REVISTA DIGITAL DE DIREITO ADMINISTRATIVO

FACULDADE DE DIREITO DE RIBEIRÃO PRETO - FDRP

UNIVERSIDADE DE SÃO PAULO – USP

Seção: Artigos Científicos

O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina

What the eyes don't see, the cameras track: facial recognition in public security and its regulations in Latin America

Bruna Dias Franqueira; Ivar A. Hartmann; Lorena Abbas da Silva

Resumo: Com o avanço do uso de tecnologia de reconhecimento facial para fins de segurança pública em diversos países da América Latina, os efeitos discriminatórios ou danosos a outras garantias individuais provocados pelo emprego desses sistemas tornaram-se evidentes. As incertezas quanto à magnitude do potencial negativo do monitoramento biométrico em espaços públicos, bem como a opacidade decorrente do uso da inteligência artificial, fazem com que seja necessário compreender qual o atual cenário de garantias legais frente esse novo instrumento de vigilância. O presente trabalho pretende investigar qual a situação regulatória do uso de tecnologias de reconhecimento facial no campo da segurança em países da América Latina que possuem, pelo menos, legislação de proteção de dados pessoais. Além de apresentar casos de uso de tecnologia de reconhecimento facial na Argentina, Brasil, Chile Colômbia, Costa Rica, México, Nicarágua Panamá, Peru, República Dominicana e Uruguai, foram verificadas normas de abrangência nacional que eventualmente regulam esse uso ou se conectam diretamente com o tema, bem como leis sobre tratamento de dados pessoais por órgãos públicos, videovigilância e segurança pública.

Palavras-chave: Reconhecimento facial. Videovigilância. Regulação. Inteligência Artificial. Segurança pública. Proteção de Dados Pessoais.

Abstract: As the usage of facial recognition technologies advance in many countries across Latin America, the discriminatory/harmful effects to other individual guarantees provoked by the use of these systems became evident. The uncertanties as to the magnitude of biometric monitoring's negative potential at public spaces, as well as the opacity revolving the use of artificial intelligence, makes it necessary to understand which is the current legal guarantee scenario upon this new vigillance instrument. This article intends to investigate the facial recognition technologies' regulatory situation in the security field throughout Latin America in countries that possess, at least, some kind of personal data protection legislation. In addition to these cases of facial recognition in Argentina, Brazil, Chile, Colombia, Costa Rica, Mexico, Nicaragua, Panama, Peru, Dominican Republic and Uruguay, nation-wide legislation that adresses this issue or directly connects to this theme were verified, as well as the legislation adressing the management of personal data by public agencies, videosurveillance and public safety.

Keywords: Facial recognition. Videosurvaillance. Regulation. Artificial Intelligence. Public safety. Personal data protection.

DOI: http://dx.doi.org/10.11606/issn.2319-0558.v8i1p171-204

O QUE OS OLHOS NÃO VEEM, AS CÂMERAS MONITORAM: RECONHECIMENTO FACIAL PARA SEGURANÇA PÚBLICA E REGULAÇÃO NA AMÉRICA LATINA

Bruna Diniz FRANQUEIRA[*]
Ivar A. HARTMANN[**]
Lorena Abbas da SILVA[***]

1. Introdução

Nos últimos anos, a incorporação de sistemas de reconhecimento facial às câmeras de monitoramento elevou a política de vigilância a outro patamar. Inobstante a timidez, ou inexistência, do debate promovido pelo poder público acerca de seus efeitos negativos, o emprego em grande escala do reconhecimento facial está se tornando mais comum, sendo utilizado inclusive para realização de prisões[1]. Apontado por entes estatais como meio mais eficiente de gestão de risco, sua implementação é defendida em nome da proteção da segurança pública, com poucos esclarecimentos sobre as precauções adotadas para mitigar a restrição a direitos fundamentais como a liberdade de expressão, a privacidade e a proteção de dados pessoais (BOTELLO, 2016).

Um dos agravantes é a opacidade desse tipo de tecnologia, no sentido de que seu funcionamento, suas causas e efeitos, são uma incógnita para o regulador, por diversas razões. Entre elas está a falta de conhecimento técnico de noções básicas de estatística e computação, o que o impedem sequer de avaliar o mérito de diferentes alternativas de regulação (SCHERER, 2016, p. 371). Conforme Daugherty *et al.* (2016, p. 10) ressaltam, o reconhecimento facial não é um sistema de riscos

[*] *Bacharel em Direito Fundação Getúlio Vargas (FGV-Rio) e pesquisadora do Centro de Tecnologia e Sociedade (CTS/FGV Direito-Rio).*
[**] *Doutorado em Direito Público pela UERJ. Mestre em Direito Público pela PUC-RS. Mestre em Direito (LL.M.) pela Harvard Law School. Professor e Pesquisador da FGV Direito Rio. Coordenador do Centro de Tecnologia e Sociedade da FGV Direito Rio e do Núcleo de Ciência de Dados Jurídicos da FGV Direito Rio.*
[***] *Doutoranda em Políticas Públicas na Universidade Federal do Rio de Janeiro (PPED/IE/UFRJ) e pesquisadora no Centro de Tecnologia e Sociedade da Fundação Getúlio Vargas (CTS/FGV Direito-Rio) com bolsa do CNPq. Mestrado e graduação em Direito pela Universidade Federal de Juiz de Fora/MG*.
[1] Na cidade brasileira de Salvador, capital do estado da Bahia, o número de pessoas presas após serem identificadas por câmeras dotadas de tal sistema chegou a 129 em fevereiro de 2020 (G1 BAHIA, 2020).

similares ao de uma biometria típica, pois é justamente nas suas características diferenciadores que o rastreamento remoto em massa e secreto se sustenta[2].

De modo geral, para que alguém possa ser identificado via reconhecimento facial, primeiro um algoritmo deve localizar o rosto da pessoa na imagem – processo chamado de detecção de face. Uma vez detectada, essa face é "padronizada" – dimensionada e alinhada – para que todas as outras faces processadas pelo algoritmo estejam na mesma posição, facilitando a comparação dos rostos. Em seguida, o algoritmo extrai as características da face que podem ser quantificadas de forma numérica, como a distância entre os olhos, nariz e boca ou a textura da pele. A padronização é importante pois tais características serão analisadas em suas variações estatísticas (KLARE *et al.*, 2012, p. 1791)[3], uma vez que os elementos tenham sido transformados em representações matemáticas, conectados de forma individualizada. Por último, o algoritmo examina grupos de imagens de rostos e emite uma pontuação que reflete a semelhança entre as características[4] das faces que constam no banco de dados (DAUGHERTY *et al.*, 2016, p. 9) e aquela que está sendo submetida a identificação.

A análise ocorre, portanto, diretamente com base em um dado do tipo biométrico, ou seja, um dado imutável que identifica ou verifica a identidade de alguém por suas características físicas ou comportamentais intrínsecas (LYNCH, 2020, p. 4). Essa análise só é possível porque o sistema foi, inicialmente, ensinado a rotular e combinar informações, por meio da classificação manual de um grupo de dados testes (MARGULIES, 2016, p. 1067-8; KLARE *et al.*, 2012, p. 1790), naquilo que se denomina técnica de aprendizado de máquina supervisionado. Por ser essencial para própria elaboração do algoritmo capaz de identificar biometricamente diversos rostos que sejam fornecidos para sua análise, a etapa de aprendizado da máquina demanda atenção e cuidado, pois poderá levar a algoritmos distintos diante de dados distintos (KLARE *et al.*, 2012, p. 1791)[5].

Desse modo, as soluções de reconhecimento facial atualmente em uso e descritas ao longo desse estudo empregam elementos de inteligência artificial (IA), aperfeiçoando a análise das milhões de imagens capturadas automaticamente. Um conceito

[2] Nas palavras dos autores: "Face recognition isn't just a different biometric; those differences allow for a different kind of tracking that can occur from far away, in secret, and on large numbers of people". (DAUGHERTY *et al.*, 2016, p. 10).

[3] Para os autores: "(...) automated face recognition algorithms are ultimately based on statistical models of the variance between individual faces". (KLARE *et al.*, 2012, p. 1791).

[4] Sobre esse aspecto, vale destacar que a composição do conjunto de dados de treinamento influencia diretamente nos tipos de imagens que um algoritmo é capaz de examinar de maneira mais ágil e precisa. Em um conjunto de treinamento com mais dados de uma determinada população (ex.: mais imagens de homens ou pessoas brancas), o algoritmo identifica melhor membros desse grupo em comparação com de outros (ex.: mulheres ou pessoas negras). (DAUGHERTY *et al.*, 2016, p. 9).

[5] Nas palavras dos autores: "However, different versions of this algorithm can be generated by training it with different sets of face images, where the sets have been separated based on demographics". (KLARE *et al.*, 2012, p. 1791).

útil de IA para discussões sobre sua regulação é oferecido por Scherer (2016, p. 362): "refere-se a máquinas capazes de realizar tarefas que, se desempenhadas por um humano, seriam descritas como exigindo inteligência." Isso não significa, é claro, que a definição de IA seja simples e livre de qualquer controvérsia. Segundo Turner (2019, p. 6), ainda não foi possível estabelecer uma definição unânime do que seja uma inteligência artificial. Entretanto, para esse autor, uma definição possível deve pressupor a habilidade de uma entidade não natural de fazer escolhas por um processo avaliativo. Já Kaplan e Haenlein (2019), entendem inteligência artificial como a capacidade de um sistema de interpretar corretamente dados externos, aprender com esses dados e utilizá-los para alcançar objetivos e realizar tarefas específicas a partir de adaptações flexíveis. Os elementos essenciais dessas conceituações estão presentes no caso de aplicações de reconhecimento facial.

A depender da natureza da técnica empregada, no entanto, os ganhos significativos na velocidade de obtenção dos resultados de correspondência entre a pessoa identificada e a base de dados são proporcionados às custas da transparência, explicabilidade, justiça, não discriminação, e outros princípios que deveriam nortear a aplicação de sistemas de reconhecimento facial[6]. Com o uso de técnicas de redes neurais, por exemplo, eventuais violações à privacidade, ou decisões discriminatórias que venham a ser tomadas pelo sistema, carecem de meios inteligíveis de justificação e verificação, dado que o próprio sistema gera, de forma autônoma, camadas escondidas para fins de uma identificação fracionada de cada um desses elementos - e depois os conecta também de forma independente (MARGULIES, 2016, p. 1067-8). Ou seja: se a capacidade de explicar os elementos que pesaram na decisão não for inserida no software desde o seu desenho inicial, nem os próprios desenvolvedores saberão indicar, após cada rosto identificado, as razões específicas que levaram a máquina àquele resultado (BLACK; MURRAY, 2019, p. 16).

De todos os sistemas biométricos, esse é o que tem as mais altas taxas de falsos positivos (quando a máquina erroneamente identifica a face buscada como sendo aquela de uma pessoa registrada na base de dados) e falsos negativos (quando a face buscada é de fato de uma pessoa registrada na base de dados, mas a máquina não identifica isso), o que acaba comprometendo sua eficácia. E tais taxas elevadas de falsos positivos afetam, sobretudo, grupos já marginalizados socialmente[7], como

[6] Lynch (2019), em um relatório promovido pela Electronic Frontier Foundation, enumerou nove princípios a serem adotados em atos normativos que busquem suprir os vácuos legislativo para limitar o uso de sistemas de reconhecimento facial - mitigando os problemas. Tais princípios são necessários diante dos desafios também apontados pela autora como a falta de precisão dos sistemas, falta de consentimento (ou até mesmo conhecimento) para captura dos dados, impactos em garantias como liberdade de expressão e de associação, impacto diferenciado em pessoas negras e riscos de segurança, diante de ameaça de atores internos e externos. (LYNCH, 2019, p. 6-12).

[7] Na ferramenta Amazon Rekognition, por exemplo, foram identificadas taxas de falsos positivos de 40% para pessoas não-brancas e de 5% para pessoas brancas. (WHITTAKER *et al.*, 2018, p. 15-6). Em pesquisa realizada pelo National Institute of Standards and Technology (NIST), a qual avaliou 189 algoritmos de 99 desenvolvedores de reconhecimento facial para medir as ocorrências de falsos positivos e falsos negativos, verificou-se uma taxa mais alta de falsos positivos para rostos asiáticos, negros e indígenas em relação

pessoas negras e mulheres (GEBRU *et al.*, 2018; LYNCH, 2020, p. 9-10; WHITTAKER *et al.*, 2018, p. 16; SCOTTISH PARLIAMENT, 2020, p. 15; FUSSEY; MURRAY, 2019, p. 21-22). O uso de tecnologias de reconhecimento facial é, portanto, especialmente arriscado em contextos nos quais determinados grupos já são historicamente objeto de tratamento discriminatório. Esse é justamente o caso de negros e pardos no âmbito da segurança pública no Brasil, seja sob o ponto de vista das prisões em flagrante (Defensoria Pública do Rio de Janeiro, 2020), seja na composição do sistema prisional (MONTEIRO; CARDOSO, 2013), no qual a taxa de encarceramento para cada 100 mil habitantes em 2012 era de 191 para brancos e 292 para negros (Secretaria-Geral da Presidência da República e Secretaria Nacional de Juventude, 2015, p. 34).

