciais, classificando-as em quatro tipos de emoções: feliz, insatisfeito, surpreso e neutro (BRASIL, 2018d, p. 5).<sup>11</sup>

Mediante análise da estatura da pessoa, o sistema é capaz de classificá-la como criança, jovem ou adulto, além de, a partir do formato do rosto, haver a identificação do gênero da pessoa, em masculino ou feminino (BRASIL, 2018d, p. 5). Note-se, que a coleta dos dados biométricos dos usuários não se destina à segurança do metrô, mas à análise da reação destes aos anúncios de publicidade veiculados nos painéis, alimentando preceitos de

<sup>10</sup> Ainda que se trate de detecção facial, e não de reconhecimento facial, os riscos subsistem. Isso porque, conforme apontado no capítulo anterior, a detecção facial é apenas a primeira etapa do processo de reconhecimento facial. Significa que, a coleta de dados obtida no processo de detecção facial pode ser utilizada para realizar posterior reconhecimento facial. A possibilidade técnica de realizar o reconhecimento facial, contrastando-se os dados coletados na detecção facial com imagens (com a respectiva identificação do titular da imagem) obtidas na internet, especialmente por meio de aplicativos como Facebook, Instagram, Snapchat e TikTok, denotam a dimensão dos riscos.

<sup>11</sup> Explica o presidente da ViaQuatro, Harald Zwetkoff, que “as portas de plataforma interativas são uma tecnologia inovadora desenvolvida pela ViaQuatro para aprimorar transmissão de informações aos passageiros da Linha 4-Amarela. Essa nova ferramenta na área de comunicação e marketing, com recursos sofisticados, pode colaborar na criação de novas estratégias para públicos específicos, visando mais efetividade na troca de mensagens importantes ou mesmo o incremento em vendas.” (BRASIL, 2018d, p. 6).



otimização publicitária. Em razão disso, o Instituto de Defesa do Consumidor (IDEC) ajuizou Ação Civil Pública, com Tutela de Urgência, que foi deferida, determinando-se o desligamento das portas interativas digitais (BRASIL, 2018d, p. 332).

Fica evidente, portanto, que a tecnologia de reconhecimento facial está se popularizando no Brasil. Uma situação controversa, no entanto, acaba tornando-se ainda mais complexa. Isso porque, no bojo das manifestações públicas que ocorreram em relação ao cenário político-econômico do Brasil em 2013, a Assembleia Legislativa do Estado do Rio de Janeiro (ALERJ) promulgou a Lei Estadual nº 6.528, de 11 de setembro de 2013, com o objetivo de regulamentar o artigo 23 da Constituição Estadual do Rio de Janeiro, que reproduz, praticamente *ipses literis*, o inciso XVI<sup>12</sup>, da Constituição Federal do Brasil de 1988, que trata sobre o direito de reunião.

No entanto, o artigo 2º da referida lei estadual dispôs que “é especialmente proibido o uso de máscara ou qualquer outra forma de ocultar o rosto do cidadão com o propósito de impedir-lhe a identificação.” (ALERJ, 2013). Ainda, o artigo 3º da lei assevera que “o direito constitucional à reunião pública para manifestação de pensamento será exercido: [...] IV - sem o uso de máscaras nem de quaisquer peças que cubram o rosto do cidadão ou dificultem sua identificação;” (ALERJ, 2013). Ainda, o §3º do mesmo artigo 3º ainda estipula que “a vedação de que trata o inciso IV do caput deste artigo não se aplica às manifestações culturais estabelecidas no calendário oficial do Estado.” (ALERJ, 2013).

A elaboração da referida lei, pelo Estado do Rio de Janeiro, naquele ano, guarda relação com as manifestações que ocorreram no Brasil. Mais especificamente, a proibição do uso de máscaras deu-se em combate ao ativismo de Black Blocs (Blocos Negros), considerado não um grupo ou movimento, mas uma tática. Pautados por ações de cunho anarquista e de prática de desobediência civil, as pessoas que participam de um Black Bloc geralmente vestem-se de preto e utilizam uma máscara para cobrir o rosto (BORGES, 2017, p. 356).

A utilização de máscaras pode ser associada a três sentidos: “esconder o próprio rosto, dificultando o trabalho de identificação pelas autoridades e protegendo os manifestantes da repressão policial; criar uma identidade coletiva, diluindo o protagonismo individual numa

<sup>12</sup> “XVI - todos podem reunir-se pacificamente, sem armas, em locais abertos ao público, independentemente de autorização, desde que não frustrem outra reunião anteriormente convocada para o mesmo local, sendo apenas exigido prévio aviso à autoridade competente;” (BRASIL, 1998).

massa; e, sentir-se mais à vontade para agir.” (ALBUQUERQUE; PEDRO, 2015, p. 1).<sup>13</sup> Nesse sentido, o Estado do Rio de Janeiro procurou agir imediatamente, para evitar que grupos de pessoas utilizando a tática Black Blocs se difundisse ainda mais, o que poderia levar ao colapso do sistema de segurança pública do estado.

