REVISTA DE DIREITO INTERNACIONAL

BRAZILIAN JOURNAL OF INTERNATIONAL LAW

Editores responsáveis por essa edição:

Editores:

Nitish Monebhurrun

Ardyllis Alves Soares

Marcelo Dias Varella

Editores convidados:

Hervé Ascensio

Julien Chaisse

ISSN 2237-1036

Revista de Direito Internacional Brazilian Journal of International Law	Brasília	v. 18	n. 2	p. 1-397	ago	2021

doi: 10.5102/rdi.v18i2.7677

O reconhecimento facial nas *smart cities* e a garantia dos direitos à privacidade e à proteção de dados pessoais

Facial recognition in *smart cities* and the guarantee of the rights to privacy and personal data protection

Diogo Dal Magro**
Vinícius Borges Fortes***

* Recebido em 12/06/2021
Aprovado em 11/11/2021

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

*** Possui Estágio de Pós-Doutorado em Direito pela Vrije Universiteit Brussel, Bélgica (2016), com pesquisa voltada aos Direitos de privacidade na internet e o sistema de proteção de dados. Doutorado em Direito pela Universidade Estácio de Sá - UNESA (2015), com período sanduíche na Universidad de Zaragoza (2014-2015), com financiamento do PDSE/CAPES. Mestrado em Direito pela Universidade de Caxias do Sul (2011). Graduação em Direito pela FAPLAN - Faculdades Planalto (2008). Atualmente, é pesquisador e Bolsista de Produtividade em Pesquisa com dedicação exclusiva ao CETID - Centro de Pesquisa, Tecnologia e Inovação Digital da Fundação Meridional. Ainda, é líder do Projeto de Pesquisa Latin America Privacy Hub (LAPH), certificado pela IMED no Diretório de Grupos de Pesquisa do CNPq, financiado pelo CETID/Fundação Meridional. Professor permanente do Programa de Pós-Graduação Stricto Sensu em Direito da IMED - Faculdade Meridional, onde foi coordenador no período 2017-2019. Professor dos cursos de Graduação em Direito e Ciência da Computação da IMED - Faculdade Meridional.
E-mail: vinicius.fortes@imed.edu.br

Resumo

As *smart cities* comportam um sistema hiperconectado de pessoas e coisas, alimentado por dados. As tecnologias de reconhecimento facial, presentes nas *smart cities* da China, contribuem para os modernos processos de *surveillance*. O objetivo geral do estudo é compreender, com base no caso chinês, as consequências da adoção do modelo de reconhecimento facial das *smart cities* no Brasil. O método de abordagem utilizado é o indutivo. O reconhecimento facial implica consequências a uma razoável expectativa de privacidade, ao anonimato e à autonomia individual. Por isso, os direitos fundamentais de privacidade e proteção de dados pessoais são limites que devem ser observados, objetivamente, para a utilização desse modelo de *smart cities* no Brasil.

Palavras-chave: *Smart Cities*; Reconhecimento facial; Privacidade; Proteção de dados pessoais.

Abstract

Smart cities have a hyperconnected system of people and things, powered by data. Facial recognition technologies, present in China's smart cities, contribute to modern surveillance processes. The general objective of the study is to understand, from the Chinese case, the consequences of adopting this model of smart cities in Brazil. The approach method used is the inductive. Facial recognition implies consequences for a reasonable expectation of privacy, anonymity and individual autonomy. For this reason, the fundamental rights of privacy and personal data protection are limits that must be observed, objectively, for the use of this model of smart cities in Brazil.

Keywords: Smart Cities; Facial recognition; Privacy; Personal data protection.

1 Introdução

Em 20 de janeiro de 2020, as autoridades da cidade chinesa de Suzhou divulgaram fotos de sete pessoas, acompanhadas de número de identificação governamental e localização, após suas condutas serem classificadas como "comportamento não civilizado". O motivo: estarem vestindo pijamas em público. A ferramenta utilizada para identificar as pessoas é o reconhecimento facial.[1]

A China, acostumada à vigilância, tem aproveitado as inovações tecnológicas fruto da sociedade da informação. Suas *smart cities*, equipadas com amplas redes hiperconectadas de pessoas e coisas, impactam, significativamente, a vida de seus cidadãos, transformando-os em cidadãos-*gamers*, pontuando suas condutas diárias – afrontando se o episódio *Nosedive* (Queda livre), de Black Mirror, ainda é distopia, ou se já é realidade.

É categórico que o Estado chinês é dotado de particularidades históricas. No entanto, a circulação, para o globo, dessas tecnologias, tem elevado as preocupações sobre privacidade, proteção de dados pessoais e *surveillance*. Diante disso, o problema de pesquisa apresenta-se por meio da indagação: de que maneira o modelo de reconhecimento facial das *smart cities* chinesas compromete os direitos fundamentais à privacidade e à proteção de dados pessoais no Brasil?

O objetivo geral destina-se a compreender, com base no caso chinês, as consequências da adoção do modelo de reconhecimento facial das *smart cities* no Brasil. Para perquirição dessa finalidade, são tomados os seguintes objetivos específicos: a) definir e correlacionar o avanço das tecnologias de reconhecimento facial como processos de *surveillance* nas *smart cities*; b) conceituar *smart cities* e suas diferentes concepções no mundo oriental e ocidental; c) estabelecer, conceitualmente, a correlação entre privacidade e proteção de dados pessoais no uso das *smart cities*; d) analisar os impactos das tecnologias de *surveillance* sob o processo democrático nas *smart cities*.

A hiperconectividade é um fator crescente nas *smart cities* e as inovações sempre constantes das tecnologias da informação e comunicação são responsáveis por ocasionar remodelagens urbanas. Daí a justificativa do presente estudo, ao analisar as decorrências da introdução dessas tecnologias na vida urbana, principalmente no caso do reconhecimento facial, em que sua operacionalização passa despercebida, eis perfectibilizada por meio de coleta de informações sem a necessidade do contato humano-máquina.

O estudo desenvolvido com base no caso da China observa a seguinte premissa: a análise realizada é a da camada fática, e não legal, do caso chinês. Examina-se, portanto, o efeito fático de fenômeno tecnológico para, após isso, arguir-se se a replicação do modelo de *smart cities* chinesas no Brasil é, ou não, recepcionado. Esse destaque é importante, principalmente, na medida em que China possui, sob o ponto de vista legal, uma frágil proteção à privacidade e aos dados pessoais.

O estudo divide-se em três partes. No primeiro capítulo, apresenta-se o modelo de *smart cities* em andamento na China e suas consequências, que nutrem a *surveillance*, especialmente, por meio do reconhecimento facial. No segundo capítulo, explica-se a operabilidade do reconhecimento facial e como essa tecnologia ocasiona profundos reflexos na privacidade. No terceiro capítulo, ao examinar o interesse do Brasil para adoção do modelo de *smart cities* chinesas, aponta-se para os limites que são impostos pela matriz constitucional brasileira a respeito da garantia dos direitos fundamentais de privacidade e proteção de dados pessoais.