Infelizmente, os riscos associados ao emprego de sistemas de reconhecimento facial em câmeras de monitoramento no Brasil, por exemplo, não têm motivado suficiente preocupação e adequada atenção no debate público e por parte dos órgãos reguladores. Ainda que por vezes seja considerado mais vantajoso em relação a outros métodos de identificação biométrica (como a leitura da digital ou da íris), por dispensar que o indivíduo realize alguma ação para que o reconhecimento aconteça (SILVA; CINTRA, 2015, p. 2), esses sistemas promovem vigilância intrusiva da privacidade e diminui as fronteiras entre espaço público e espaço privado (FUSSEY; MURRAY, 2019, p. 19-20).

Diante disso, combinando as abordagens descritiva e exploratória de pesquisa (DESLAURIERS; KÉRISIT, 2008), pretende-se investigar – e aí está delimitado nosso problema de pesquisa – a situação regulatória do uso de tecnologias de reconhecimento facial no campo da segurança pública em países da América Latina que possuem, pelo menos, legislação de proteção de dados pessoais[8]. A existência dessa lei como critério para abordagem do país neste trabalho justifica-se por dois motivos. Primeiro, por uma questão formal, relativa ao escopo da pesquisa, tendo em vista a quantidade de países que compõem a América Latina, alguns inclusive com populações muito pequenas. Segundo, porque o reconhecimento facial envolve a coleta e o tratamento de dados pessoais que devem ser apropriadamente regulados em lei específica, dispondo sobre as garantias fundamentais dos cidadãos perante aqueles que exploram esses dados. Os países que atendem a esse critério são: Argentina, Brasil, Chile, Colômbia, Costa Rica, México, Nicarágua, Panamá, Peru, República Dominicana e Uruguai.

a pessoas brancas. Mulheres negras são o grupo mais atingido, segundo o estudo. (NISTIR, 2019). Esses erros podem sustentar acusações falsas, fazendo com que um dos direitos mais caros à sociedade, o direito à liberdade, seja privado sem provas concretas para fazê-lo.

[8] Parte da escolha pela abordagem dessa região resulta também de uma cerca uniformidade da proteção de direitos humanos na América Latina, o que dá alguma similaridade ao tratamento de questões de restrições desses direitos para atingir objetivos de segurança pública, especialmente quando se trata da proteção da dignidade da pessoa humana. (LEGALE; VAL, 2017).

Recorre-se neste trabalho à pesquisa bibliográfica e documental (SILVEIRA; CÓRDOVA, 2009, p. 37) para levantamento de referências sobre o tema. As informações utilizadas são tanto de natureza direta, como leis e decretos, quanto indireta, como artigos, relatórios de pesquisa e livros. Além das leis de proteção de dados pessoais, sempre que possível, são abordadas normas que regulam a atividade vigilante por parte dos atores que têm incorporado as tecnologias de reconhecimento facial para analisar como o tema é tratado no ordenamento nacional.

Importante destacar que o objetivo não é empreender uma pesquisa de direito comparado sobre os países citados acima. Para além de questões relacionadas às condições de acesso a fontes e materiais sobre o ordenamento jurídico estrangeiro, as controvérsias apresentadas no texto não são melhor solucionadas por uma simples contraposição entre as diversas possibilidades de tratamento jurídico aos quais o objeto de pesquisa está submetido em cada um dos países onde é utilizado. Em razão da atualidade do tema e a recente intensificação do uso das técnicas de reconhecimento facial em massa, muitos arranjos institucionais estão em fase de construção e implementação, tornando difícil generalizar certos resultados além do próprio contexto. O objetivo da contribuição oferecida pelo presente estudo, ao responder a pergunta de pesquisa, é permitir o conhecimento das diferentes estratégias regulatórias desses países latino-americanos e julgá-las por seu valor de face. Evidentemente, futuros estudos devem incluir análises menos abrangentes e mais aprofundadas, incluindo estudos de direito comparado, que pressupõe o conhecimento e discussão dos mais diversos aspectos do sistema jurídico de cada país.

Na próxima seção são apresentados casos de incorporação da tecnologia de reconhecimento facial agrupados por país, expondo os fundamentos legais sobre os quais a prática eventualmente se sustenta. Um levantamento por meio de pesquisa bibliográfica e documental foi realizado para mapear a utilização dos sistemas de reconhecimento facial nos países selecionados, bem como normas de abrangência nacional que eventualmente regulam esse uso ou se conectam diretamente com o tema, como leis sobre tratamento de dados pessoais por órgãos públicos, videovigilância e segurança pública. Dessa maneira, o estudo constitui também exemplo de análise da complexa regulação setorial de uma aplicação de inteligência artificial (COUTINHO FILHO, 2018, p. 270), com especial preocupação para os aspectos da transparência e *accountability* (DESAI; KROLL, 2017) e, ao mesmo tempo, parte do pressuposto da complexidade da proteção de dados (ALBERS, 2016), que é um fator evidente da regulação do uso de reconhecimento facial.

2. Casos concretos e bases legais

2.1 Argentina

Pereyra (2018, p. 257-9) destaca o pioneirismo da Argentina em relação à adoção de ferramentas biométricas. Para isso, o país desenvolveu ao longo dos anos uma

estrutura normativa que naturalizou o emprego da biometria, inclusive como requisito para o exercício da cidadania. Por outro lado, isso abriu a porta para usos abusivos dos dados pessoais para monitoramento. Em abril de 2019, a Resolução 398/MJYSGC/2019[9] implementou na capital argentina o *Sistema de Reconocimiento Facial de Prófugos* (SRFP), programa para identificação via reconhecimento facial de pessoas foragidas (*Consulta Nacional de Rebeldías y Capturas* - CONARC) (GARAY, 2019, p. 3-4). Na cidade, onde existem mais de 7 mil câmeras de vigilância, o SRFP foi instalado em 300 delas (LUNA, 2019) e motivou cerca de 174 prisões em menos de três meses (INFOBAE, 2019).

A utilização do SRFP é parte da política de segurança, prevista na Lei nº 5.688/2016 (*Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires*)[10] e está conectada com outros textos legais argentinos[11], que estabelecem princípios e deveres para o funcionamento de sistemas como esse. A própria Resolução 398/MJYSGC/2019 indica os princípios da proporcionalidade e da razoabilidade no emprego do sistema para fins de segurança pública e a necessidade de verificação do impacto em garantias como o direito à imagem, à intimidade e à privacidade, guiada pela pretensão de intervenção mínima. O texto, entretanto, logo após o reconhecimento de tais garantias, destaca que não há necessidade de obtenção de consentimento para coleta dos dados faciais dos cidadãos argentinos, apoiando-se na exceção estabelecida pela Lei 25.326/2000, lei de proteção de dados pessoais argentina. O fundamento da excepcionalidade não é exclusivo do contexto argentino e sim um argumento presente em quase todas as legislações encontradas.

Com relação aos possíveis erros na identificação das pessoas, as autoridades argentinas atribuem o problema à base de dados do CONARC[12]. Em agosto de 2019, um homem passou 6 dias preso após ter sido identificado equivocadamente pelas câmeras de reconhecimento facial nas ruas de Buenos Aires. A pessoa que havia cometido o delito possuía um nome muito parecido e, segundo o secretário de Justiça e

[9] Resolución nº 398/2019, disponível em: https://bit.ly/2OAuCs4.

[10] Ley 5.688/2016, disponível em: http://www2.cedom.gob.ar/es/legislacion/normas/leyes/ley5688.html.

[11] São estes: (i) Constitución de la Nación Argentina; (ii) Constituición de la Cuidad Autónoma de Buenos Aires (artigos 12 e 34); (iii) Ley nº 5.688/2016 (Sistema Integral de Seguridad Pública de la Ciudad Autónoma de Buenos Aires), (artigos 68, 75, ponto 7, 474); (iv) Ley nº 24.059/1991 (Seguridad Interior); (v) Decreto PEN 346/09, (criou a base de Consulta Nacional de Rebeldías y Capturas - CONARC); (vi) o Decreto PEN 1766/11 (cria o Sistema Federal de Identificación Biométrica para la Seguridad - SIBIOS); (vii) Ley 13.482 (alterada pela Lei 17.617) (criou o Registro Nacional de las Personas - RENAPER); (viii) Ley 25.326/2000 (Ley de Protección de los Datos Personales).

[12] "El objetivo preliminar trazado fue alcanzar una tasa alta de reconocimiento exitoso. Por tal motivo se han realizado sucesivos ajustes del software a efectos de generar alertas recién cuando se alcanza un porcentaje elevado de coincidencia biométrica. Con la configuración actual, la tasa de aciertos de las alertas que dispara el SRFP se encuentra por encima del 90%. El margen de error, además, en la mayor parte de las ocasiones obedece a errores cuyo origen está en la base de datos del CONARC, de la cual se nutre el sistema local (por caso, el más común es la indicación y consecuente carga errónea del documento de identidad de la persona requerida por la justicia)". Resposta à pergunta C (p. 4) da consulta realizada pela Asociación por los Derechos Civiles, disponível em: https://bit.ly/2SibvET.

Segurança da capital, Marcelo D'Alessandro, o número do documento de identidade nacional do rapaz preso estava errado em todos os bancos de dados do país. O secretário refutou expressamente a hipótese de falso positivo[13] do sistema (R3D, 2019).

Conforme esclarece a *Asociación por los Derechos Civiles* (ADC) (2019a, p. 2-3), a maior parte dos sistemas de reconhecimento facial que operam atualmente no território argentino foram implementados mediante decretos ou resoluções do poder público, com fundamento em normas que excepcionam a coleta e processamento de dados em defesa da segurança nacional, mas sem a devida salvaguarda de direitos fundamentais. Segundo a *Asociación*, as normas que preveem o uso da biometria para fins penais violam o princípio da proporcionalidade porque constituem limitação a um direito constitucional sem cumprir o requisito da explícita previsão em lei, sancionada pelo legislativo, com sua finalidade, necessidade e proporcionalidade bem definidas.

A ADC realizou consulta pública perante o governo para obter uma explicação mais detalhada ou o acesso ao código-fonte do sistema. Como resposta, foi dito que a obrigação de prover tais informações é excepcionada nos casos de proteção por direito intelectual, segredo comercial ou industrial e segredo profissional, ou quando a divulgação desses dados possa provocar um risco à sociedade. O Governo da Cidade de Buenos Aires declarou ainda que a taxa de acerto do sistema ultrapassa os 90% – o que deveria ser confirmado por auditoria independente – e reproduziu informações genéricas que já haviam sido publicadas no anúncio de implementação dos sistemas de reconhecimento facial, alegando que testes foram realizados com uma população controlada da equipe de trabalho, empregando variações das condições da câmera (ângulo, iluminação, ambientes), e também de adereços utilizados pelos indivíduos testados (barba, bigode, gorro, capuz, capacete) (UCCIFERRI, 2019).

No final de outubro de 2019, a ADC ingressou com uma ação perante o Tribunal Superior de Justiça da Cidade de Buenos Aires para que o SRFP seja considerado inconstitucional e a Resolução 398/MJYSGC/2019 perca sua vigência (ADC, 2019b). A apreciação da ação pelo tribunal ainda está pendente[14].

2.2 Brasil

Segundo relatório do Instituto Igarapé (2019), a utilização de sistemas de reconhecimento facial no Brasil em diferentes áreas é reportada pelo menos desde 2011. Apesar da intensa utilização, destaca-se que há grande dificuldade em acessar as

[13] Quando um sistema de reconhecimento facial gera um resultado "falso negativo" significa que ele não identificou que duas imagens correspondem à mesma pessoa; já os "falsos positivos", ocorrem quando imagens de duas pessoas diferentes são consideradas como representativas do mesmo indivíduo (NISTIR 8280, 2019).

[14] Consulta Processo nº 17642, página do Tribunal Superior de Buenos Aires (https://bit.ly/3fvNxjJ).

informações relativas à avaliação dos impactos da implementação dessa tecnologia no território brasileiro.

Na cidade de São Paulo, o uso de câmeras de reconhecimento facial no sistema de transporte público ocorre desde 2017. Só nos dois primeiros anos, mais de 300 mil bilhetes foram bloqueados por suposto uso indevido (GARAY, 2019, p. 7). Em abril de 2018, a ViaQuatro, concessionária responsável pela linha 4-Amarela dos trens metropolitanos da capital paulista, anunciou também a utilização de tecnologia de reconhecimento facial em painéis publicitários de algumas estações para monitorar as reações dos usuários da linha (CARVALHO, 2018), o que à época acabou sendo impedido judicialmente[15].