Tão logo a lei obteve vigência, o Diretório Regional do Partido da República e a Seccional do Estado do Rio de Janeiro da Ordem dos Advogados do Brasil ingressaram com as Ações Diretas de Inconstitucionalidade nº 0052756-30.2013.8.19.0000 e nº 0053071-58.2013.8.19.0000. Os argumentos lançados nas representações são de que a lei limita a liberdade de manifestação do pensamento e introduz restrições ao direito de reunião que não são previstas no artigo 23 da Constituição Estadual – que, reitera-se, reproduz o artigo 5º, inciso XVI, da Constituição Federal (BRASIL, 2016).

As referidas representações de inconstitucionalidade argumentam que “também não haveria anonimato quando o manifestante está fisicamente presente na reunião, hipótese em que deve se identificar, uma vez instado pelas autoridades policiais.” (BRASIL, 2016). E que, “proibir o uso de máscaras significaria cercear a liberdade de expressão. Além disso, a lei ainda seria excessiva e desproporcional.” (BRASIL, 2016).

O relator originário designado para as ações foi o Desembargador Sérgio de Souza Verani, que julgava procedentes as representações e declarava a inconstitucionalidade da lei. No entanto, o relator foi voto vencido.<sup>14</sup> Em seu voto, destacou que a lei confunde liberdade

<sup>13</sup> “Resumidamente, podemos dizer que as máscaras escondem, protegem, revelam e potencializam rostos, indivíduos, ideias e ações. Nessa primeira reflexão, encontramos três sentidos que a conexão manifestantes-máscaras assumiram nos protestos de 2013. O primeiro expõe o que gostaríamos de chamar de imperativo da visibilidade e o quanto ela pode nos deixar vulneráveis e submetidos a uma constante vigilância. Buscar a invisibilidade, usando máscara, pode significar a busca por uma proteção e ao mesmo tempo ser incriminador. Numa realidade em que a exposição de si se coloca cada vez mais naturalizada, ter algo a esconder pode soar estranho e perturbador.

O segundo sentido tende a se opor e questionar a ideia de que as ações são individuais. O que parece estar em disputa é até que ponto os atos são coletivos ou individuais. Enquanto a polícia tenta identificar indivíduos, apostando que seu isolamento pode neutralizar a ação dos grupos, os grupos tentam se organizar diluindo a centralidade do poder, para que a ação seja maior que os indivíduos. É uma atitude que além de servir como resistência à ação policial, questiona e se opõe à tradicional organização hierarquizada e formal dos partidos políticos e da democracia representativa.

O terceiro sentido aponta para a possibilidade de se expor com mais intensidade. Usar máscara não significa se esconder, mas ampliar a atuação na visibilidade. Num mundo que se constrói cada vez mais vigiado, esconder-se não se apresenta como a única resistência a uma visibilidade que se impõe. A possibilidade de construir uma imagem e poder operar, escolhendo o que deve ser visto, também encontra seus caminhos de resistência.” (ALBUQUERQUE; PEDRO, 2015, p. 11)

<sup>14</sup> “Em seu voto, o relator originário anotou a seguinte epígrafe: “Bloom: Sou pela reforma da moral municipal e dos dez mandamentos puros. Novos mundos para os velhos. União de todos, o judeu, o muçulmano e o gentio. Três acres e uma vaca para cada filho natural. Coches-fúnebres-salão a motor. Trabalho manual compulsório para todos. Todos os parques públicos abertos dia e noite. Lava-louças elétricos. Tuberculose, aluação, guerra e



de reunião com liberdade de pensamento, uma vez que o anonimato somente é vedado na manifestação do pensamento (BRASIL, 2016). Assentou, ainda, que “as manifestações populares não podem ser controladas e regulamentadas com a rigidez que cerceia a criatividade, característica fundamental de qualquer manifestação pública, seja de natureza política, cultural, social, carnavalesca.” (BRASIL, 2016).