O método de abordagem utilizado é o indutivo. Esse método consiste em "pesquisar e identificar as partes de um fenômeno e colecioná-las de modo a ter uma percepção ou conclusão geral [...]".[2] A seleção desse método de abordagem dá-se pela análise da premissa específica do modelo da *smart cities* da China. Com base no caso analisado, serão reunidas as partes que comporão as premissas gerais da análise, de modo a utilizá-las para a compreensão do modelo de *smart cities* a serem projetadas para o Brasil. Quanto ao método de procedimento, este é o comparativo, uma vez que analisa parte dos fenômenos observados no caso chinês, sendo replicada essa análise aos fenômenos que serão utilizados como parâmetro no Brasil.

[1] AMY QIN. Chinese city uses facial recognition to shame pajama wearers. *The New York Times*, jan. 2020. Disponível em: https://www.nytimes.com/2020/01/21/business/china-pajamas-facial-recognition.html?searchResultPosition=13 Acesso em: 11 abr. 2021.

[2] PASOLD, Cesar Luiz. *Metodologia da pesquisa jurídica*: teoria e prática. 11. ed. Florianópolis: Conceito Editorial; Millenium Editora, 2008. p. 86.

2 *Smart surveillance*: o caso de reconhecimento facial aplicado às smart cities chinesas

O movimento das *smart cities* não é um resultado acidental recente. Tendo surgido com o avanço econômico e com o desenvolvimento urbano, a partir da década de 1970, faz parte de um plano evolutivo das cidades, sendo classificadas em cidade competitiva, cidade sustentável e cidade inteligente, não sendo esta, contudo, uma classificação clara, linear ou temporal.[3] Uma *smart city* possui, portanto, aspectos diferentes, em decorrência de configurações econômicas, geográficas, históricas e tecnológicas específicas de cada localidade.[4]

O conceito de *smart city* gera divergências e convergências na literatura.[5] Certo é que, no âmbito da convergência, a literatura é uníssona em estabelecer um núcleo ao conceito de *smart city*: *"technology, in the context of the rise of the knowledge economy."*[6] A tecnologia tem sido o elemento nevrálgico definidor de uma cidade como *smart city*, de modo que a evolução da tecnologia da informação e da economia do conhecimento[7] facilitaram o avanço do movimento das *smart cities*, utilizando, principalmente, mecanismos de *big data*[8] e *Internet of Things (IoT)*[9].[10]

Com base nessas tecnologias, as *smart cities* atingem seus objetivos de incluir, em seu contexto, pessoas inteligentes, ambiente inteligente, mobilidade inteligente, economia inteligente, governança inteligente, serviços inteligentes, infraestrutura inteligente e vida inteligente.[11] As tecnologias disruptivas[12] também são um

[3] HU, Richard. Planning for economic development. *In:* HEIN, Carola. *The Routledge Handbook of Planning History*. London; New York: Routledge, 2017. p. 313-324.

[4] HU, Richard. The state of smart cities in China: the case of Shenzhen. *Energies*, v. 12, n. 22, p.4375-4393, nov. 2019. p. 2. DOI: http://dx.doi.org/10.3390/en12224375 Disponível em: https://www.mdpi.com/1996-1073/12/22/4375 Acesso em: 29 mar. 2021.

[5] "*Several systematic and comprehensive literature reviews converge on an understanding that the smart city concept is multi-faceted, complex, confusing, ambiguous, contingent, fragmented, and lacks cohesion."* Tradução livre: "Várias revisões sistemáticas e abrangentes da literatura convergem no entendimento de que o conceito de cidade inteligente é multifacetado, complexo, confuso, ambíguo, contingente, fragmentado e carece de coesão." HU, Richard. The state of smart cities in China: the case of Shenzhen. *Energies*, v. 12, n. 22, p.4375-4393, nov. 2019. p. 2. DOI: http://dx.doi.org/10.3390/en12224375 Disponível em: https://www.mdpi.com/1996-1073/12/22/4375 Acesso em: 29 mar. 2021.

[6] Tradução livre: "tecnologia, no contexto da ascensão da economia do conhecimento." HU, Richard. The state of smart cities in China: the case of Shenzhen. *Energies*, v. 12, n. 22, p.4375-4393, nov. 2019. p. 2. DOI: http://dx.doi.org/10.3390/en12224375 Disponível em: https://www.mdpi.com/1996-1073/12/22/4375 Acesso em: 29 mar. 2021.

[7] *"We define the knowledge economy as production and services based on knowledge-intensive activities that contribute to an accelerated pace of technological and scientific advance as well as equally rapid obsolescence. The key components of a knowledge economy include a greater reliance on intellectual capabilities than on physical inputs or natural resources, combined with efforts to integrate improvements in every stage of the production process, from the R&D [Research and Development] lab to the factory floor to the interface with customers."*. Tradução livre: "Definimos a economia do conhecimento como produção e serviços baseados em atividades intensas de conhecimento que contribuem para um ritmo acelerado de avanço tecnológico e científico, bem como para uma obsolescência igualmente rápida. Os componentes principais de uma economia do conhecimento incluem uma dependência maior de recursos intelectuais do que de insumos físicos ou recursos naturais, combinados com esforços para integrar melhorias em todas as etapas do processo de produção, desde o laboratório de pesquisa e desenvolvimento até o chão de fábrica e a interface com os clientes." POWELL, Walter W.; SNELLMAN, Kaisa. The knowledge economy. *Annual Review of Sociology*, v. 30, n. 1, p. 199-220, ago. 2004. p. 201. DOI: http://dx.doi.org/10.1146/annurev.soc.29.010202.100037 Disponível em: https://www.annualreviews.org/doi/full/10.1146/annurev.soc.29.010202.100037 Acesso em: 27 mar. 2021.

[8] "Big data é um termo em evolução que descreve qualquer quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que têm o potencial de ser explorados para obter informações." MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV, 2018. p. 22.

[9] "Existem fortes divergências em relação ao conceito de IoT, não havendo, portanto, um conceito único que possa ser considerado pacífico ou unânime. De maneira geral, pode ser entendido como um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade." MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV, 2018. p. 20.

[10] HU, Richard. The state of smart cities in China: the case of Shenzhen. *Energies*, v. 12, n. 22, p.4375-4393, nov. 2019. p. 3. DOI: http://dx.doi.org/10.3390/en12224375 Disponível em: https://www.mdpi.com/1996-1073/12/22/4375 Acesso em: 29 mar. 2021.

[11] HONG XU; XUEXIAN GENG. People-centric service intelligence for smart cities. *Smart Cities*, v. 2, n. 2, p.135-152, abr. 2019. DOI: http://dx.doi.org/10.3390/smartcities2020010 Disponível em: https://www.mdpi.com/2624-6511/2/2/10/xml Acesso em: 15 mar. 2021.