No Rio de Janeiro, a tecnologia passou a fazer parte das políticas de proteção à segurança pública em 2019. Segundo informações da Polícia Militar do Estado do Rio de Janeiro (PMERJ), o projeto-piloto teve início no Carnaval com a instalação de 34 câmeras. A implementação dos sistemas foi feita de forma gratuita, por meio de um convênio com a empresa do ramo de telefonia Oi. O sistema permite o envio de informações online para o Centro Integrado de Comando e Controle, onde os operadores analisaram os alertas de correspondência (PMERJ, 2019a; 2019b). Em julho de 2019, iniciou-se uma segunda fase para expansão do projeto na cidade carioca. O número de câmeras com reconhecimento facial saltou de 34 para 140. No mesmo mês, pelo menos duas pessoas foram vítimas de falsos positivos no Rio de Janeiro (G1 RIO, 2019; ALMEIDA, 2019).

Não existe no Brasil norma que determine os limites e padrões a serem seguidos por sistemas de videovigilância, muito menos para aqueles capazes de fazer reconhecimento facial. Em sentido contrário, a Portaria nº 793 do Ministério da Justiça e Segurança Pública, emitida em outubro de 2019, autoriza o uso de dinheiro do Fundo Nacional de Segurança Pública para o "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* – OCR, uso de inteligência artificial ou outros" (BRASIL, 2019). Segundo Nunes (2019, p. 70), o país tem caminhado na contramão do estabelecimento de premissas básicas de transparência de dados sobre segurança pública e criminalidade. De acordo com o autor, os estados de Minas Gerais, Espírito Santo, Pará e o Distrito Federal declararam estar em processo de contratação/implementação da tecnologia de reconhecimento facial para o trabalho de policiamento. O mesmo

[15] Na ocasião, o Instituto Brasileiro de Defesa do Consumidor (IDEC) ingressou com uma ação civil pública contra a ViaQuatro, alegando, entre outros argumentos, violação do direito à intimidade e à vida privada, do direito à informação e à liberdade de escolha, já que a medida se impõe a todos os usuários que utilizam o serviço de transporte indistintamente. A Justiça de São Paulo determinou que a empresa interrompesse a coleta de dados de imagem, de som ou quaisquer outros por meio das câmeras, ordenando o desligamento das mesmas em um prazo de 48 horas, sob pena de multa diária de R$50 mil em caso de descumprimento. (BRASIL, 2018). A petição inicial do IDEC está disponível para consulta em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. E a decisão do TJSP: https://bit.ly/39uRFg7.

acontece com estados do Nordeste que, desde 2019, estudam projetos para tornar a região mais conectada (FOLHA DE SÃO PAULO, 2019).

Diante dessa situação, as garantias mínimas que deveriam ser observadas nesse uso específico estão previstas na Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD), visto que o dado biométrico é expressamente reconhecido como dado pessoal e de natureza sensível. No entanto, apesar dos princípios gerais de proteção e direitos do titular previstos pela LGPD serem plenamente aplicáveis ao uso de reconhecimento facial, a lei excepciona de sua aplicação o tratamento de dados para manutenção de segurança pública e persecução ou mitigação de prática de delitos.

Um ponto sensível em relação à LGPD e a apreciação de vetos e alterações durante os últimos tempos, diz respeito ao seu artigo 20, que garante ao titular os direitos à explicação e à revisão das decisões tomadas unicamente com base em tratamento automatizado. Entre a redação proposta inicialmente e a atual, foi retirada do texto a expressão "pessoa natural", como responsável para a realização das referidas revisões, abrindo margem para que isso seja feito de maneira também automatizada. Essa opção fragiliza de certa maneira os direitos dos titulares frente ao agente de tratamento, além de ser um reforço ao poder desse agente que, pelo §2º do mesmo artigo, já poderia se eximir de fornecer explicações claras sobre os critérios e procedimentos adotados em observância ao segredo comercial e industrial.

Em 2019, dois decretos presidenciais (Decreto nº 10.046/2019[16] e Decreto nº 10.047/2019[17]) possibilitaram a criação de uma grande base unificada de dados pessoais dos cidadãos que será compartilhada entre órgãos do governo federal e também do Legislativo e Judiciário. Os decretos evidenciam os atuais riscos de estabelecimento de sistemas de vigilância em massa, uma vez que permitem o armazenamento de dados biométricos faciais, associados a diversos outros dados biográficos[18]. Em sede de parecer, Lucia Maria Teixeira Ferreira (2019, p. 28-9), na qualidade de membra da Comissão de Proteção de dados e Privacidade da OAB/RJ, sugere que a criação das bases integradora e temática pelo artigo 2º, incisos VI e VII do Decreto 10.046/2019, e também a criação de termos estranhos à LGPD, aumentam os riscos de cruzamento de informações biométricas com informações biográficas

[16] Decreto nº 10.046/2019, de 09 de outubro de 2019. Disponível em: https://bit.ly/2OR7t48.

[17] Decreto nº 10.047/2019, de 09 de outubro de 2019. Disponível em: https://bit.ly/32ONbk7.

[18] Segundo o artigo 18 do Decreto nº 10.046/2019 (grifos nossos): "Art. 18. A **base integradora** será, inicialmente, disponibilizada com os dados biográficos que constam da **base temática** do CPF. § 1º Os atributos biográficos e cadastrais que inicialmente comporão a base integradora serão, no mínimo, os seguintes: I - número de inscrição no CPF; II - situação cadastral no CPF; III - nome completo; IV - nome social; V - data de nascimento; VI - sexo; VII - filiação; VIII - nacionalidade; IX - naturalidade; X - indicador de óbito; XI - data de óbito, quando cabível; e XII - data da inscrição ou da última alteração no CPF. **§ 2º A base integradora será acrescida de outros dados, provenientes de bases temáticas, por meio do número de inscrição do CPF, atributo chave para a consolidação inequívoca dos atributos biográficos, biométricos e cadastrais**" (...).

como “fatos de sua vida” e “grupo familiar”, o que pode ser usado para controle político.

Esse tipo de medida legislativa confronta mecanismos necessários para garantir privacidade e segurança em bases de dados que contenham dados biométricos. Lynch (2020, p. 25-8), por exemplo, ao sugerir os nove princípios que devem ser seguidos por formadores de políticas públicas de reconhecimento facial, alerta expressamente para a necessidade de não armazenar os dados biométricos relacionados a outros dados biográficos, ou, no mínimo, utilizar mecanismos de anonimização.

2.3 Chile

Um dos primeiros usos para a biometria no Chile foi no sistema de identificação e migração. Desde setembro de 2013, o Serviço de Registro e Identificação chileno utiliza o Sistema de Identificação Multibiométrica para complementar as tradicionais impressões digitais com os dados de biometria facial dos cidadãos chilenos (ADC, 2017, p. 3).

Outro exemplo de aplicação da biometria da face é o sistema instalado no metrô da cidade chilena de Valparaíso para controlar os usuários com benefício de redução da tarifa de transporte (DERECHOS DIGITALES, 2018). Sobre esse caso, Garay (2019, p. 7) alerta para a inexistência de informações sobre as perdas financeiras que possíveis fraudes acarretariam para a rede de transportes, dificultando a análise da proporcionalidade da medida.

Observa-se que a adoção dos sistemas de reconhecimento facial no Chile cresce e se expande[19] para além dos fins de segurança pública e proteção de espaços comerciais tradicionalmente controversos[20]. Apesar de a Lei nº 19.628 de 1999[21] - Lei de Proteção da Vida Privada - não explicitar que dados biométricos são dados pessoais, é possível inferir que os dados biométricos se enquadraram na categoria de dados sensíveis (IGLESIAS; CASTELLARO, 2017, p. 72-3), cujo tratamento segue dependente de autorização legal e consentimento do titular. O consentimento só é dispensado, segundo os artigos 20 e 22 da lei chilena, para a coleta de dados realizada por

[19] Sobre o crescimento do uso de reconhecimento facial no Chile, ver: https://bit.ly/2UFjVbt e https://bit.ly/2SsJhGN.

[20] O anúncio de instalação de câmeras com reconhecimento facial no centro comercial Mall Plaza, por exemplo, chamou atenção à época para duas questões: primeiro, se trata de uma intervenção privada sobre um espaço semi-público; e segundo, quando o software utilizado passou por testes pela Polícia de Investigações chilena, uma taxa de falsos positivos de cerca de 90% foi detectada (GARAY, 2019, p. 6-7). Mais informações sobre o caso em: https://bit.ly/2vfEFMs; https://bit.ly/38ddXCB. Não se ignora, é claro, os potenciais benefícios das parcerias público privadas, como no âmbito da concretização do direito à saúde (SILVA e SILVA, 2019), porém é preciso cuidado quando tais parcerias viabilizam implementações de novas tecnologias que, caso levadas à cabo exclusivamente pela Administração, seriam sujeitas a restrições para proteção de direitos fundamentais.

[21] Ley de Protección de la Vida Privada, disponível em: https://www.leychile.cl/Navegar?idNorma=141599.

órgãos públicos em cumprimento das funções de sua competência previamente estabelecidas por lei.

Entretanto, não há lei regule o emprego dos sistemas de videovigilância com reconhecimento facial (BECKER *et al.*, 2018, p. 41-3; CANALES; LARA, 2018, p. 30-1). De acordo com Becker *et al (*2018, p. 41-2), o país conta apenas com leis e decretos legislativos que determinam a obrigatoriedade ou autorização do uso de sistemas de vigilância em áreas específicas ou situações concretas - como instituições financeiras - e com dispositivos sobre segurança pública, cujas previsões serviram de base legal para celebração do convênio com a polícia ostensiva chilena (os *carabineros*) que propiciou a expansão do monitoramento no país.

Sem uma lei que estabeleça os limites da expansão do monitoramento, o Conselho Para a Transparência (CPLT, na sigla em espanhol) do Chile recomendou - Ofício nº 2309 - a não utilização de dispositivos de videovigilância para fins de segurança, quando existirem meios menos invasivos à vida privada (CONSEJO POR LA TRANSPARENCIA, 2017a, p. 4; 2017b). Essa garantia se alinha ao posicionamento da Suprema Corte quando determinou que há expectativa de privacidade mesmo em espaços públicos, sendo possível interpretar que a coleta de dados biométricos por meio de sistemas de reconhecimento facial frustra tal pretensão, assim como a pretensão do anonimato (BECKER *et al.*, 2018. p. 42). Apesar da série de medidas de segurança para garantir a proteção da confidencialidade e integridade dos dados coletados, como (i) a proibição de comunicação de dados, exceto em caso de flagrante delito; (ii) a definição clara do perfil de quem poderá acessar as imagens - mas sem expor os critérios para essa definição, e (iii) a encriptação dos dados, em caso de transferência (CONSEJO POR LA TRANSPARENCIA, 2017a, p. 4-5), o documento não possui caráter vinculante (CANALES; LARA, 2018, p. 31), tornando suas previsões opcionais em cada um dos municípios.

O artigo 20 da Lei nº 19.628/99, referenciada acima, e a Lei 20.931 de 2016[22] (que possibilita a troca de dados sobre acusados ou condenados entre Ministério Público, *carabineros* e Polícia de Investigações) são utilizados como base legal para a captura e gravação de imagens obtidas por câmeras de videovigilância (CONSEJO PARA LA TRANSPARENCIA, 2017a, p. 3). Esses dados, por força do artigo 22 da Lei de Proteção da Vida Privada, devem constar do Serviço de Registro Civil e Identificação (CONSEJO PARA LA TRANSPARENCIA, 2017a, p. 5), tornando-se acessíveis para vários órgãos simultaneamente, o que pode representar um risco à proteção desses dados.

Conforme sinalizam Iglesias e Castellaro (2017, p. 85-8), a videovigilância e o reconhecimento facial com sistemas biométricos devem estar previstos na estrutura

[22] Ley nº 20.931 de 2016, Facilita la Aplicación Efectiva de las Penas Establecidas para los Delitos de Robo, Hurto y Receptación y Mejora la Persecución Penal en dichos Delitos. Disponível em: https://www.leychile.cl/Navegar?idNorma=1092269.

normativa de maneira que não interfiram arbitrária ou ilegalmente na privacidade ou em outros direitos dos indivíduos, ou seja, devem estar em plena conformidade com os princípios de legalidade, necessidade e proporcionalidade. Segundo os autores, do ponto de vista regulatório o panorama chileno é obscuro e atrasado. Isso tem inúmeras consequências no campo da videovigilância biométrica, que vão desde a violação da privacidade até os chamados efeitos panópticos sobre os cidadãos que, ao serem constantemente monitorados, deixam de agir naturalmente, situação na qual os direitos à liberdade de expressão, de criação, de reunião, entre outros, são fortemente restringidos (IGLESIAS; CASTELLARO, 2017, p. 85-8).