Já a relatora designada – em função do voto vencido do relator originário –, a Desembargadora Nilza Bitar, reconheceu a constitucionalidade da norma, vez que, a norma “regulamenta o exercício do direito fundamental de reunião, naquilo que autorizado pela própria Constituição e sem qualquer mácula a seu núcleo essencial.” (BRASIL, 2016). Destacou, ainda, que “[...] acaso não tivesse havido as notórias cenas de vandalismo – e fatos notórios prescindem de prova –, não haveria o clamor pela proibição das malfadadas máscaras.” (BRASIL, 2016). Assim, as ações diretas de inconstitucionalidade foram julgadas improcedentes pelo Tribunal de Justiça do Estado do Rio de Janeiro, sendo declarada a constitucionalidade da legislação em comento.<sup>15</sup>

O Diretório Regional do Partido da República, então, interpôs recurso extraordinário, alegando ofensa ao art. 5º, inciso II, inciso IV, e inciso XVI, da Constituição Federal, bem como violação aos princípios da razoabilidade e proporcionalidade. No entanto, o recurso extraordinário foi inadmitido pelo Tribunal de Justiça, sob o argumento que a violação seria apenas reflexa, e não direta (BRASIL, 2016).

Em seguida, o mesmo polo ativo interpôs agravo em recurso extraordinário, haja vista a inadmissão do recurso. Desse modo, o celeuma galgou até o Supremo Tribunal Federal, sob o Recurso Extraordinário com Agravo 905.149/Rio De Janeiro, com relatoria do Ministro Luís Roberto Barroso. Em 26 de agosto de 2016, o plenário virtual do STF, por unanimidade,

---

mendicância devem cessar já. Anistia geral, carnaval semanal, licença de uso de máscaras, abonos para todos, esperanto a fraternidade universal. Não mais patriotismo de mama-bares e impostores hidrôpicos. Dinheiro livre, amor livre e uma igreja laica livre num estado laico livre.” (James Joyce – Ulisses – trad. Antônio Houaiss).” (BRASIL, 2016).

<sup>15</sup> Eis a ementa: “Ação Direta de Inconstitucionalidade. Lei Estadual regulamentando o direito constitucional à reunião pública para manifestação de pensamento (Artigos 15, inciso XVI, da Constituição da República, e 23, da Constituição do Estado). Estabelecimento de vedação ao uso de máscara ou qualquer outra forma de ocultar o rosto do cidadão com o propósito de impedir-lhe a identificação. Conceituação de arma para fins do exercício do direito fundamental em apreço. Determinação da autoridade à qual se deve fazer a prévia comunicação da manifestação. Alegação de vícios formais e materiais na norma impugnada. Teses trazidas pelos representantes e pelo amicus curiae que não se sustentam. Inexistência, na legislação em comento, de qualquer ofensa à ordem constitucional vigente. Representações que se julgam improcedentes, declarando, por conseguinte, a constitucionalidade da Lei Estadual nº 6.583/2013.” (BRASIL, 2016).



julgou constitucional a questão e reconheceu a existência de Repercussão Geral (Tema 912) na matéria, que ainda não teve julgamento de mérito proferido (BRASIL, 2016).

Hoje, mesmo que se reconheça a possibilidade de utilização de máscaras em manifestações públicas, ou seja, não reputando-se constitucionais legislações como a do Rio de Janeiro e semelhantes que proíbem o seu uso, a identidade da pessoa não é mais, necessariamente, protegida com a utilização de máscaras, a depender do seu modelo. Daí porque, caso o Supremo Tribunal Federal entenda pela inconstitucionalidade das referidas legislações, o Estado poderá aplicar a tecnologia de reconhecimento pela região dos olhos, o que tornaria inócua a utilização de máscaras sob o prisma da proteção da identidade individual.

Nesse sentido, a decisão judicial, embora ainda pendente, inaugura, desde já, especulações sobre nova discussão da temática e, eventualmente, pode-se analisar as premissas que possibilitem ou não a utilização da nova tecnologia, em quais situações, sob quais condições, com a observância de que regramentos. Mas, até lá, novas técnicas podem adicionar outras controvérsias ao caso, o que demanda do judiciário atenção, conhecimento e informação.

## CONCLUSÃO

Arriscar conclusões sobre uma discussão envolvendo uma complexidade de fatores, inter-relacionando questões que a Constituição Federal estabeleceu há mais de trinta anos, com ideias e fenômenos novos, emergentes, dinâmicos e, sobretudo, controversos, não é tarefa simples. Mais do que isso, as conclusões, ainda que sejam provisórias, por natureza, tendem, nessa seara, a cumprir um papel também dinâmico. Novos fatos sociais surgem, os problemas se transformam e as respostas se tornam obsoletas. Essas são características das ciências sociais aplicadas.