[12] *"Disruptive technologies can be considered scientific discoveries that break through the usual product/technology capabilities and provide a basis for a new competitive paradigm."*. Tradução livre: "As tecnologias disruptivas podem ser consideradas descobertas científicas que rompem com os recursos usuais de produto/tecnologia e fornecem uma base para um novo paradigma competitivo." KOSTOFF, Ronald N.; BOYLAN, Robert; SIMONS, Gene R. Disruptive technology roadmaps. *Technological Forecasting and Social Change*, v. 71, n. 1-2, p. 141-159, jan. 2004. p. 142. DOI: http://dx.doi.org/10.1016/s0040-1625(03)00048-9 Disponível em: https://www.sciencedirect.com/journal/technological-forecasting-and-social-change/vol/71/is-

componente importante das *smart cities*, visto que são responsáveis por introduzir novos produtos e serviços, alterando a lógica de consumo e de comportamento então predominantes, intencionalmente.

A utilização de tecnologias da informação como IoT tem possibilitado a vivência de uma sociedade hiperconectada[13] de pessoas e coisas. Governos visionários ao redor do globo têm compreendido esse cenário como possibilidade de criação de projetos de cidades onipresentes ('*u-city*', abreviação de '*ubiquitous city projects*'), compreendidas como cidades equipadas com redes por meio das quais as autoridades (gerais ou locais) são capazes de monitorar tudo o que acontece.[14]

Em 18 de outubro de 2017, por ocasião do *19th National Congress of the Communist Party of China,* o presidente da China, Xi Jinping, encaminhou ao evento o documento *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era*. Nele, o presidente exprime por tornar a China um país de inovadores, por meio dos horizontes da ciência e da tecnologia.

> *These efforts will provide powerful support for building China's strength in science and technology, product quality, aerospace, cyberspace, and transportation; and for building a digital China and a smart society.*[15]

O conceito de *smart society* representa uma expansão conceitual e uma aspiração ambiciosa do conceito de *smart city*, tornando-a uma estratégia nacional, sendo descrita como uma inovação teórica que corresponde a uma nova versão do modelo chinês de *smart city*.[16] Em 2014, o Conselho de Estado da China divulgou o *Planning Outline for the Construction of a Social Credit System (2014–2020)*[17], planejando o aprimoramento[18] de um dos principais métodos já em utilização em várias *smart cities* chinesas: o Sistema de Créditos[19] Sociais.

sue/1 Acesso em: 15 abr. 2021.

13 "O termo *hiperconectividade* está hoje atrelado às comunicações entre indivíduos (*person-to-person,* P2P), indivíduos e máquinas (*human-to-machine,* H2M) e entre máquinas (*machine-to-machine,* M2M) valendo-se, para tanto, de diferentes meios de comunicação. Há, nesse contexto, um fluxo contínuo de informações e massiva produção de dados.". MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV, 2018. p. 21.

14 DONG-HEE SHIN. Ubiquitous city: urban technologies, urban infrastructure and urban informatics. *Journal of Information Science*, v. 35, n. 5, p. 515-526, set. 2009. DOI: http://dx.doi.org/10.1177/0165551509100832 Disponível em: https://journals.sagepub.com/doi/10.1177/0165551509100832 Acesso em: 27 mar. 2021.

15 Tradução livre: "Esses esforços fornecerão um apoio poderoso para fortalecer a força da China em ciência e tecnologia, qualidade de produtos, aeroespaço, ciberespaço e transporte; e para construir uma China digital e uma sociedade inteligente." XI JIPING. *Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with chinese characteristics for a new era.* 2017. p 27. Disponível em: http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf. Acesso em: 26 mar. 2021.

16 HONG XU; XUEXIAN GENG. People-centric service intelligence for smart cities. *Smart Cities*, v. 2, n. 2, p.135-152, abr. 2019. p. 7. DOI: http://dx.doi.org/10.3390/smartcities2020010 Disponível em: https://www.mdpi.com/2624-6511/2/2/10/xml Acesso em: 15 mar. 2021.

17 O referido documento planeja o aprimoramento do Sistema de Créditos Sociais (SCS) sob três aspectos: i) comprometer-se em implantar o sistema nacionalmente até 2020; ii) expandir o número de colabores envolvidos na construção técnica do Sistema de Créditos Sociais; iii) construir plataformas nacionais de dados a fim de coletar, armazenar, compartilhar e extrair dados de toda a população. LIANG, Fan *et al*. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, v. 10, n. 4, p.415-453, ago. 2018. p. 11-12. DOI: http://dx.doi.org/10.1002/poi3.183 Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.183 Acesso em: 05 abr. 2021.

18 A origem do Sistema de Créditos Sociais (SCS) remonta aos anos 1990, na chamada Dívida do Triângulo. Após reformas econômicas do governo chinês, várias empresas passaram a ficar em débito umas com as outras. Para solucionar o problema, o governo resolveu realizar empréstimo para empresas, não sem antes realizar uma avaliação do crédito, por meio de companhias de avaliação de crédito. A partir dos anos 2000, passaram a ser feitas, também, por meio de empresas estatais, avaliações do crédito dos consumidores. Em 2002, o presidente Jiang Zemin defendeu a criação de um sistema de crédito social compatível com a economia modernizada. A partir de 2007, passaram a ocorrer Sistemas de Reuniões Ministeriais Conjuntas, a fim de promover a criação de um sistema de crédito a nível nacional. Até esse momento, a área de abrangência do sistema de crédito era o econômico. A partir de 2011, o sistema de crédito passou a abranger assuntos governamentais, comportamentos comerciais, atividades sociais e assuntos judiciais. O principal objetivo da construção de um sistema de crédito destinava-se a uma análise financeira do crédito. Entretanto, embora a China tenha tentado construir plataformas de dados para o sistema de crédito, não conseguiu dados suficientes para pontuar o crédito. Isso porque o governo tinha dados escassos para avaliar os domínios econômico e financeiro das pessoas, além de que o projeto inicial abrangia toda a sociedade. Somente em 2014, o aspecto social do crédito foi incluído, dando origem ao Sistema de Crédito Social. LIANG, Fan *et al*. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, v. 10, n. 4, p.415-453, ago. 2018. p. 10-11. DOI: http://dx.doi.org/10.1002/poi3.183 Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.183 Acesso em: 05 abr. 2021.