2.4 Colômbia

A classificação de certos dados pessoais como biométricos na Colômbia é complexa e via de regra ocorre em função de sua natureza e circulação. Para a *Delegatura de Protección de Datos* colombiana, uma fotografia ou um vídeo, por exemplo, podem ser classificados como dado biométrico e, portanto, sensível, apenas quando alguma técnica é implementada para "a extração de elementos particulares da face", seguindo a ideia do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (FUNDACIÓN KARISMA, 2019, p. 6-9).

Essa interpretação se aplicaria ao caso das imagens capturadas por câmeras instaladas no sistema de transporte público TransMilenio, em Bogotá, a partir de 2015 (TECNOSFERA, 2019). A experiência, no entanto, fracassou, conforme avaliam instituições como a *Fundación Karisma* (2018), não só pelo claro desrespeito à diversas garantias fundamentais, mas também por conta de uma grave falha técnica: o Fundo de Vigilância e Segurança, responsável pelo projeto que custou mais de 11 milhões de pesos, esqueceu da necessidade de uma lista de referência prévia, com os dados biométricos faciais das pessoas a serem identificadas pelos sistemas (MONTES, 2020). Ou seja, o sistema não possuía uma base com dados biométricos faciais prévios dos indivíduos que se buscava monitorar pelas imagens de vigilância.

De todo modo, caso essa falha não tivesse ocorrido, não existiriam limitações legais à coleta dos dados imagéticos (fotos e vídeos), apesar de sua natureza sensível. Isso porque, de acordo com a Corte Constitucional da Colômbia[23] - no exercício do controle de constitucionalidade -, os princípios da lei de proteção de dados colombiana, Lei 1581/2012[24], se aplicam a todos os casos de processamento de dados pessoais, exceto para situações específicas, como composição de bancos de dados de inteligência, controle de lavagem de dinheiro, financiamento do terrorismo e informação estatística oficial (FUNDACIÓN KARISMA, 2019, p. 14), justificativas oferecidas pelos governos para realizar investidas de controle massivo, como esse caso da TransMilenio.

[23] Sentencia C-748-11. Disponível em: https://bit.ly/3kZdquQ.
[24] Ley Estatutaria 1581 de 2012, disponível em: https://bit.ly/3aJlJpT.

Nos arredores do estádio Atanasio Girardot, na cidade de Medellín, equipamentos com reconhecimento facial também foram instalados para monitorar o espaço especialmente em dias de jogo. Outro projeto, visando expandir a vigilância em espaços esportivos, foi previsto também para as cidades de Cali, Bogotá e Barranquilla (FUNDACIÓN KARISMA, 2018, p. 27-8). Em Cali, a vigilância em larga escala já é uma realidade: na pequena cidade que fica a sudoeste de Bogotá, mais de 250 câmeras do governo monitoram as pessoas e veículos que transitam pelas vias públicas. São utilizadas também câmeras corporais (*bodycam*) pelos policiais responsáveis pela patrulha. O sistema público de videovigilância funciona ainda de maneira integrada a câmeras privadas, o que permite o compartilhamento e a centralização das informações pela polícia (NOTÍCIAS CARACOL, 2019).

Verifica-se, portanto, que na ausência de um marco normativo específico para uso de biometria nos sistemas de vigilância, o emprego dessas tecnologias - consideradas mais eficazes para prevenção e reação às práticas criminosas - ocorre na Colômbia, como em outros países da América Latina, por um regime de excepcionalidade e sem evidências adequadas de sua eficácia prática na diminuição da criminalidade (FUNDACIÓN KARISMA, 2018, p. 29-30).

2.5 Costa Rica

A incorporação de tecnologias de reconhecimento facial na Costa Rica, especialmente no âmbito dos sistemas de videovigilância em larga escala, é um fenômeno relativamente mais recente e incipiente, se comparado a outros países da América Latina. Villalobos Fonseca (2020, p. 89) explica, por exemplo, que as plataformas de informação da equipe da Força Pública não são totalmente integradas e automatizadas, mas que as melhorias na segurança pública são prioridades do mandato do atual presidente da Costa Rica, Carlos Alvarado Quesada. Em razão disso, inclusive, a negociação de um empréstimo para o país já estava em andamento junto ao Banco Interamericano de Desenvolvimento (BID) para arrecadar recursos e investir na modernização da força policial nacional (VILLALOBOS FONSECA, 2020, p. 93).

O Supremo Tribunal Eleitoral (TSE) da Costa Rica também anunciou a incorporação do reconhecimento facial como método de identificação associado às impressões digitais utilizadas há mais de duas décadas no país por meio Sistema de Verificação de Identidade (VID) (CORDERO, 2019). Um acordo foi firmado entre o Poder Executivo e o TSE para promover o desenvolvimento e utilização de tecnologias biométricas mais modernas, como um dos desdobramentos da Estratégia de Transformação Digital do Bicentenário para a Costa Rica[25], que busca incentivar a adoção e o desenvolvimento de novas tecnologias no país para melhoria da qualidade de vida (ÁVALOS, 2019).

[25] Disponível em: https://www.micit.go.cr/sites/default/files/estrategia-tdhcrb.pdf.

As principais demonstrações de esforços, ainda que tímidas, de incorporação de tecnologias de reconhecimento facial para atividades de segurança pública, no entanto, se dão em âmbito municipal. Um exemplo disso é o município costarriquenho de Naranjo, onde foi instalado, em 2019, um sistema de videovigilância com tecnologia de alta definição, reconhecimento facial, detecção de movimento e grande capacidade de armazenamento, incluindo 35 câmeras (EL PAÍS.CR, 2019).

Apesar de investidas tecnológicas mais intensas como essa terem ocorrido nos últimos dois anos, a Costa Rica possui histórico de mais de uma década acerca da utilização de sistemas de vigilância de espaços públicos, regulado pelo Ministério de Segurança Pública via Decreto 34104-G-MSP de 2007[26] e Decreto 35532-MSP de 2009[27]. Essas normas encontram-se, todavia, além de desatualizadas em relação às tecnologias de vigilância mais recentes, desconectadas com a legislação de proteção de dados pessoais costarriquenha, Lei nº 8968 de 2011[28] e o Regramento 37554-JP de 2012[29] (CHACÓN, 2019, p. 105).

Nesse cenário normativo, Chacón (2019, p. 173) explica que, apesar da competência para o manejo dos sistemas de vigilância ser do Ministério da Segurança, na realidade são os municípios que administram e operam esses sistemas a partir de uma interpretação extensiva das competências dos governos locais, desprovidos, portanto, de fundamentação legal própria. Segundo a autora, as especificações técnicas de informação aos cidadãos sobre o monitoramento dos espaços (artigo 7º do Decreto 34104-G-MSP) não são devidamente cumpridas. O município de San José, por exemplo, coloca uma pequena placa junto às câmeras indicando apenas ser propriedade do município (CHACÓN, 2019, p. 186-7).

Para além da excepcionalidade do tratamento de dados para segurança pública[30], Chacón (2019, p. 201) ressalta que muitos aspectos relacionados a esse tratamento não estão contemplados nos decretos, como a temporalidade, a participação da Agência de Proteção de Dados dos Habitantes (PRODHAB), a vigilância para fins particulares, entre outros. Sobre a Agência de Proteção, inclusive, vale destacar suas

[26] Reglamento Regulador de la Vigilancia de Calles, Avenidas, Carreteras y Caminos mediante Dispositivos Tecnológicos o Técnicos, disponível em: https://bit.ly/3fmb0DY.
[27] Reforma Reglamento Regulador de la Vigilancia de Calles, Avenidas, Carreteras y Caminos Mediante Dispositivos Tecnológicos o Técnicos, Decreto Ejecutivo N° 34104, disponível em: https://bit.ly/2SAQOUT.
[28] Ley de Protección de la Persona frente al tratamiento de sus datos personales, disponível em: https://bit.ly/3c37Kew.
[29] Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales, disponível em: https://bit.ly/3c2MghD.
[30] "De a acuerdo con el Decreto 34104-G-MSP y sus reformas, es posible utilizar las imágenes obtenidas por medio de los CCTV con fines de investigación o persecución policial, como medio de prueba para dilucidar los hechos o la identidad de los sospechosos, sin incurrir en una violación de los derechos civiles,, siempre y cuando la fuente de la prueba se haya obtenido lícitamente sin menoscabar los derechos fundamentales de las personas involucradas, buscando el límite entre el principio de la libertad probatoria y la búsqueda de la verdad material". (CHACÓN, 2019, p. 176).

competências limitadas sobre os projetos de vigilância na Costa Rica, posto que suas resoluções não são vinculantes (CHACÓN, 2019, p 175).

Salvo a possibilidade de regulamentação residual por decretos, verifica-se que as delimitações dos projetos de vigilância na Costa Rica deveriam ser regulados segundo o princípio da reserva legal, ou seja, mediante lei própria e não decreto, uma vez que esse tipo de política gera restrições de direitos fundamentais, como o direito à imagem e proteção de dados pessoais (CHACÓN, 2019, p. 201), mesmo que não incorpore tecnologias avançadas de reconhecimento facial, o que, como visto, já passou a ser uma realidade no país.

2.6 México

Botello (2016, p. 206-7), em pesquisa sobre a gestão de câmeras de vigilância no México, alertou para o problema da debilidade da regulação mexicana, como de outros países latino-americanos, em compreender o uso de sistemas de vigilância não só como um instrumento de garantia de segurança pública, mas também como um instrumento de valor político. Apesar da falha regulatória, o autor entende que há alguma preocupação em reconhecer a necessidade de cuidado quanto à vulnerabilidade de direitos sociais face ao emprego da tecnologia, cuja expansão também é, por outro lado, defendida.

Essa aparente contradição se reflete na legislação mexicana (de forma variada) em três dimensões principais: i) responsabilidade e decisão da aplicação da tecnologia; ii) gestão e uso das câmeras; e iii) manipulação das imagens. Essas preocupações, no entanto, se voltam para a proteção de dados e deixam de lado os processos de classificação e tipificação social que podem decorrer do uso da tecnologia (BOTELLO, 2016, p. 207).

Com relação à primeira esfera, enquanto em alguns municípios a legislação atribui o controle e a tomada de decisão sobre questões de videovigilância para segurança às comissões compostas por membros do poder público encarregados da segurança e também a grupos da sociedade civil[31], em outros locais a lei não atribui essa responsabilidade a um comitê, mas sim a autoridades específicas do Estado[32], como o prefeito da municipalidade onde os sistemas serão implementados (BOTELLO, 2016, p. 212).

No segundo âmbito de preocupação, as legislações de Durango, Colima e Aguascalientes, e os marcos regulatórios de Guadalajara[33] e de Sayula, reconhecem que o princípio da proporcionalidade deve ser observado na gestão e uso de câmeras de

[31] Ley de Videovigilancia del Estado de Aguascalientes (22/06/2009), Ley que Regula la Videovigilancia del Estado de Colima (22/08/2009), Ley que regula la bideovigilancia del estado de Durango (19/06/2009).
[32] Reglamento del Centro de Monitoreo, Videovigilancia, Biometria y Cabina del Municipio de Sayula, Jalisco (28/09/2012), Ley que Regula el uso de Tecnologia para la Seguridad Pública del Destrito Federal.
[33] Reglamento de Videovigilancia del Municipio de Guadalajara (10/06/2011).

videovigilância, estabelecendo que os critérios para utilização dos equipamentos devem considerar o perigo iminente. Assim, para que a vigilância ocorra, é necessário que ela proporcione de fato uma atmosfera segura e que intervenção na privacidade seja mínima (BOTELLO, 2016, p. 212). A lei do distrito federal, por outro lado, não obriga a observância dos princípios da proporcionalidade e intervenção mínima na instalação de sistemas de vigilância, e justifica a implementação dos sistemas de monitoramento somente com base em dados estatísticos sobre informações dos registros criminais[34], posicionamento totalmente contrário ao nível municipal, que privilegia uma gestão mais flexível (BOTELLO, 2016, p. 212-3).

Por fim, no que diz respeito à manipulação das imagens, Botello (2016, p. 214) destaca que as preocupações legislativas estão focadas em três pontos: o primeiro deles é a proteção da privacidade, o segundo é a fidelidade das imagens (e consequentemente, das informações que se extraem delas), e o terceiro é a destruição posterior dessa informação. Em alguns lugares, como da Cidade do México, essas preocupações são mais evidentes do que em outros: na cidade, um documento detalhado indica como as informações foram obtidas pelo Poder Público, quem teve acesso às imagens e com qual finalidade, sendo assegurado um compromisso de confidencialidade (BOTELLO, 2016. p. 214-5). O tempo de armazenamento, por sua vez, não é especificado na Lei do Distrito Federal, ao contrário de outras cidades, como Sayula, nas quais o armazenamento não pode ultrapassar 180 dias (BOTELLO, 2016, p. 208-11).