Há quase uma década, a sociedade civil procura discutir a constitucionalidade de um diploma legal que proíbe o uso de máscaras em manifestações, em nome da garantia da segurança pública. Ainda sem resposta, essa discussão ganhou um novo capítulo com o advento do reconhecimento facial pela região periocular. Dado o histórico interesse do Brasil em tecnologias de reconhecimento facial, a mesma tenderá a estar logo disponível para as autoridades públicas.





Cumpridos, assim, o problema de pesquisa e s objetivos lançados, ainda que sabido, é preciso registrar que as novas tecnologias, das quais o reconhecimento facial e reconhecimento pela região perioclar são exemplos, não são ontologicamente positivas ou negativas. Evidentemente, são instrumentos, ferramentas, e enquanto tais, tendem a ser potencialmente lesivas. Daí porque, se o Estado utiliza de tais meios, é preciso que haja a adequada regulamentação e utilização, sempre utilizando-se como parâmetro a Constituição Federal, essencialmente, no que tange aos direitos e garantias fundamentais.

## Referências

ALBUQUERQUE, Luciana Santos Guilhon; PEDRO, Rosa Maria Leite Ribeiro. Vigilância e visibilidade nas manifestações de 2013. **Anais da ReACT – Reunião de Antropologia da Ciência e da Tecnologia**. Porto Alegre, v.2, n.2, maio 2015. Disponível em: <http://ocs.ige.unicamp.br/ojs/react/article/view/1360>. Acesso em: 13 abr. 2021.

ALERJ (Assembleia Legislativa do Estado do Rio de Janeiro). **Lei nº 6.528, de 11 de setembro de 2013**. Regulamenta o artigo 23 da Constituição do Estado. Disponível em: <http://alerjln1.alerj.rj.gov.br/contlei.nsf/4734bd1980be7a2003256b2a0061e644/95394833846e60a583257be5005ec84a?OpenDocument>. Acesso em: 13 abr. 2021.

AMAZON. **We are implementing a one-year moratorium on police use of Rekognition**. 10 jun. 2020. Disponível em: <https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition?ots=1&slotNum=0&imprToken=6eb95095-0645-b999-2cb&tag=curbedcom06-20&linkCode=w50>. Acesso em: 10 abr. 2021.

BAHIA. Bahia apresenta resultado do Reconhecimento Facial na China. Secretaria de Segurança Pública. **Governo do Estado da Bahia**. Publicado em: 14 maio 2019. Disponível em: <http://www.ssp.ba.gov.br/2019/05/5695/Bahia-apresenta-resultado-do-Reconhecimento-Facial-na-China.html>. Acesso em: 13 abr. 2021.

BENAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. **Wiley Encyclopedia of Electrical and Electronics Engineering**, [s.l.], p. 1-28, 15 jun. 2015. John Wiley & Sons, Inc. DOI: <http://dx.doi.org/10.1002/047134608x.w8257>. Disponível em: <http://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257>. Acesso em: 10 abr. 2021.

BENTHAM, Jeremy. O Panóptico ou a casa de inspeção. In: SILVA, Tomaz Tadeu da. (Org.). **O Panóptico**. 2. ed. Belo Horizonte: Autêntica, 2008.



BORGES, Rosa Maria Zaia. Democracia, Liberdade de expressão e Black Blocs / Democracy, Freedom of Expression and Black Blocs. **Revista Direito e Práxis**, [S.L.], v. 8, n. 1, p. 354-385, 8 mar. 2017. Universidade de Estado do Rio de Janeiro. <http://dx.doi.org/10.12957/dep.2017.21203>. Acesso em: 13 abr. 2021.

BOWYER, Kevin W.; CHANG, Kyong; FLYNN, Patrick. A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition. **Computer Vision and Image Understanding**, [s.l.], v. 101, n. 1, p. 1-15, jan. 2006. Elsevier BV. DOI: <http://dx.doi.org/10.1016/j.cviu.2005.05.005>. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1077314205000822>. Acesso em: 10 abr. 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 11.140/2018**. Brasília, DF: Câmara dos Deputados, [2018b]. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2188455>. Acesso em: 12 abr. 2021.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 9.736/2018**. Brasília, DF: Câmara dos Deputados, [2018a]. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011>. Acesso em: 12 abr. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 13 abr. 2021.

BRASIL. **Projeto de Lei nº 3372/2004**. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=24969>. Acesso em: 12 abr. 2021.