19 A tradução, da língua chinesa, do conceito de "crédito", traz algumas complicações. O termo pode ser utilizado para indicar ideias de "integridade", "crédito", "reputação" e "credibilidade". Historicamente, a China utiliza o conceito de "crédito" para indicar princípios morais, principalmente no que concerne aos aspectos éticos individuas. Apenas na história mais recente, o termo passou indicar aspectos sociais, financeiros e jurídicos. LIANG, Fan *et al*. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, v. 10, n. 4, p.415-

Esse sistema já está em vigor, em nível local, em algumas cidades da China, servindo como modelos embrionários. No Condado de Suining, Província de Jiangsu, foi estabelecido, em 2010, um sistema de créditos, a fim de medir e pontuar a conduta dos cidadãos, operando do seguinte modo: cada cidadão inicia com um total de 1.000 pontos, sendo que a cada quebra de normas, há uma subtração de pontos, dando origem ao *score* (pontuação) individual. Essa dedução ocorre não apenas pelo infringimento de normas legais (estritas), mas também por infringir normas administrativas e inclusive morais.[20]

Entre as condutas que podem levar a uma perda de pontos, tem-se: conduzir automóvel embriagado acarreta a perda de 50 pontos; ter um bebê fora das permissões do planejamento familiar custa 35 pontos; não realizar o pagamento de empréstimos gera uma dedução de 30 a 50 pontos. Gradativamente, os cidadãos podem recuperar os pontos perdidos dentro de um período de 2 a 5 anos, a depender da norma violada e da gravidade da infração.[21]

A partir do *score* individual, cidadãos são categorizados em classes de A a D. Enquanto cidadãos da classe A possuem acesso preferencial a oportunidades de emprego, indivíduos das demais classes são submetidos, relativamente, à classe pertencente, a um exame minucioso de requisitos específicos para poder, exemplificativamente: tornar-se membro de partido político; realizar alistamento militar; qualificar-se em processo para concorrer a moradias de baixo custo; obter licenças de funcionamento na categoria de comerciante individual.[22]

O governo de Suining também criou um registro público do score de cada cidadão, contendo os nomes e as ações dos infringidores, prática posteriormente conhecida como *blacklist* (lista negra). Após receber críticas, o sistema de classificação de A a D e a *blacklist* foram descartadas. Nada obstante, a experiência de Suining deixou legados: a ideia de desincentivos para cidadãos que infringirem normas; a publicização do nome dos agressores, expondo-os à vergonha; e, principalmente, a expansão da utilização do mecanismo de crédito para além do contexto econômico, atingindo, também, a violação de normas administrativas e de gestão urbana.[23]

O grande avanço que permite o desenvolvimento de sistemas de controle sofisticados é o reconhecimento facial.[24] Por essa razão, está em construção, na China, um projeto lançado em 2015 pelo Ministério da Segurança, capaz de identificar qualquer indivíduo entre seus 1,3 bilhão de habitantes em, apenas, três segundos. As informações relativas à imagem dos cidadãos perfazem um total de 13 terabytes, enquanto o banco de dados completo totaliza 90 terabytes[25].[26]

Tal qual o Sistema de Créditos Sociais, o emprego de reconhecimento facial é realidade em diversos pontos, em nível local. Em Pequim, alguns banheiros públicos

453, ago. 2018. p. 10. DOI: http://dx.doi.org/10.1002/poi3.183 Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.183 Acesso em: 05 abr. 2021.

[20] CREEMERS, Rogier. China's Social Credit System: an evolving practice of control. *Ssrn Electronic Journal*, p. 1-32, maio 2018. DOI: http://dx.doi.org/10.2139/ssrn.3175792 Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 Acesso em: 15 mar. 2021.

[21] CREEMERS, Rogier. China's Social Credit System: an evolving practice of control. *Ssrn Electronic Journal*, p. 1-32, maio 2018. DOI: http://dx.doi.org/10.2139/ssrn.3175792 Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 Acesso em: 15 mar. 2021.

[22] CREEMERS, Rogier. China's Social Credit System: an evolving practice of control. *Ssrn Electronic Journal*, p. 1-32, maio 2018. p. 10. DOI: http://dx.doi.org/10.2139/ssrn.3175792 Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 Acesso em: 15 mar. 2021.

[23] CREEMERS, Rogier. China's Social Credit System: an evolving practice of control. *Ssrn Electronic Journal*, p. 1-32, maio 2018. p. 10. DOI: http://dx.doi.org/10.2139/ssrn.3175792 Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 Acesso em: 15 mar. 2021.

[24] O número de câmeras de reconhecimento facial em uso na China era de 176 milhões em 2017, subindo para 626 milhões em 2020. DUDLEY, Lauren. China's Ubiquitous Facial Recognition Tech Sparks: Privacy Backlash Privacy concerns remain largely unaddressed in proposed Chinese facial recognition standards. *The Diplomat*, mar. 2020. Disponível em: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/ Acesso em: 01 abr. 2021.

[25] O sistema está sendo desenvolvido pela Isvision, empresa de segurança com sede em Xangai. Câmeras da Isvision com capacidade de reconhecimento facial foram instaladas em Pequim ainda em 2003, na Praça Tiananmen (famosa Praça da Paz Celestial). Conectado ao banco de dados policial, o sistema era capaz de reconhecer e rastrear suspeitos em meio à multidão. STEPHEN CHEN. China to build giant facial recognition database to identify any citizen within seconds. *South China Morning Post*, 12 out. 2017. Disponível em: https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any. Acesso em: 01 abr. 2021.

[26] STEPHEN CHEN. China to build giant facial recognition database to identify any citizen within seconds. *South China Morning Post*, 12 out. 2017. Disponível em: https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any. Acesso em: 01 abr. 2021.

utilizam reconhecimento facial em máquinas automáticas de *dispenser,* negando papel higiênico às pessoas que o solicitarem, mais de uma vez, em determinando período de tempo.[27]

Algumas habitações públicas de Pequim também utilizam reconhecimento facial para que os moradores tenham acesso às suas moradias, processo que leva menos de um segundo. A medida visa coibir o arrendamento desses imóveis, prática proibida. Desse modo, além de moradores, apenas determinadas empresas de entrega possuem acesso aos locais.[28]

Outra experiência recente é a metrópole de Shenzhen, que passou a punir cidadãos que atravessarem a rua fora da faixa de pedestres. Utilizando sistemas de câmeras com reconhecimento facial, indivíduos que cruzam a rua fora da faixa de pedestres, ou quando não é permitido, têm sua identidade reconhecida imediatamente, além de seu nome e fotografia instantaneamente publicizados em grandes telas localizadas nas laterais das ruas.[29]

Medidas como as de Shenzhen têm por fundamento punir socialmente, por meio do envergonhamento social. Trata-se de uma medida que visa banir comportamentos sociais moralmente indesejados, por meio da exposição pública. A utilização do Sistema de Créditos Sociais também tem, em seus objetivos, a construção de uma sociedade baseada na sinceridade e na confiabilidade, elementos ligados às formas de governo autoritárias e totalitárias, demonstrando a dimensão do controle social.[30]

Em 2016, o governo de Xangai lançou o aplicativo *"Honest Shanghai"*. De um lado, o aplicativo permite a consulta da reputação de crédito de empresas e estabelecimentos comerciais, incluindo a condição de higiene de restaurantes, por exemplo. Por outro lado, por meio do número de identificação governamental (ID) e realização do reconhecimento fácil, cidadãos podem acessar seu próprio relatório de crédito.[31]

As informações são extraídas de registros policiais e da previdência social, e contêm dados como: local de trabalho, carteira de habilitação e passaporte. Após um período de, aproximadamente, 24 horas, o aplicativo envia ao usuário uma avaliação pública do seu crédito (*score*). Com ela, os cidadãos podem ter acesso a recompensas, incluindo descontos em passagens aéreas pela Spring Airlines.[32]

Em que pese a ocorrência já corriqueira de uso de reconhecimento facial em aeroportos, estações de metrô, praças e locais públicos, em novembro de 2019, a China enfrentou seu primeiro caso noticiado de disputa judicial envolvendo o reconhecimento facial. Guo Bing, professor de direito da Universidade de Ciência e Tecnologia de Zhejiang, ajuizou ação contra o Hangzhou Safari Park, após o parque anunciar que passaria a utilizar tecnologia de reconhecimento em seu sistema de entrada e que os membros deveriam registrar as informações faciais antes de acessarem o parque.[33]

A argumentação de Guo Bing é de que o uso obrigatório de reconhecimento facial para a simples entrada

[27] STEPHEN CHEN. China to build giant facial recognition database to identify any citizen within seconds. *South China Morning Post*, 12 out. 2017. Disponível em: https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any. Acesso em: 01 abr. 2021.