Fica claro, analisando as três esferas de preocupação, que os esforços além de insuficientes estão concentrados na questão da privacidade. Em âmbito nacional, a medida mais significativa é o Comunicado IFAI 065/13, elaborado pelo *Instituto Federal de Acceso a la Información y Protección de Datos* (IFAI, 2013), que determina que o aviso de que a área é sujeita às tecnologias de vigilância deve ser acompanhado pelo nome, razão social e domicílio do responsável pela operação e gestão das câmeras vigilância, além da finalidade da operação para que seja mais fácil identificar e denunciar eventuais violações à privacidade (BOTELLO, 2016, p. 225).

A insuficiência das medidas legais voltadas para normatização de políticas de vigilância agrava-se diante do emprego das tecnologias de reconhecimento facial[35] e o tratamento de dados biométricos, cuja previsão legal merece atenção. Na jurisdição mexicana, a proteção dos dados pessoais se consolida e delineia a partir de duas leis federais: a Lei Geral de Proteção de Dados Pessoais em Posse de Sujeitos Obrigados[36]

[34] Sobre o assunto, Isaac (2018) ressalta que deve-se levar em conta que os registros criminais também refletem o contexto cultural e político da localidade, já que a denúncia de crimes depende tanto da concentração da força policial, como do que a sociedade considera moralmente perigoso, suspeito e reprovável, exigindo medidas policiais.

[35] Segundo o autor Botello (2016, p. 202), em Tuxtla Gutiérrez há sistema de reconhecimento facial instalados em algumas das 230 câmeras de monitoramento do município do sudoeste do país.

[36] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017. Disponível em: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

(LGPDPPSO) e a Lei Federal de Proteção de Dados Pessoais em Posse de Particulares[37] (LFPDPPP). Considerando que ambas essas leis não explicam como se dá o tratamento dos dados biométricos, o *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales* (INAI) (2018) aborda o tema em um guia específico.

De acordo com o INAI (2018, p. 18-9), os dados biométricos são considerados dados pessoais quando identificam diretamente uma pessoa ou quando sua identificação for possível por meio da aplicação de tecnologias apropriadas. Isso porque, conforme dispõe a lei e esclarece o guia produzido pelo INAI (2018), um dado pode ser considerado dado pessoal se atender a dois critérios: se referir a uma pessoa física e identificar ou tornar identificável seu titular. Os dados sensíveis, por sua vez, seriam aqueles que expressam informações íntimas sobre o titular, cujo uso indevido ou ilegítimo possa servir como base discriminatória ou oferecer grave risco.

Desse modo, a caracterização do dado como dado pessoal e sensível no contexto mexicano será circunstancial. Ao coletar as imagens dos rostos das pessoas, processá-las em um banco de dados para cruzar informações e identificá-las, sistemas de reconhecimento facial presumem o uso de dados pessoais segundo o direito mexicano.

A questão que se coloca mais uma vez, entretanto, é que o arcabouço legislativo, especificamente quanto aos órgãos do poder público, e conforme a LGPDPPSO, excepciona e limita a aplicação das regras gerais de proteção dos dados pessoais para as atividades de coleta e processamento de dados por razões de segurança nacional. O consentimento, requisito importantíssimo no contexto do tratamento de dados pessoais, é totalmente dispensado nos casos em que uma transferência das informações entre órgãos ou instituições ocorre com fundamento na segurança (MÉXICO, 2017).

2.7 Nicarágua

Em 2012, a Assembleia Nacional da República da Nicarágua aprovou tanto a Lei nº 787[38], quanto o Decreto nº 36-2012[39] (NICARÁGUA, 2012a; 2012b), relativos à proteção de dados pessoais no país. Diferentemente da maioria das legislações sobre dados pessoais encontradas até então, a lei nicaraguense não dispõe expressamente sobre a inaplicabilidade de seu conteúdo à determinadas atividades ligadas, por exemplo, à segurança pública, serviços de inteligência ou coleta de dados para uso doméstico.

Pela leitura integral do texto da Lei nº 787, verifica-se a exceção relacionada à transferência dos dados e seu consentimento, dispensado em caso de coleta para fins de

[37] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010. Disponível em: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.
[38] Ley de Protección de Datos Personales (Ley nº 787), disponível em: https://bit.ly/2yrpbqv.
[39] Reglamento de la Ley nº 787 "Ley de Protección de Datos Personales" (Decreto nº 36-2012), disponível em: https://bit.ly/2KXgarJ.

saúde pública, interesse social, segurança nacional ou outra especificação prevista em lei (artigo 13), e à coleta e ao tratamento dos dados pessoais para fins de segurança e defesa nacional, investigação de delitos, por parte dos órgãos de inteligência da Polícia Nacional e do Exército (artigo 24).

Apesar de não existir, nessa lei, dispositivo que afasta totalmente sua aplicação nessas situações especiais, isso não significa que problemas em relação ao uso abusivo das informações pessoais por parte do poder público não sejam possíveis – sobretudo diante das exceções de necessidade de consentimento para transferência de dados mencionadas acima. Mas é preciso pontuar, de todo modo, que limites para esse tratamento que se aplicam invariavelmente às instituições públicas e privadas estão na própria lei, o que não ocorre em todos os lugares.

2.8 Panamá

No Panamá, os sistemas de videovigilância se difundiram pela capital e cidades, como Colón, onde foi inaugurado um centro de operações de segurança e emergências, financiado pelo governo da China. O centro possui 291 torres de videovigilância espalhadas em diversos pontos da cidade, postos de leitura de placas de veículos, reconhecimento facial, entre outras tecnologias à disposição (ZAMBRANO, 2019). A capital, Cidade do Panamá, conta com centros semelhantes e, no final de 2019, o Aeroporto Internacional de Tocumen, principal aeroporto do país e localizado estrategicamente na rota aérea entre as Américas, teve seu sistema de reconhecimento facial reforçado com mais 150 câmeras inteligentes (PANAMÁ AMÉRICA, 2019).

A lei panamenha sobre proteção de dados pessoais, Lei nº 81/19[40], foi sancionada em março de 2019, mas somente entrará em vigor em 2021 (artigo 47). Entretanto, seguindo a tendência observada em outros países da América Latina, o tratamento dos dados por autoridades para fins de prevenção, investigação, identificação ou julgamento de infrações ou execução de sanções penais, não se submete ao regime desta nova lei (artigo 3, Lei nº 81/19).

A situação do Panamá é complexa quando se trata do tema de vigilância, pois o país já passou por um caso grave no governo do ex-presidente Ricardo Martinelli (2009-2014), quando o mesmo contratou ilegalmente as empresas M.L.M. Protection Ltd. e NSO Group para adquirir tecnologias para interceptar comunicações por cerca de por 13,5 milhões de dólares. O Supremo Tribunal de Justiça do Panamá acusou o ex-presidente de usar fundos públicos para espionar ilegalmente mais de 150 oponentes políticos (PEÑA, 2018).

2.9 Peru

[40] Ley nº 81 de 26 de marzo de 2019, sobre Protección de Datos Personales, disponível em: https://bit.ly/2zcbNGK.

No Peru, a verificação biométrica começou a ser usada há pouco mais de 20 anos. Em 2013, o AFIS (Sistema de Identificação Automática de Impressões Digitais), que é o sistema utilizado pelo Registro Nacional de Identificação e Estado Civil (RENIEC), foi atualizado para coletar as impressões digitais (representadas por dez dígitos) das duas mãos e as características faciais dos cidadãos peruanos. Embora as atualizações dos procedimentos busquem reduzir fraudes e aumentar a segurança, isso é feito sem nenhuma transparência. Não se sabe quem gerencia o banco de dados, como funciona na prática o registro biométrico ou quem são as partes envolvidas nesse processo (ADC, 2017, p. 19-20).

Ao final de 2019, a implementação de sistemas de reconhecimento facial iniciou em pelo menos três distritos da capital peruana: Miraflores, San Martin de Porres e La Victoria. Cada um dos distritos teve um processo de implementação distinto. Em La Victoria, por exemplo, o projeto foi realizado em mais de uma etapa, tendo começado pelo empório comercial de Gamarra e contou com a inauguração de um centro de monitoramento e controle local. Em Miraflores, o plano piloto foi construído com o apoio da Polícia Nacional do Peru, que também acompanha diretamente a instalação das câmaras em San Martin de Porres. Neste último distrito, inclusive, informações sobre antecedentes criminais são fornecidas pela embaixada da Venezuela (ARROYO, 2019).

A Lei nº 29733 de 2011[41], regulamentada pelo Decreto Supremo N° 003-2013-JUS[42], trata da proteção de dados pessoais no território peruano, estabelecendo regras e requisitos mínimos para que esses dados possam ser coletados, processados, armazenados ou transferidos. Essa lei considera expressamente os dados biométricos como sendo de natureza sensível, quando identificam seu titular (artigo 2.5), e estabelece, entre outros princípios, o consentimento como necessário para o tratamento dos dados pessoais dos indivíduos peruanos (artigo 5). Também dispõe que quaisquer limitações ao exercício do direito fundamental à proteção dos dados pessoais deverão ser estabelecidas em lei e bem fundamentadas no respeito a outros direitos fundamentais ou bens protegidos pela Constituição (artigo 13.2).

A norma não se aplica, entretanto, aos dados que têm como destino a composição dos bancos de dados da administração pública para o estrito cumprimento de suas competências legais, para defesa nacional e segurança pública, além do desenvolvimento de atividades em matéria penal, como investigação e repressão de crimes (artigo 3). Desse modo, a captura e processamento de imagens por sistemas de videovigilância com reconhecimento facial para investigar ou reprimir a criminalidade, ainda que possa ser considerada como forma de tratamento de dados pessoais, tanto pela Lei nº 29733 (Artigo 2.17 da Lei nº 29733 de 2011) (PERU, 2011) quanto pela Diretiva de Tratamento de Dados Pessoais por Sistemas de Videovigilância

[41]Ley nº 29733, Ley de Protección de Datos Personales, disponível em: https://bit.ly/3dpThcL.
[42]Decreto Supremo nº 003-2013-JUS (Reglamento de la Ley Nº 29733), disponível em: https://bit.ly/2WdWhDx.

(Directiva n° 01-2020-JUS/DGTAIPD)[43] (Ponto 5.24) (PERU, 2020), estaria dispensada do cumprimento dos princípios e deveres essenciais à proteção da privacidade e dos dados pessoais no país.

Conforme ressalta Chávez (2019, p. 145), observa-se que as situações que envolvem a proteção da vida e da integridade, a tutela da propriedade privada ou a garantia da segurança pública, inspiram a legalidade e a constitucionalidade da videovigilância. Segundo o autor, as primeiras normas que autorizaram essa prática em âmbito nacional - a Lei de Apoio a Segurança Cidadã com Câmeras de Videovigilância Públicas e Privadas (Lei 30120 de 2013) e o Decreto Legislativo nº 1218 de 2015 - basearam-se numa mesma conjuntura ainda vigente no país: a prevenção, a investigação e o combate ao crime (CHÁVEZ, 2019, p. 151).

Constata-se, assim, diante da ausência de subsunção às exigências comuns de proteção de dados pessoais e da excepcionalidade prevista nas leis e na diretiva de videovigilância, que a prática de monitoramento em larga escala por câmeras, sobretudo com sistema de reconhecimento facial (o que sequer é citado nas normas encontradas), não encontra limites na legislação peruana quando são contrapostos valores como proteção à segurança e incolumidade pública, de um lado, e privacidade, proteção de dados e liberdades civis, de outro.

2.10 República Dominicana

As diretrizes constantes na norma de proteção de dados pessoais da República Dominicana, Lei nº 172-13[44] de 2013, como acontece nos demais países vistos até então, também não se aplicam aos organismos de investigação e inteligência, Forças Armadas, órgãos de segurança e polícia, encarregados de prevenção e punição de delitos, conforme dispõe o artigo 4º, ponto 2 e o artigo 40 da Lei nº 172-13. (REPÚBLICA DOMINICANA, 2013b). Essa norma, segundo Peláez (2020) destaca, é muito focada no tratamento de dados pessoais realizado por órgãos do setor de crédito.

Em novembro de 2019, uma declaração do senador estadunidense Marco Rubio, afirmando que as câmeras com sistema de reconhecimento facial doadas pelo governo da China e espalhadas pela República Dominicana, inclusive nos aeroportos[45], fazem parte do plano de vigilância em massa chinês[46], levou o Sistema Nacional de Atenção a Emergências e Segurança 9-1-1 a emitir um comunicado sobre o assunto.