BRASIL. Supremo Tribunal Federal. **Repercussão Geral no Recurso Extraordinário com Agravo 905.149/Rio De Janeiro [2016]**. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=4819708>. Acesso em: 13 abr. 2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Ação Civil Pública nº 1090663-42.2018.8.26.0100**. 37ª Vara Cível da Comarca de São Paulo. Ajuizado em 30 de agosto de 2018d. Disponível em: <https://esaj.tjsp.jus.br/cpopg/open.do>. Acesso em: 13 abr. 2021.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Ação de Produção Antecipada de Provas nº 1006616-14.2020.8.26.0053**. 1ª Vara da Fazenda Pública da Comarca de São Paulo. Ajuizado em: 02 fev. 2020c. Disponível em: <https://esaj.tjsp.jus.br/cpopg/open.do>. Acesso em: 13 abr. 2021.

FOUCAULT, Michel. **Vigiar e Punir**. Lisboa: Almedina, 2013.





INSTITUTO IGARAPÉ. **Infográfico reconhecimento facial no Brasil**. 2019. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>. Acesso em: 12 abr. 2021.

KRISHNA, Arvind. **IBM**. Armond, NY: 08 jun. 2020. Disponível em: <https://www.ibm.com/blogs/policy/wp-content/uploads/2020/06/Letter-from-IBM.pdf>. Acesso em: 10 abr. 2021.

LI, Jane. China's facial-recognition giant says it can crack masked faces during the coronavirus. **Quartz**. 18 fev. 2020. Disponível em: <https://qz.com/1803737/chinas-facial-recognition-tech-can-crack-masked-faces-amid-coronavirus/>. Acesso em: 10 abr. 2021.

LI, Stan Z.; JAIN, Anil K. (Orgs.). **Handbook of Face Recognition**, London: Springer London, 2011.

LYON, D. **Surveillance after Snowden**. Cambridge; Malden: MA: Polity Press, 2015.

MANN, Steve; NOLAN, Jason; WELLMAN, Barry. Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. **Surveillance & Society**, [s.l.], v. 1, n. 3, p. 331-355, 1 set. 2002. Queen's University Library. DOI: <http://dx.doi.org/10.24908/ss.v1i3.3344>. Disponível em: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3344>. Acesso em: 10 abr. 2021.

MARAUX, Alberto. Reconhecimento Facial captura 42 foragidos na folia. Secretaria de Segurança Pública. **Governo do Estado da Bahia**. Publicado em: 26 fev. 2020b. Disponível em: <http://www.ssp.ba.gov.br/2020/02/7296/Reconhecimento-Facial-captura-42-foragidos-no-Carnaval-de-Salvador.html>. Acesso em: 12 abr. 2021.

MARAUX, Alberto. SSP amplia cobertura do Reconhecimento Facial no Carnaval. Secretaria de Segurança Pública. **Governo do Estado da Bahia**. Publicado em: 17 fev. 2020a. Disponível em: <http://www.ssp.ba.gov.br/modules/noticias/article.php?storyid=7236>. Acesso em: 12 abr. 2021.

MENEZES NETO, Elias Jacob de. **Surveillance, Democracia e Direitos Humanos: os limites do Estado na era do big data**. 2016. 293 f. Tese (Doutorado em Direito) - Programa de Pós-Graduação em Direito, Universidade do Vale do Rio dos Sinos - UNISINOS, São Leopoldo, 2016.

METZ, Rachel. Think your mask makes you invisible to facial recognition? Not so fast, AI companies say. **CNN**. Publicado em: 12 ago. 2020. Disponível em: <https://edition.cnn.com/2020/08/12/tech/face-recognition-masks/index.html>. Acesso em: 10 abr. 2020.

NASCIMENTO, Silvânia. Reconhecimento Facial resulta nas prisões de 33 pessoas. Secretaria de Segurança Pública. **Governo do Estado da Bahia**. Publicado em: 29 abr. 2019. Disponível em: <http://www.ssp.ba.gov.br/2019/04/5613/Reconhecimento-Facial-resulta-nas-prisoas-de-33-pessoas.html>. Acesso em: 12 abr. 2021.



PASOLD, Cesar Luiz. **Metodologia da Pesquisa Jurídica**: teoria e prática. 11. ed. Florianópolis: Conceito Editorial; Millenium Editora, 2008.

POLLARD, Martin. Even mask-wearers can be ID'd, China facial recognition firm says. **Reuters**. 09 mar. 2020. Disponível em: <https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL>. Acesso em: 10 abr. 2021.

XINHUA. **Chinese company develops 3D facial recognition system**. 04 mar. 2020. Disponível em: [http://www.xinhuanet.com/english/2020-03/04/c\\_138842757.htm](http://www.xinhuanet.com/english/2020-03/04/c_138842757.htm). Acesso em: 10 abr. 2021.