[28] XINHUA. *Across China*: facial recognition, new watchdog of Beijing public rental neighborhoods. 2019. Disponível em: http://www.xinhuanet.com/english/2019-07/22/c_138247731.htm Acesso em: 01 abr. 2021.

[29] HIRANAND, Ravi. Jaywalk in Shenzhen get fined on WeChat: Shenzhen's jaywalkers get scolded on WeChat and shamed on public screens. *Abacus,* mar. 2018. Disponível em: https://www.abacusnews.com/future-tech/shenzhens-jaywalkers-get-scolded-wechat-and-shamed-public-screens/article/2138928 Acesso em: 01 abr. 2021.

[30] "Os movimentos totalitários são organizações maciças de indivíduos atomizados e isolados. Distinguem-se dos outros partidos e movimentos pela exigência de lealdade total, irrestrita, incondicional e inalterável de cada membro individual. Essa exigência é feita pelos líderes dos movimentos totalitários mesmo antes de tomarem o poder e decorre da alegação, já contida em sua ideologia, de que a organização abrangerá, no devido tempo, toda a raça humana. Contudo, onde o governo totalitário não é preparado por um movimento totalitário (como foi o caso da Rússia em contraposição com a Alemanha nazista), o movimento tem de ser organizado depois, e as condições para o seu crescimento têm de ser artificialmente criadas de modo a possibilitar a lealdade total que é a base psicológica do domínio total." ARENDT, Hannah. *Origens do totalitarismo*. São Paulo: Companhia das Letras, 1989. p. 373.

[31] O'MEARA, Sarah. New app rates Shanghai Citizens' Honesty: pilot ideas for nationwide social credit system are rolled out in China's biggest city. *Sixth Tone,* nov. 2016. Disponível em: http://www.sixthtone.com/news/1554/new-app-rates-shanghai-citizens%20-honesty Acesso em: 01 abr. 2021.

[32] O'MEARA, Sarah. New app rates Shanghai Citizens' Honesty: pilot ideas for nationwide social credit system are rolled out in China's biggest city. *Sixth Tone,* nov. 2016. Disponível em: http://www.sixthtone.com/news/1554/new-app-rates-shanghai-citizens%20-honesty Acesso em: 01 abr. 2021.

[33] MA ZHENHUAN. Park alters entry rules following facial recognition tech lawsuit. *China Daily,* nov. 2019. Disponível em: http://global.chinadaily.com.cn/a/201911/07/WS5dc38381a310cf3e35575f3a.html. Acesso em: 01 abr. 2021.

em um parque viola a legislação de proteção do consumidor. O caso foi aceito pelo Tribunal Popular do Distrito de Fuyang, em Hangzhou, capital da Província de Zhejiang.[34]

Também em 2019, a China protagonizou um caso de racismo (automatizado) utilizando reconhecimento facial, a fim de traçar um perfil e identificar uigures. Os uigures compõem um grupo minoritário, formado em sua maioria por muçulmanos, que vivem na cidade de Yarkand, região de Xinjiang. Os padrões de vida dos uigures remontam há séculos. Porém, recentemente, esse grupo vem sofrendo controle do governo chinês, a fim de enfraquecer seus compromissos com o Islã e transferi-los das fazendas para as fábricas.[35]

Com o intento de obter controle sobre a região de Xinjiang, postos de polícias, câmeras instaladas em ruas e dispositivos são equipados com tecnologia de reconhecimento facial, controlando quem entra e quem sai da região e o viver diários dos uigures. Por meio da inteligência artificial, um perfil dos uigures é traçado com base em características faciais, a fim de identificar indivíduos que são integrantes da minoria social.[36] [37]

Em meio ao surto de coronavírus (COVID-19), a empresa chinesa de inteligência artificial, SenseTime, anunciou o uso, em três locais públicos, de um sistema de reconhecimento facial aliado com câmeras de imagem térmica, a fim de identificar pessoas com temperatura elevada (sistema de detecção de febre). A partir disso, usuários do software passariam a receber alertas (*pop-up*) com os dados de identificação dessas pessoas como forma de aviso de possíveis pacientes do vírus.[38]

A SenseTime também informou que o software é capaz de identificar pessoas que não estavam usando máscaras em locais públicos, como forma de exigir que utilizassem a proteção para acessar edifícios. Para além disso, com a adição de algoritmos, o reconhecimento facial do software é capaz de identificar pessoas, com alto índice de precisão, mesmo utilizando máscaras.[39] [40]

O conjunto de tecnologias empregadas nas *smart cities*, como *big data*, IoT, inteligência artificial, reconhecimento facial, utilizadas pelos sistemas de crédito social, *blacklist* e monitoramento de pessoas, concebem o panorama de um Estado de vigilância.[41] Utilizar dessas

[34] MA ZHENHUAN. Park alters entry rules following facial recognition tech lawsuit. *China Daily,* nov. 2019. Disponível em: http://global.chinadaily.com.cn/a/201911/07/WS5dc38381a310cf3e35575f3a.html. Acesso em: 01 abr. 2021.

[35] BUCKLEY, Chirs; MYERS, Steven Lee. Battered but resilient after China's Crackdown. The New York Times, 18 jan. 2020. Disponível em: https://www.nytimes.com/2020/01/18/world/asia/china-uighurs-xinjiang-yarkand.html. Acesso em: 01 abr. 2021.

[36] BUCKLEY, Chirs; MYERS, Steven Lee. Battered but resilient after China's Crackdown. The New York Times, 18 jan. 2020. Disponível em: https://www.nytimes.com/2020/01/18/world/asia/china-uighurs-xinjiang-yarkand.html. Acesso em: 01 abr. 2021.

[37] Uma reportagem interativa realizada pelo *The New York Times*. BUCKLEY, Chirs; MOZUR, Paul; RAMZY, Austin. How China turned a city into a prision: a surveillance state reaches new Heights. *The New York Times*, 04 abr. 2019. Disponível em: https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html. Acesso em: 01 abr. 2021.

[38] JANE LI. China's facial-recognition giant says it can crack masked faces during the coronavirus. *Quartz,* fev. 2020. Disponível em: https://qz.com/1803737/chinas-facial-recognition-tech-can-crack-masked-faces-amid-coronavirus/ Acesso em: 01 abr. 2021.