[43]Directiva n° 01-2020-JUS/DGTAIPD, Tratamiento de Datos Personales mediante Sistemas de Videovigilância. Disponível em: https://bit.ly/2zm4w7e. Foi aprovada pela Resolución Directoral N° 02-2020-JUS/DGTAIPD, disponível em: https://bit.ly/2YPJZTz.

[44] Ley Orgánica sobre Protección de Datos de Carácter Personal, disponível em: https://indotel.gob.do/media/6200/ley_172_13.pdf.

[45] Mais informações em: https://bit.ly/2YBhCYV.

[46] Sobre as declarações do senador e os desdobramentos, ver: https://bit.ly/2YAevjU; https://bit.ly/3dkWrym; https://bit.ly/3c7ZJoF.

O órgão, que concentra a responsabilidade para gerenciar todas as emergências de segurança do território nacional, assumiu que as câmeras citadas fazem parte do sistema de segurança do país que "tem melhorado a segurança das cidades desde sua implementação em 2014"[47].

Apesar de os responsáveis pela gestão do Sistema 9-1-1 advogarem pela transparência das ações realizadas para garantir a segurança da população por meio dos sistemas automatizados de vigilância em todo o país, com o avanço da tecnologia e a incorporação de novos métodos de monitoramento, é preciso que as informações fornecidas à população sejam mais claras e as normas sejam atualizadas. Como ressaltado no início e ao longo do trabalho, a utilização de sistemas de reconhecimento facial impõe uma restrição aos direitos fundamentais dos cidadãos e, por isso, sua adoção deve estar acompanhada de parâmetros legais muito bem definidos.

Com relação à videovigilância dos espaços pelo poder público, a Lei nº 102-13[48], também de 2013, é que dispõe sobre o tema, atribuindo ao Ministério Público a competência para supervisionar a instalação das câmeras, a coleta e o tratamento das imagens e sons (artigo 2º). A lei coloca expressamente a necessidade de se observar o princípio da proporcionalidade, em sua dupla perspectiva, para a utilização das câmeras. Em um primeiro aspecto, de idoneidade, as câmeras de segurança só podem ser utilizadas quando essa medida for adequada, em uma situação concreta, para manutenção da segurança dos cidadãos. Por outro lado, em uma perspectiva de mínima intervenção, é preciso ponderar em cada caso a finalidade e o nível de afetação que o emprego das câmeras gera face aos direitos à honra, à própria imagem e à intimidade (artigo 8º) (REPÚBLICA DOMINICANA, 2013a).

2.11 Uruguai

A modernização do sistema de videovigilância em Montevidéu, capital do Uruguai, começou em 2012, no bairro Ciudad Vieja, e faz parte da estratégia de segurança avançada do Ministério do Interior do país para redução do índice de criminalidade. (URUGUAY PRESIDENCIA, 2017). Em julho de 2014, o Ministério chegou a divulgar uma avaliação parcial positiva sobre os impactos da medida na queda das ocorrências delituosas (URUGUAY, 2014). A instalação de mais de 6.500 câmeras no território uruguaio, via convênio firmado com a empresa Sonda Uruguay S.A., é resultado da expansão do programa. Um centro de monitoramento funciona em Montevidéu para controlar as câmeras que contam com software para identificação de placas de carros e padrões comportamentais, como excesso de velocidade e deslocamento de pessoas (URUGUAY PRESIDENCIA, 2017). O Uruguai recebeu ainda uma doação de

[47] Trecho original: "#Importante Las cámaras de seguridad a las que hace referencia el senador @Marcorubio forman parte de nuestro sistema de atención a emergencias, las cuales han mejorado la seguridad de nuestras ciudades desde su implementación en 2014, gracias a la colaboración de varios socios." Publicado na página oficial do Sistema 9-1-1 do Twitter em 14 nov. 2019. Disponível em: https://bit.ly/3c7ZJoF.

[48] Disponível em: http://www.poderjudicial.gob.do/documentos/pdf/leyes/LEY_102_13.pdf.

1.000 câmeras do governo da China, algumas instaladas inclusive na fronteira com o Brasil (URUGUAY PRESIDENCIA, 2017; MONTEVIDEO PORTAL, 2018).

Os sistemas de reconhecimento biométrico facial têm sido utilizados com maior frequência em estádios de futebol (CDTLatam, 2017), para controle laboral com base na Lei de Segurança Privada, Lei nº 19.721 de 2019[49] e no controle migratório e de passageiros nos aeroportos. No final de 2018, inclusive, o Aeroporto Internacional de Carrasco foi o primeiro da América Latina a incorporar o controle total do fluxo de passageiros, desde a migração até a entrada na aeronave, por meio de tecnologia biométrica facial (URUGUAY, 2018a).

Em 2019, o Ministério do Interior uruguaio lançou uma chamada pública para aquisição de sistema de reconhecimento facial capaz de identificar o nome e o documento das pessoas com imagens registradas em vídeo. Diferentemente dos outros exemplos analisados até então, o governo uruguaio determinou que o sistema não poderia ter uma taxa de erro inferior a 95%, e que a taxa de falsos positivos deveria ser inferior a 0,1%, em ambientes controlados (LOSA, 2019). Mesmo sem determinar o que seriam "ambientes controlados", o governo claramente optou pela menor quantidade de falsos positivos, ainda que isso implicasse em aumento dos falsos negativos. Essa decisão de cunho político é deixada, via de regra, para as empresas, sem determinação de quaisquer parâmetros de segurança e proteção de direitos fundamentais por parte dos contratantes, ainda que agentes públicos.

No Uruguai, seguindo os ditames da Lei nº 18.331[50] de 2008, os dados biométricos também são dados pessoais sensíveis porque correspondem às representações faciais que identificam uma pessoa. Do mesmo modo, a norma excepciona a necessidade de consentimento para coleta dos dados que seja realizada para fins de segurança pública, defesa nacional e atividades estatais de matéria penal, notadamente investigação e repressão de delito (artigo 3). Essa exceção cabe para os dados que forem essencialmente necessários para o cumprimento estrito das finalidades previstas por lei (artigo 25).

O *Dictamen* 10/010[51], de 16 de abril de 2010, orienta a forma pela qual deveriam ser regulados sistemas de vigilância no país. Além de reconhecer a exceção para fins de segurança pública, o documento determina que o uso de sistemas vigilância deverá ser regido pela Lei 18.331/2008 e suas normas complementares, reconhecendo que as finalidades devem ser "a proteção das pessoas físicas, o direito à propriedade, a ordem pública, a detecção ou prevenção de delitos e outros interesses legítimos"[52]. Com base no *Dictamen* nº 10/010, o governo uruguaio disponibilizou

[49] Ley 19.721/2019, disponível em: https://bit.ly/3hpLlu6.
[50] Ley nº 18.331, disponível em: https://www.impo.com.uy/bases/leyes/18331-2008.
[51] Dictamen 10/010, disponível em: https://bit.ly/3dUYGJu.
[52] Trecho original: "Que la videovigilancia tiene como principales finalidades la protección de las personas físicas, del derecho de propiedad, la tutela del orden público, la detección y prevención de delitos, así como otros intereses legítimos".

outros documentos para orientar, por exemplo, a instalação de sistemas de videovigilância em edifícios privados, conjuntos habitacionais e cooperativas, entidades públicas ou para fins de controle laboral (URUGUAY, 2018b; 2018c). Além de limitarem o emprego de tais sistemas, impedindo a instalação em locais públicos, preveem a necessidade de sua inscrição no registro de bases de dados pessoais.

Da mesma forma que podemos extrair diversas orientações do *Dictamen* 10/010, o mesmo poderá ser o caso do *Dictamen* 05/019[53]. No documento, o *Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales* dispõe que não existe vulneração da proteção de dados se as câmeras não permitem a identificação dos sujeitos com a filmagem, quando são colocadas em lugares em que a captação será feita de uma forma mais geral, quando há a aplicação de filtros de privacidade ou ainda caso as imagens coletadas sejam de baixa qualidade. Caso contrário, o consentimento individual prévio e expresso deverá ser obtido por parte do responsável pelo sistema de vigilância. Não há esclarecimentos, entretanto, se os avisos de vigilância posicionados de forma visível ao público, cujos modelos são disponibilizados pelo próprio governo uruguaio, são suficientes para configurar o consentimento expresso do indivíduo ou não.

Sobre essa exigência de consentimento expresso, questiona-se ainda a extensão da determinação aos agentes públicos no exercício de suas funções de garantia da segurança pública. O *Dictamen* 15/018[54], voltado para uso de vigilância para controle de trânsito, em resposta à solicitação feita pelo município de Florida, apesar de prever que o consentimento dos titulares não é necessário para os fins de segurança pública, não fez referência ao emprego de processamento de dados biométricos pelo software de reconhecimento facial que se pretendia implementar nas próprias câmeras de vigilância do local para monitoramento em tempo real ou não.

O risco da ausência de uma norma clara, todavia, se demonstra no país pela observação do caso em que uma companhia responsável por introduzir sistemas de reconhecimento facial em shoppings e cassinos levantou a hipótese de uso da referida tecnologia para identificar e impedir o ingresso de pessoas com ludopatia em tais locais (LOSA, 2019). A tecnologia, que não foi usada somente por insatisfações com a precisão técnica, poderá ser desenvolvida para fins de identificação (e posterior limitação de ingresso) de outras enfermidades, promovendo um uso discriminatório.

3. Considerações finais

A ausência de um marco legal específico para o uso de sistemas de reconhecimento facial é um problema verificável em diversos países da América Latina. Grande parte dos países acabam apoiando a base legal do seu uso em legislações de proteção de

[53] Dictamen 05/019, disponível em: https://bit.ly/2ORm7s8.
[54] Dictamen 15/018, disponível em: https://bit.ly/2WNHU8H.

dados que são, por sua vez, textos gerais - que excepcionam, muitas vezes, os limites da coleta de dados pessoais para fins de segurança pública -, ou por meio de outros documentos não vinculantes, que tentam (de forma incipiente) suprir as falhas da negligência dos reguladores. Esse cenário, conforme verificado ao longo do texto, coloca os direitos fundamentais em risco e produz impactos perversos que deveriam levar os países a questionar a própria possibilidade do uso da tecnologia[55].

A regulação de sistemas de reconhecimento facial única e exclusivamente com base em previsão normativa sobre proteção de dados, da forma como ocorre nos países analisados, é problemática principalmente por duas razões. Primeira, porque essas normas apenas autorizam o uso dessa tecnologia para segurança pública a título de exceção geral. Ou seja, não há expressa decisão do Legislativo de permitir o uso especificamente do reconhecimento facial em larga escala e nos mais diversos ambientes. Segunda, e talvez mais importante, porque para além da mera permissão de adoção da tecnologia, essa base normativa não oferece absolutamente nenhuma baliza ou diretriz sobre como tais sistemas deveriam operar, quais níveis de transparência e *accountability* eles deveriam respeitar, quais taxas de falsos positivos e falsos negativos são toleráveis em quais situações, qual o procedimento para auditoria independente periódica dessas taxas e assim por diante. Mera permissão por via de exceção generalizada está muito aquém de regulação responsiva e criteriosa. O avanço do reconhecimento facial nesses países é evidente e já ocorre há alguns anos, exigindo já uma resposta dos órgãos de controle e, principalmente, do Legislador, considerando o grau de novidade e complexidade dessa aplicação da inteligência artificial.

O fornecimento de segurança como um serviço, conforme defende a autora Silvana Pereyra (2018, p. 252), levou à normalização do uso e compartilhamento de dados para os fins de vigilância. No entanto, o desenvolvimento dessa tecnologia por atores privados, sem quaisquer parâmetros regulatórios, tem levado à negligência dos efeitos de um falso positivo em caso de uso de reconhecimento facial, por exemplo, para persecução penal. Petrescu (2019, p. 237-8; 243) reforça a importância de medidas de qualidade de fatores como iluminação, expressão, imagem e ruído em sistemas de reconhecimento facial, já que, assim como a qualidade das próprias imagens fornecidas como referência (GARVIE, 2019) podem reforçar falsos positivos.

Além disso, o uso de reconhecimento facial em espaços públicos, ao alterar a percepção sobre o espaço, redefine sua utilização, já que as pessoas modificam seus comportamentos quando sabem ou suspeitam que estão sendo observadas ou vigiadas. Portanto, o debate que antes poderia estar centralizado somente nas preocupações acerca da eficiência da instalação de câmeras de vigilância e dos respectivos custos de manutenção e implementação diante de uma eventual obrigatoriedade de

[55] Um marco regulatório pode ser relevante até mesmo para proibir determinados usos da tecnologia de reconhecimento facial, em que se verifica que os benefícios de eficiência na segurança pública não se mostram suficientes para permitir seu uso, diante dos outros prejuízos identificados.

seu uso, passa a ser também um debate de controle social, já que o intenso fluxo de informações pessoais produzidas por câmeras instaladas em ambientes públicos torna-se operacionalizável diante do emprego de sistemas de reconhecimento facial e a coleta de dados sensíveis (CARDOSO, 2013, p. 57-8).