[39] JANE LI. China's facial-recognition giant says it can crack masked faces during the coronavirus. *Quartz,* fev. 2020. Disponível em: https://qz.com/1803737/chinas-facial-recognition-tech-can-crack-masked-faces-amid-coronavirus/ Acesso em: 01 abr. 2021.

[40] Tecnologias de reconhecimento facial de pessoas utilizando máscaras também já é desenvolvida por empresas como Wisesoft, sediada na Província de Sichuan, que faz a análise facial em 3D e possui precisão de 98% em 1.000 pessoas analisadas. XINHUA. *Chinese company develops 3D facial recognition system*. 2020. Disponível em: http://www.xinhuanet.com/english/2020-03/04/c_138842757.htm Acesso em: 01 abr. 2021. A empresa Hanwang Technology Ltd, com sede em Pequim, também anunciou o desenvolvimento da tecnologia de reconhecimento artificial de pessoas utilizando máscaras, aliada a verificação de temperatura corporal, capaz de reconhecer 30 pessoas em 1 segundo, com uma precisão de 95%. POLLARD, Martin. Even mask-wearers can be ID'd, China facial recognition firm says. *Reuters,* mar. 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL Acesso em: 01 abr. 2021.

[41] Aqui um registro. Enquanto a China segue no aperfeiçoamento de tecnologias de reconhecimento facial durante a COVID-19, a empresa norte americana IBM (*International Business Machines Corporation*), após o assassinato de George Perry Floyd Jr., enviou carta ao *United States Congress*, datada de 8 de junho de 2020, assinada pelo CEO Arvind Krishna, afirmando que: *"Responsible technology policies - technology can increase transparency and help police protect communities but must not promote discrimination or racial injustice. IBM no longer offers general purpose IBM facial recognition or analysis software. IBM firmly opposes and will not condone uses of any technology, including facial recognition technology offered by other vendors, for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose which is not consistent with our values and Principles of Trust and Transparency. We believe now is the time to begin a national dialogue on whether and how facial recognition technology should be employed by domestic law enforcement agencies. Artificial Intelligence is a powerful tool that can help law enforcement keep citizens safe. But vendors and users of AI systems have a shared responsibility to ensure that AI is tested for bias, particularly when used in law enforcement, and that such bias testing is audited and reported. Finally, national policy also should encourage and advance uses of technology that bring greater transparency and accountability to policing, such as body cameras and modern data analytics techniques."* Tradução livre: "Políticas tecnológicas responsáveis - a tecnologia pode aumentar a transparência e ajudar a polícia a proteger as comunidades, mas não deve promover discriminação ou injustiça racial. A IBM não

tecnologias sem garantia de proteção aos direitos dos cidadãos, pode acarretar a construção de sistemas políticos de máximo controle e opressão social. Digno de um cenário orwelliano, a China vive o momento em que o *big data* encontra o *Big Brother*.[42] [43]

Importa apresentar que a ideia de vigilância, hoje aperfeiçoada, é pré orwelliana. Sua origem reside no projeto desenvolvido pelo pai do utilitarismo. O panóptico, modelo de prisão[44] elaborado pelo irmão de Jeremy Bentham, mas apresentado por esse, consistia em celas de prisão, dispostas em formato de círculo, entorno de um posto de guarda. A luminosidade, que entrava pelo lado exterior das celas, possibilitava que todos os movimentos de qualquer detento fossem monitorados por apenas um guarda.[45]

A essência da engenhosidade do panóptico consiste no aspecto de poder ver, sem ser visto. Com mecanismos capazes de impedir que os detentos vejam a presença do inspetor no posto de inspeção, as pessoas passam a sentir-se como estando sempre sob observação ou, ao menos, sob uma grande possibilidade dessa vigilância estar ocorrendo.[46] [47]

Com Michel Foucault o panóptico é utilizado como conceito filosófico para apontar e descrever os mecanismos de opressão e controle social que caracterizam o mundo moderno. Nesse sentido, para além de um mo-

oferece mais software de análise ou reconhecimento facial IBM de uso geral. A IBM se opõe firmemente e não tolerará o uso de nenhuma tecnologia, incluindo a tecnologia de reconhecimento facial oferecida por outros fornecedores, para vigilância em massa, criação de perfil racial, violações de direitos humanos e liberdades básicas ou qualquer finalidade que não seja consistente com nossos valores e Princípios de Confiança e Transparência. Acreditamos que agora é a hora de iniciar um diálogo nacional sobre onde e como a tecnologia de reconhecimento facial deve ser empregada pelas agências policiais nacionais. A inteligência artificial é uma ferramenta poderosa que pode ajudar a aplicação da lei a manter os cidadãos seguros. Porém, fornecedores e usuários de sistemas de IA têm uma responsabilidade compartilhada de garantir que a IA seja testada quanto a vieses [*human bias*], principalmente quando usada na aplicação da lei, e que esses testes de vieses [*human bias*] sejam auditados e relatados. Por fim, a política nacional também deve incentivar e avançar nos usos de tecnologias que tragam maior transparência e responsabilidade ao policiamento, como câmeras corporais e técnicas modernas de análise de dados." KRISHNA, Arvind. *IBM*. Armond, New York, jun. 2020. Disponível em: https://www.ibm.com/blogs/policy/wp-content/uploads/2020/06/Letter-from-IBM.pdf Acesso em: 10 jun. 2021. Na mesma direção, a Amazon publicou nota, em 10 de junho de 2020, afirmando que: *"We're implementing a one-year moratorium on police use of Amazon's facial recognition technology. We will continue to allow organizations like Thorn, the International Center for Missing and Exploited Children, and Marinus Analytics to use Amazon Rekognition to help rescue human trafficking victims and reunite missing children with their families. We've advocated that governments should put in place stronger regulations to govern the ethical use of facial recognition technology, and in recent days, Congress appears ready to take on this challenge. We hope this one-year moratorium might give Congress enough time to implement appropriate rules, and we stand ready to help if requested."* Tradução livre: "Estamos implementando uma moratória de um ano no uso policial da tecnologia de reconhecimento facial da Amazon. Continuaremos a permitir que organizações como Thorn, o Centro Internacional para Crianças Desaparecidas e Exploradas e o Marinus Analytics usem o Amazon Rekognition para ajudar a resgatar vítimas de tráfico humano e reunir crianças desaparecidas com suas famílias. Defendemos que os governos implementem regulamentações mais rígidas para governar o uso ético da tecnologia de reconhecimento facial e, nos últimos dias, o Congresso parece pronto para enfrentar esse desafio. Esperamos que esta moratória de um ano dê tempo ao Congresso para implementar regras apropriadas e estamos prontos para ajudar, se solicitado." AMAZON. *We are implementing a one-year moratorium on police use of Rekognition*. 2020. Disponível em: https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition Acesso em: 10 mar. 2021.

[42] *Big Brother* (Grande Irmão) é um personagem do romance distópico 1984, de George Orwell. Em um cenário em que as pessoas estão sob forte vigilância das autoridades do Estado, a figura do Grande Irmão, líder do partido, aparece para os cidadãos por meio de teletelas, dizendo frases como "o Grande Irmão zela por ti" e "o Grande Irmão está te observando".

[43] BOTSMAN, Rachel. Big data meets Big Brother as China moves to rate its citizens. *Wired,* 2017. Disponível em: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion. Acesso em: 29 mar. 2021.

[44] O termo utilizado é "casa de inspeção". Sem prejuízo disso, nos termos do próprio autor, "para dizer tudo em uma palavra, ver-se-á que ele é aplicável, penso eu, sem exceção, a todos e quaisquer estabelecimentos, nos quais, num espaço não demasiadamente grande para que possa ser controlado ou dirigido a partir de edifícios, queira-se manter sob inspeção um certo número de pessoas. Não importa quão diferentes, ou até mesmo quão opostos, sejam os propósitos: seja o de punir o incorrigível, encerrar o insano, reformar o viciado, confinar o suspeito, empregar o desocupado, manter o desassistido, curar o doente, instruir os que estejam dispostos em qualquer ramo da indústria, ou treinar a raça em ascensão no caminho da educação, em uma palavra, seja ele aplicado aos propósitos das prisões perpétuas na câmara da morte, ou prisões de confinamento antes do julgamento, ou casas penitenciárias, ou casas de correção, ou casas de trabalho, ou manufaturas, ou hospícios, ou hospitais, ou escolas.". BENTHAM, Jeremy. O panóptico ou a casa de inspeção. *In*: SILVA, Tomaz Tadeu da (org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008. p. 19-20.

[45] BENTHAM, Jeremy. O panóptico ou a casa de inspeção. *In*: SILVA, Tomaz Tadeu da (org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008. p. 20-13.

[46] BENTHAM, Jeremy. O panóptico ou a casa de inspeção. *In*: SILVA, Tomaz Tadeu da (org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008. p. 28-30.

[47] "Regozijo-me com o fato de que há, agora, pouca dúvida de que o plano possui as vantagens fundamentais que venho atribuindo a ele: quero dizer, a aparente onipresença do inspetor (se os teólogos me permitirem a expressão), combinada com a extrema facilidade de sua real presença.". BENTHAM, Jeremy. O panóptico ou a casa de inspeção. *In*: SILVA, Tomaz Tadeu da (org.). *O panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008. p. 30-31.

delo de poder elevado à sua forma ideal, "[...] na verdade, é uma figura de tecnologia política que pode e deve ser distinguido de qualquer uso específico.".[48]

Tal modelo clássico de vigilância recebeu incrementos com base nas inovações tecnológicas, principalmente por meio de infraestruturas de tecnologias da informação. Esses avanços propiciam a transformação da vigilância, que, além de evoluir em termos quantitativos, passa a ser acrescida também do elemento qualitativo dos dados, inclusive ultrapassando uma simples ideia de vigilância digital, para dar origem ao fenômeno da *surveillance*.[49] Ainda que não dissociadas, *surveillance* denota um fenômeno mais amplo e complexo do que a vigilância.[50]

A literatura também tem sinalizado, em semelhante avanço teórico, a diferença entre "*traditional surveillance*" em contraste à "*new surveillance*", sendo esta constituída a partir das novas tecnologias de coleta de informações pessoais.[51] Nesse sentido, é partir desse cenário que ocorre uma das dimensões da *surveillance*, em que "[...] *governments engage in mass surveillance on their own citizens – contradicting basic democratic practice*."[52]

Por isso, a tecnologia não é apenas um fator terceiro (externo) na *surveillance*, mas um componente próprio e, portanto, interno, das relações sociais cotidianas.[53] Fato é que o fenômeno da *surveillance*, além de ser tenro, é permanentemente renovado. Nesse passo, na medida em que a tecnologia é um fator determinante de uma cidade como *smart city*, a *surveillance* desenvolve-se em consonância e em linear velocidade, sendo aquela uma condição para a existência dessa.

O reconhecimento facial opera para além da função de simples olhos do inspetor do panóptico, indicando a superação do panoptismo. O uso da tecnologia permite que o Estado: veja, sem ser visto; identifique indivíduos com facilidade e rapidez; controle comportamentos dos indivíduos pelo simples temor de estarem sob observação. Em uma *smart surveillance*, tais formas de coação, ainda que sutis, são concretas, apontando para uma limitação à liberdade individual, elemento definidor de um Estado como democrático.

3 O impacto do reconhecimento facial das *smart cities* na privacidade

As advertências de George Orwell e Aldous Huxley hoje soam como um clichê. Talvez, porque os cenários distópicos por eles descritos são hoje uma realidade já superada. À vista disso, este capítulo destina-se a verificar como o reconhecimento facial opera e como, *per se*, ou aliado a outras tecnologias como a inteligência artificial, quando empregado nas *smart citites*, pode acarretar complicações ao direito à privacidade.

Compreende-se que *"face identification involves one-to-many matching that compares a query face against multiple faces in the enrollment database to associate the identity of the query face to one of those in the database."*[54].[55] Desse modo, o processo de reconhecimento facial pode ser aplicado, simplesmente, para a identificação de pessoas ou, por

[48] FOUCAULT, Michel. *Vigiar e Punir*. Lisboa: Almedina, 2013. p. 158.

[49] De imediato, pontua-se que, na língua inglesa, "*surveillance*" e "*vigilance*" são conceitos diferentes, mas que acabam sendo traduzidos como "vigilância". Ainda, o já popular termo "*dataveillance*", que expressa a noção de "vigilância de dados", não é suficiente para expressar o fenômeno aqui em análise. De igual modo, a palavra de "*sousveillance*", cunhada na língua francesa a partir da substituição do prefixo "*sur*" (acima) por "*sous*" (abaixo), denota a ideia de que enquanto na *surveillance* o governo monitora seus cidadãos (de cima para baixo), a *sousveillance* expressa a vigilância dos cidadãos para com suas autoridades (de baixo para cima). MANN, Steve; NOLAN, Jason; WELLMAN, Barry. Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, v. 1, n. 3, p. 331-355, set. 2002. p. 332-333. DOI: http://dx.doi.org/10.24908/ss.v1i3.3344 Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3344 Acesso em: 15 abr. 2021.

[50] MENEZES NETO, Elias Jacob de. *Surveillance, democracia e direitos humanos*: os limites do Estado na era do big data. 2016. Tese (Doutorado em Direito) - Universidade do Vale do Rio dos Sinos - UNISINOS, São Leopoldo, 2016. p. 90-101.

[51] MARX, Gary T. What's new about the "new surveillance"?: classifying for change and continuity. *Knowledge, Technology & Policy*, v. 17, n. 1, p. 18-37, mar. 2004. p. 18. DOI: http://dx.doi.org/10.1007/bf02687074 Disponível em: https://link.springer.com/article/10.1007/BF02687074 Acesso em: 15 abr. 2021.