A regulação nos países latino-americanos analisados não dá devida atenção aos prejuízos à liberdade de expressão e associação e parece estar centrada nas garantias de proteção de dados - mesmo assim, de forma tímida. A *Asociación por los Derechos Civiles* recomenda estudos para certificar que essa é a melhor medida para lidar com os problemas de segurança, que o debate legislativo conte com ampla participação social e que a legislação tenha previsões expressas sobre a transparência, supervisão e controle do funcionamento das ferramentas de reconhecimento facial para evitar abusos (ADC, 2019a, p. 4-5).

E é preciso que esse debate seja contextualizado, para que indivíduos dos grupos mais vulneráveis ao controle social estejam sendo adequadamente protegidos pela regulação. Conforme ressalta Botello (2016, p. 219), a escolha dos locais de instalação das câmeras com reconhecimento facial e outros sistemas de vigilância é realizada na maior parte das vezes por grupos de poder já centralizados, que classificam e tipificam grupos sociais como perigosos e suspeitos com base em crenças muitas vezes discriminatórias já fortemente imbricadas na sociedade, estabelecendo limitações severas na possibilidade de autodeterminação de grupos historicamente marginalizados. Ao optar por incluir tais recursos tecnológicos somente em localidades onde há incidência de contravenções associadas a determinados grupos, como focos de prostituição, de venda de produtos por ambulantes ou de consumo de drogas, as autoridades responsáveis pela gestão das câmeras realizam uma escolha acerca de quais grupos exigem maior monitoramento social. A limitação da autonomia e do controle sobre a própria vida não alcança, por exemplo, os locais onde crimes de colarinho branco são praticados, reforçando representações estereotipadas que consideram apenas grupos alvos de preconceitos históricos como desviantes do padrão de normalidade (BOTELLO, 2016, p. 221).

Ao refletir sobre possibilidades regulatórias em âmbito nacional, vale destacar algumas sugestões de Botello (2016), as quais podem ser aprimoradas e aplicadas para além do contexto mexicano, especificamente estudado pelo autor. Segundo Botello (2016, p. 226-7), é importante que exista um texto legal de aplicação obrigatória e imediata a qualquer autoridade, que estabeleça os critérios para instalar, administrar e gerir a operação de sistemas de videovigilância, incorporando o princípio da proporcionalidade e preceitos que limitem processos discriminatórios pelo emprego da tecnologia. Para que o princípio da proporcionalidade seja contemplado, o autor sugere ainda que sejam realizados estudos prévios sobre os impactos da implantação de sistemas de videovigilância na configuração do espaço urbano. Além disso, o autor também sugere a criação de comissões estaduais e municipais, com vistas a reduzir a já mencionada opacidade dessa aplicação de inteligência artificial,

as quais deverão contar com a presença tanto de instituições governamentais quanto de grupos da sociedade civil - especialmente aqueles que historicamente são alvos de discriminação e que podem ser mais afetados pelas alterações das dinâmicas sócio-espaciais provocadas pela tecnologia (BOTELLO, 2016, p. 227-8).

Fussey e Murray (2019), por sua vez, sugerem que todas as hipóteses de treinamento dos algoritmos de reconhecimento facial em ambientes simulados sejam esgotadas antes de implementá-los nos espaços para o grande público. Quando o teste é concomitante à implementação em larga escala inexiste a figura do consentimento para participação, o que abre margem para confusões em relação à natureza da aplicação do sistema, ou seja, se de fato são testes das tecnologias ou se são operações policiais oficiais com o intuito de identificar potenciais suspeitos. Para os autores, é necessário que o poder público institucionalize uma metodologia clara acerca das técnicas que devem ser empregadas nos sistemas de reconhecimento facial (FUSSEY; MURRAY, 2019, p. 28). Esse é outro elemento importante sem o qual uma política regulatória para o reconhecimento facial não está completa.

Lynch (2020, p. 26-8) destaca medidas essenciais para lidar com alguns dos problemas de precisão típicos dessa tecnologia, como a limitação da coleta de dados até o mínimo necessário para atingir os objetivos do governo, a definição de quando e como o reconhecimento facial pode ser utilizado na ausência de proibição total desse sistema, a limitação da quantidade e do tipo de dado armazenado, a restrição à combinação de vários dados biométricos em um único banco de dados e a adoção de procedimentos técnicos de segurança específicos para essas aplicações biométricas, entre outras.

Conforme abordado ao longo do texto, a utilização das tecnologias de reconhecimento facial para fins de proteção à segurança pública apoia-se na verdade em um regime de excepcionalidade, presente nas leis de dados pessoais, leis de videovigilância desatualizadas ou outros instrumentos normativos. Verifica-se, portanto, uma incorporação desses sistemas às tradicionais estruturas de vigilância em âmbito penal principalmente, que são tradicionalmente discriminatórias, sem qualquer debate, estudo prévio ou legislação apropriada.

Em um contexto de elevada insegurança social, no qual o apelo pela implementação de sistemas de vigilância por parte do Poder Público se torna mais cabível, motivada para fins de redução de danos, é essencial que a discussão da aplicação dessa tecnologia seja acompanhada de preocupações éticas relacionadas aos possíveis processos discriminatórios e de estratificação do espaço urbano que podem surgir a partir da sua instalação. O debate deve abranger também as discussões sobre a proteção da privacidade e dos dados pessoais dos indivíduos submetidos a essa forma de controle, mas é imprescindível entender que um sistema de reconhecimento facial em pleno e rigoroso respeito a todo um arcabouço regulatório sobre proteção de dados

pessoais pode ainda ser problemático por diversas outras razões ligadas à proibição de discriminação, direito de locomoção e liberdade de expressão.

4. Referências bibliográficas

ADC. **Cuantificando identidades em América Latina**. Asociación por los Derechos Civiles (ADC), maio 2017. Disponível em: https://bit.ly/2W6qXoW. Acesso em: 20 abr. 2020.

ADC (2019a). **Briefing sobre biometría para periodistas**. Asociación por los Derechos Civiles (ADC), abril 2019. Disponível em: https://bit.ly/36dyKGd. Acesso em: 20 abr. 2020.

ADC (2019b). **El reconocimiento facial para vigilancia no pertenece a nuestro espacio público**. Asociación por los Derechos Civiles (ADC), 06 nov. 2019. Disponível em: https://bit.ly/38d7Eir. Acesso em: 08 fev. 2020.

ALBERS, Marion. A complexidade da proteção de dados. **Revista Brasileira De Direitos Fundamentais & Justiça**, 10(35), 2016, p. 19-45. Disponível em: https://bit.ly/2Q7N6QX

ALMEIDA, Emily. Homem é preso por engano em Copacabana. **Band News FM Rio**, 24 jul. 2019. Disponível em: https://bit.ly/3dEUflp.

ARROYO, Verónica. Cámaras con reconocimiento facial en Lima. **Access Now**, 14 nov. 2019. Disponível em: https://bit.ly/2KMn5Ef.

ÁVALOS, Ángela. Huella dactilar y rostro serán los nuevos 'documentos' de identidad de losticos. **La Nación**, 17 fev. 2019. Disponível em: https://bit.ly/2W0vudA. Acesso em: 30 abr. 2020.

BECKER, Sebastián; LARA, J. Carlos; CANALES, María Paz. Parte I: Algunos ejemplos de regulación actual en América Latina. *In*: DERECHOS DIGITALES. **La construcción de estándares legales para la vigilancia en América Latina**. Set. 2018.

BLACK, Julia; MURRAY, Andrew. Regulating AI and Machine Learning: Setting the Regulatory Agenda. European Journal of Law and Technology, v. 1, i. 3, 2019,

BOTELLO, Nelson Arteaga. Regulación de la videovigilancia en Mexico. Gestión de la ciudadanía y acceso a la ciudad. **Espiral**, Guadalajara, vol. 23, nº 66, ago. 2016. Disponível em: https://bit.ly/2SxQBkJ.

BRASIL. Tribunal de Justiça do Estado de São Paulo - 37ª Vara Cível. **Ação Civil Pública - Transporte Ferroviário nº 1090663-42.2018.8.26.0100**. Requerente: IDEC - Instituto Brasileiro de Defesa do Consumidor. Requerido: Concessionária da Linha 4 do Metrô de São Paulo S.A (ViaQuatro). Juíza Adriana Cardoso dos Reis. São Paulo, 14 set. 2018. Disponível em: https://bit.ly/39uRFg7. Acesso em: 07 fev. 2020.

BRASIL. Ministério da Justiça e Segurança Pública. Gabinete do Ministro. Portaria nº 793, de 24 de outubro de 2019. **Diário Oficial da União**, Brasília, DF, 25 out. 2019. p. 55. Disponível em: https://bit.ly/3fQqfVK.

CANALES, María Paz; LARA, Juan Carlos. Parte III: Propuesta de Estándares legales para la vigilancia en Chile. *In*: DERECHOS DIGITALES. **La construcción de estándares legales para la vigilancia en América Latina**. Set. 2018. Disponível em: https://bit.ly/2WwVSfn.

CARDOSO, Bruno. Câmeras legislativas: videovigilância e leis no Rio de Janeiro. **Revista Brasileira de Ciências Sociais**, São Paulo, vol. 28, n. 81, p. 50-61, 2013. Disponível em: https://bit.ly/3fob8Tn.

CARVALHO, Lucas. Metrô de São Paulo vai usar reconhecimento facial em anúncios. **Olhar Digital**, 13 abr. 2018. Disponível em: https://bit.ly/2tM3Cic. Acesso em: 08 fev. 2020.

CDTLatam. **Sistema de Reconocimiento Facial - Uruguay - CDTLatam**. CDTLatam Reconocimiento Facial (canal no YouTube), vídeo postado em 15 set. 2017. Disponível em: https://www.youtube.com/watch?v=wEio9EXOz4k&t=158s.

CHÁVEZ, Javier A. M. «Brace yourselves! La Videovigilancia ya viene»: situación de la videovigilancia en el ordenamiento jurídico peruano. Derecho PUCP, n. 83, 2019, p. 133-178. Disponível em: https://bit.ly/2D1Lc1e. Acesso em: 22 jul. 2020.

CHACÓN, Ivannia Madrigal. **El uso de los sistemas de videovigilancia como medida de seguridad y su incidencia en los derechos de vida privada, propia imagen y la protección de datos personales**. 2019. 253 f. Tesis para optar por el grado de Licenciatura en Derecho (Facultad de Derecho), Universidad de Costa Rica. Disponível em: http://repositorio.sibdi.ucr.ac.cr:8080/jspui/bitstream/123456789/9099/1/44119.pdf. Acesso em: 01 maio 2020.

CONSEJO PARA LA TRANSPARENCIA (CPLT) (2017a). **Ofício Nº 2309**. Raúl Ferrada Carrasco (diretor geral do Conselho). Santiago, 06 mar. 2017. Disponível em: https://bit.ly/2WGeXdQ.

CORDERO, Carlos. Servicio de reconocimiento facial del TSE estaría en septiembre del 2020. **DPL News**, 15 maio 2019. Disponível em: https://bit.ly/35pY3nZ. Acesso em: 30 abr. 2020.

COUTINHO FILHO, Augusto. Regulação 'Sandbox'como instrumento regulatório no mercado de capitais: principais característicase prática internacional. Revista Digital de Direito Administrativo. V. 5, n. 2, 2018.

DAUGHERTY, Moriah *et al.* The Perpetual Line-Up: Unregulated Police Face Recognition in America. **Georgetown Law Center on Privacy & Technology**,

out. 2016. Disponível em: https://www.perpetuallineup.org/. Acesso em: 23 abr. 2020.

DEFENSORIA PÚBLICA DO RIO DE JANEIRO. Perfil dos entrevistados pela Defensoria Pública do Rio de Janeiro nas audiências de custódia entre setembro de 2017 e setembro de 2019. **Diretoria de Estudos e Pesquisas de Acesso à Justiça.** Disponível em: https://bit.ly/2Q8AoBK. Acesso em: 19 de ago. 2020

DESLAURIERS, Jean-Pierre; KÉRISIT, Michèle. O delineamento de pesquisa qualitativa. *In*: POUPART, Jean *et al.* (Org.). **A pesquisa qualitativa**: enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2008. p. 127-153.

DESAI, Deven. KROLL, Joshua. *Trust but verify: a guide to algorithms and the law.* In. **Harvard Journal of Law and Technology**. Vol, 31, n 1., 2017, p. 1-64. Disponível em: https://bit.ly/2EdHTV7

EL PAÍS.CR. Naranjo refuerza seguridad con sistema de videovigilancia de RACSA. **El País.cr**, 04 maio 2019. Disponível em: https://bit.ly/3d9xKVJ. Acesso em: 30 abr. 2020.

FERREIRA, Lucia Maria Teixeira. **Parecer sobre a legalidade dos Decretos nº 10.046/2019 e 10.047/2019 (...)**. Disponível em: https://bit.ly/3fNDiH7.

FOLHA DE SÃO PAULO. Nordeste vira palco de guerra fria tecnológica entre EUA e China. **Folha de São Paulo**, 30 ago. 2020. Disponível em: https://bit.ly/2WTsuig. Acesso em: 21 fev. 2020

FUNDACIÓN KARISMA. **Cámaras inDiscretas - FAQ**. Bogotá, 2018. Disponível em: https://bit.ly/35RLaTR. Acesso em: 20 abr. 2020.

FUNDACIÓN KARISMA. **Biometría en el Estado colombiano** ¿Cuándo y cómo se ha justificado su uso? Bogotá, 2019. Disponível em: https://url.gratis/vnXRe.

FUSSEY, Pete; MURRAY, Daragh. **Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology**. The Human Rights, Big Data and Technology Project - Human Rights Center, University of Essex, 2019. Disponível em: https://bit.ly/36vQ3AP.

G1 BAHIA. Procurado por roubo é preso por reconhecimento facial em Salvador. **G1 Bahia**, 06 fev. 2020. Disponível em: https://glo.bo/39gYXnp.

G1 RIO. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **G1 Rio de Janeiro**, 11 jul. 2019. Disponível em: https://glo.bo/2SLinec.

GARAY, Vladimir. Mal de Ojo: Reconocimiento Facial em América Latina. *In*: DERECHOS DIGITALES. **Latin America in a Glimpse**. Nov. 2019. Disponível em: https://bit.ly/2H2baQA. Acesso em: 04 fev. 2020.

GARVIE, Clare. Garbage In, Garbage out: Face Recognition on flawed data. Georgetown Law Center on Privacy & Technology. Maio, 2019. Disponível

em: https://www.flawedfacedata.com/#footnote6_c28hfft. Acesso em: 06 mar. 2020.

IGLESIAS, Romina Garrido; CASTELLARO, Sebastián Becker. La biometría en Chile y sus riesgos. **Revista Chilena de Derecho y Tecnología**, [s.l.], vol. 6, n. 1, 2017, p. 67-91. Disponível em: https://rchdt.uchile.cl/index.php/RCHDT/article/view/45825/48403.

IFAI. **Comunicado IFAI 065/13**. Personas físicas y morales que video vigilen deben contar con aviso de privacidad. México, jul. 2013. Disponível em: https://bit.ly/2UDLMsr.

INAI. Guía para el Tratamiento de Datos Biométricos. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. 2018. Disponível em http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf.

INFOBAE. En menos de tres meses, se logró detener a 174 prófugos gracias al sistema de reconocimiento facial. **Infobae**, Buenos Aires, 2019. Disponível em: https://bit.ly/2Wl4wgQ. Acesso em: 15 abr. 2020.

INSTITUTO IGARAPÉ. **Desde 2011 vem sendo utilizado o reconhecimento facial no Brasil**. 2019 [data estimada pela redação]. Disponível em: https://bit.ly/2L89rvh.

ISAAC, William S. Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice. **Ohio State Journal of Criminal Law**, vol. 15, n. 2, 2018, p. 543-558. Disponível em: https://kb.osu.edu/handle/1811/85814.

KAPLAN, Andreas; HAENLEIN, Michael. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. **Business Horizons**, [s.l.], v. 62, n. 1, p. 15-25, jan. 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S0007681318301393.

KLARE, Brenda F. *et al*. Face recognition performance: role of demographic information. **IEEE Transactions on Information Forensics and security.** vol 7:6, 2012, p. 1789-1801. Disponível em: https://ieeexplore.ieee.org/document/6327355.

LEGALE, Siddharta; VAL, Manuel Eduardo. A dignidade da pessoa humana e a jurisprudência da Corte Interamericana de Direitos Humanos. **Revista Brasileira De Direitos Fundamentais & Justiça**, 11(36), 2017, p. 175-202. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/117.

LYNCH, Jennifer. **Face Off**: Law Enforcement Use of Face Recognition Technology. Electronic Frontier Foundation, abril 2020. Disponível em: https://url.gratis/1YSxY.

LOSA, Guillermo. Ministerio del Interior usará tecnología de identificación facial en las calles. **El Observador**, 20 mar. 2019. Disponível em: https://url.gratis/Agk7P.

LUNA, Mauricio. Reconocimiento facial en la ciudad de Buenos Aires: cómo será el sistema que ayudará a capturar a los 46 mil prófugos de la Justicia. **Infobae**, abril de 2019. Disponível em: https://bit.ly/2WNcj65.

MARGULIES, Peter. Surveillance By Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights. **Fla. L. Rev.**, [s.l.], vol. 68, nº 4, 2016. Disponível em: https://url.gratis/WfdRA.

MONTEIRO, Felipe Mattos; CARDOSO, Gabriela Ribeiro. A Seletividade do sistema prisional brasileiro e o perfil da população carcerária. Um Debate Oportuno. **Civitas**, Porto Alegre, v. 13, n. , 2013, p. 93-77. Disponível em: https://bit.ly/31a5nU0

MONTES, Álvaro. El reconocimiento facial no es una buena opción. **Semana**, 22 fev. 2020. Disponível em: https://bit.ly/2xmC1pC. Acesso em: 20 abr. 2020.

MONTEVIDEO PORTAL. Uruguay busca potenciar el uso de tecnología china en materia de seguridad. 09 nov. 2018. Disponível em: https://bit.ly/2WZRkgq.

NISTIR. **NIST Interagency/Internal Report (NISTIR) 8280** - Face recognition vendor test part 3: Demographic Effects. Dez. 2019. Disponível em: https://bit.ly/2U1I0co. Acesso em: 10 jan. 2020.

NOTICIAS CARACOL. Así es el sofisticado sistema de videovigilancia que se estrenó en cali. **Noticias Caracol**, 19 dez. 2019. Disponível em: https://bit.ly/2SjB0Wr.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. *In*: REDE DE OBSERVATÓRIOS DA SEGURANÇA. **Retratos da Violência Cinco meses de monitoramento, análises e descobertas**. CESEC, jun. - out. 2019, p. 67-70. Disponível em: https://bit.ly/35Om1tj.

PANAMÁ AMÉRICA. Suman 150 cámaras para fortalecer sistema de Reconocimiento Facial. **Panamá América**, 05 dez. 2019. Disponível em: https://bit.ly/36bbTep.

PELÁEZ, Arístides Victoria. República Dominicana: ¿Y nuestros datos? Breve análisis sobre la actual normativa de protección de datos y las nuevas tendencias. **ECIJA**, 31 mar. 2020. Disponível em: https://bit.ly/2yyKVRp. Acesso em: 03 maio 2020.

PEÑA, Paz (coord.). **Recomendaciones para la transparencia y anticorrupción en la adquisición y uso de tecnologías de vigilancia por parte de los Estados americanos**. Grupo de trabajo: Transparencia y derechos humanos en las políticas en torno a las tecnologías de vigilancia, março 2018. Disponível em: https://bit.ly/2T6HCYz.

PEREYRA, Silvana E. S., Biometría y vigilancia social en Sudamérica: Argentina como laboratorio regional de control migratorio. **Revista Mexicana de Ciencias Políticas y Sociales**. ano 53, num. 232. 2018, p. 247-68. disponível em: http://www.scielo.org.mx/pdf/rmcps/v63n232/0185-1918-rmcps-63-232-247.pdf. Acesso em: 20 abr. 2020

PETRESCU, Relly Victoria Virgil. Face Recognition as a Biometric Application. **Journal of Mechatronics and Robotics**, [s.l.], vol. 3, 2019, p. 237-57. Disponível em: https://thescipub.com/pdf/10.3844/jmrsp.2019.237.257. Acesso em: 02 fev. 2020.

PMERJ (2019a). **Polícia Militar vai implantar programa de reconhecimento facial e de plana de veículos**. Polícia Militar do Estado do Rio de Janeiro, 22 jan. 2019. Disponível em: https://bit.ly/3bcqDdC.

PMERJ (2019b). **OAB convida polícia militar para debater reconhecimento facial**. Polícia Militar do Estado do Rio de Janeiro, 02 dez. 2019. Disponível em: https://bit.ly/2WexHlP.

R3D. Un hombre estuvo seis días arrestado por un error de reconocimiento facial en buenos aires. **R3D - Privacidad**, 06 ago. 2019. Disponível em: https://bit.ly/2Si3gc3.

Secretaria-geral da Presidência da República e Secretaria Nacional de Juventude. **Mapa do encarceramento: os jovens do Brasil**. Brasília, 2015. Disponível em: https://bit.ly/34eWqe9.

SCHERER, Matthew U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. **Harv. J. L. & Tech.**, vol. 29, n. 2, 2016.

SIC - Superintendencia Indústria y Comércio. **Protección de Datos Personales en Sistemas de Videovigilancia**. Set. 2016. Disponível em: https://bit.ly/3cYmDio.

SILVA, Alex Lima Silva; CINTRA, Marcos Evandro. Reconhecimento de padrões faciais: Um estudo. *In*: **XII Encontro Nacional de Inteligência Artificial e Computacional (ENIAC)**, 2015, Natal. Disponível em: https://bit.ly/36T0A99. Acesso em: 02 fev. 2020.

SILVA, Leire Taíze Ribeiro da e SILVA, Marcelo Alves da. Parceria público-privada como instrumento de concretização do direito à saúde. Revista Digital de Direito Administrativo. V. 6, n. 1, 2019.

SILVEIRA; Denise Tolfo; CÓRDOVA, Fernanda Peixoto. A Pesquisa Científica. *In*: GERHARDT, Tatiana Engel; SILVEIRA, Denise Tolfo. **Métodos de pesquisa**. Porto Alegre: Editora da UFRGS, 2009. p. 31-42.

TECNOSFERA. En que vá el reconocimiento facial en Colombia?. **EL TIEMPO**, 17 maio 2019. Disponível em: https://bit.ly/3cYBTf6.

TURNER, Jacob. **Robot Rules**: Regulating Artificial Intelligence. Nova Iorque: Palgrave Macmillan, 2019.

UCCIFERRI, Leandro. #ConMiCaraNo: Reconocimiento facial en la ciudad de Buenos Aires. Asociación por los Derechos Civiles, 23 maio 2019. Disponível em: https://url.gratis/Kd0un.

URUGUAY. Ministerio del Interior. **Análisis Preliminar de los Efectos del Sistema de Videovigilancia de la Ciudad Vieja**. Javier Donnangelo, Director División Estadística y Análisis Estratégico. Jul. 2014. Disponível em: https://bit.ly/3czvEi2.

URUGUAY (2018a). Ministerio del Interior. El Aeropuerto de Carrasco incorporó el reconocimiento facial en las puertas de embarque. **UNICOM**, Montevideo, 29 out. 2018. Disponível em: https://bit.ly/2z1HXVA.

URUGUAY (2018b). Unidad Reguladora y de Control de Datos Personales (URCDP). **Guía de videovigilancia en las entidades públicas**, 14 dez. 2018. Disponível em: https://bit.ly/2UDiPvX.

URUGUAY (2018c). Unidad Reguladora y de Control de Datos Personales (URCDP). Guía de videovigilancia en el ámbito laboral, 14 dez. 2018. Disponível em: https://bit.ly/2UCQBle.

URUGUAY PRESIDENCIA. Cinco años de sistema de videovigilancia erradicaron 4 de cada 5 hurtos en Ciudad Vieja y 73% de las rapiñas. **Uruguay Presidencia - Noticias**, 07 dez. 2017. Disponível em: https://bit.ly/35Z2zKi.

VILLALOBOS FONSECA, Hazel. El desarrollo tecnológico en materia policial: una receta de éxito para la prevención del delito. **Revista Relaciones Internacionales, Estrategia y Seguridad**, [s.l.], vol. 15, n. 01, jan.-jun. 2020. p. 79-97. DOI: https://doi.org/10.18359/ries.4243. Acesso em: 30 abr. 2020.

WHITTAKER, Meredith *et al.* **AI Now Report 2018**. Disponível em: https://ainowinstitute.org/AI_Now_2018_Report.pdf. Acesso em: 22 jan. 2020.

ZAMBRANO, Abdías. Cámaras de videovigilancia: ¿Nos cuidan o nos vigilan?. **IPANDETEC**, 18 jan. 2019. Disponível em: https://bit.ly/3fNNtMc.