[52] Tradução livre: "governos se envolvem na vigilância em massa de seus próprios cidadãos – contradizendo a prática democrática básica." LYON, D. *Surveillance after Snowden*. Cambridge; Malden: MA: Polity Press, 2015. p. 337.

[53] MENEZES NETO, Elias Jacob de. *Surveillance, democracia e direitos humanos*: os limites do Estado na era do big data. 2016. Tese (Doutorado em Direito) - Universidade do Vale do Rio dos Sinos - UNISINOS, São Leopoldo, 2016. p. 93.

[54] Tradução livre: "Identificação de face envolve a correspondência um-para-vários que compara uma face de consulta com várias faces no banco de dados de registro para associar a identidade da face consultada a uma daquelas no banco de dados."

[55] STAN Z. LI *et al.* (orgs.). *Handbook of Face Recognition*. London: Springer London, 2011. p. 3.

outro lado, para verificação e confirmação da identidade de pessoas[56].[57]

Ambos os sistemas operam de forma similar, apresentando, usualmente, as seguintes etapas: aquisição de dados, pré-processamento de dados, extração de características e classificação.[58] Naturalmente, as técnicas utilizadas para o desenvolvimento de cada etapa podem variar, sem que, contudo, perca-se sua essência.

A etapa primeira de todo o processo é a de aquisição de dados. A entrada dos dados pode ser realizada por meio de tecnologias 2D ou 3D. No modelo 2D, câmeras realizam a captura de imagens estáticas ou imagens dinâmicas (vídeo) que serão posteriormente analisadas. Já na tecnologia 3D, a coleta é realizada por meio de scanner 3D ou sensor de profundidade.[59] Independentemente da técnica utilizada, as imagens capturadas constituem dados que deram entrada ao sistema de reconhecimento.

Após adquiridas as imagens, inicia-se a fase de pré-processamento dos dados. Os dados obtidos na fase anterior entram no processo de forma bruta. Isso significa que, seja em 2D ou 3D, as imagens podem conter ruídos, podendo ter sido gerados por componentes ópticos dos sensores (exemplo, lente), por condições externas (exemplo, luminosidade) ou por propriedades da face (exemplo, textura). Nessa fase, técnicas são aplicadas para remoção ou redução desses ruídos.[60]

Além de ruídos, as imagens são adquiridas sob diferentes condições de iluminação, diferentes ângulos da cabeça e com resoluções variadas. Por essa razão, é necessária a aplicação de diversas operações de pré-processamento, a fim de uniformizar os dados obtidos.[61]

A terceira etapa consiste na extração de características. As imagens obtidas como resultado das fases anteriores passam por um processo[62] de codificação, de modo que as informações (recursos) fotométricas (em imagens 2D) ou geométricas (em imagens 3D) são extraídas e reduzidas a códigos (discriminadas). As fases seguintes do processo utilizam as características (recursos) extraídos dessa etapa, e não a imagem inteira.[63]

Por fim, inicia-se a etapa de classificação. Para tal, importante esclarecer a pré-existência de um banco de dados, no qual consta um conjunto de informações referentes à indivíduos que, posteriormente, são submetidos ao reconhecimento facial. Posto isso, a classificação opera de dois modos diversos, de acordo com o objetivo do reconhecimento facial, ou seja, de um modo, para a identificação e, de outro, para a verificação.

---

[56] BOWYER, Kevin W.; CHANG, Kyong; FLYNN, Patrick. A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition. *Computer Vision and Image Understanding*, v. 101, n. 1, p. 1-15, jan. 2006. Disponível em: https://www.sciencedirect.com/science/article/pii/S1077314205000822 Acesso em: 14 abr. 2021.

[57] *"In a recognition scenario, the matching is one-to-many, in the sense that a probe is matched against all of the gallery to find the best match above some threshold. In an authentication scenario, the matching is one-to-one, in the sense that the probe is matched against the gallery entry for a claimed identity, and the claimed identity is taken to be authenticated if the quality of match exceeds some threshold."*. Tradução livre: Em um cenário de reconhecimento, a correspondência é de um-para-muitos, no sentido de que uma análise é comparada com toda a galeria para encontrar a melhor correspondência acima de algum limite. Em um cenário de autenticação, a correspondência é individual, no sentido de que o examinado é correspondido com a entrada da galeria para uma identidade reivindicada, e a identidade reivindicada é considerada autenticada se a qualidade da correspondência exceder algum limite. BOWYER, Kevin W.; CHANG, Kyong; FLYNN, Patrick. A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition. *Computer Vision and Image Understanding*, v. 101, n. 1, p. 1-15, jan. 2006. Disponível em: https://www.sciencedirect.com/science/article/pii/S1077314205000822 Acesso em: 14 abr. 2021.

[58] BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

[59] BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

[60] BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

[61] BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

[62] Há uma ampla variedade de métodos de extração de características, citando-se, exemplificativamente, *Eigenfaces, Fisherfaces, Laplacianfaces, Independent Component Analysis (ICA)* e *Discrete Cosine Transform (DCT)*. BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

[63] BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

Na identificação, o resultado do processamento das fases anterior é confrontado com todo o banco de dados, ou seja, uma correspondência de um para muitos. A imagem do banco de dados (galeria) mais próxima daquela em análise, com pontuação acima de determinado limite, é, então, utilizada para dar identidade ao indivíduo em análise.[64]

O indivíduo em análise pode ou não estar no banco de dados (galeria). Assim, exemplificativamente, na utilização de reconhecimento facial para encontrar um foragido em meio a uma multidão, os dados do foragido encontram-se no banco de dados (galeria), enquanto os da multidão não estão armazenados. Entretanto, o reconhecimento facial realiza as etapas de aquisição de dados, pré-processamento e extração de características, para, na fase final de classificação, concluir que, exceto o foragido, nenhum daqueles indivíduos fora identificado.

Já no modo verificação, os dados obtidos no processamento são comparados com as informações no banco de dados pertencentes à identidade que está sendo reivindicada, ou seja, uma correspondência de um para um. Havendo similaridade, acima de determinado limite, entre as identidades, há a verificação (autenticação) da identidade do indivíduo.[65]

Os sistemas de reconhecimento facial têm recebido extensas evoluções, precipuamente, através da inteligência artificial[66], por meio de *machine learning*[67] e *deep*

[64] BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

[65] BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

[66] O estudo fundador da inteligência artificial foi publicado em 1950, por Alan M. Turing, baseando-se na pergunta "*Can machines think*?" ("As máquinas podem pensar?"). TURING, A. M. Computing machinery and intelligence. *Mind,* v. 54, n. 236, p. 433-460, 1950. p. 433. *"Artificial Intelligence (AI), broadly (and somewhat circularly) defined, is concerned with intelligent behavior in artifacts. Intelligent behavior, in turn, involves perception, reasoning, learning, communicating, and acting in complex environments. AI has as one of its long-terms goals the development of machines that can do these things as well as humans can, or possibly even better. Another goal of AI is to understand this kind of behavior whether it occurs in machines or in humans or other animals. Thus, AI has both engineering and scientific goal."* Tradução livre: "Inteligência Artificial (IA), definida de maneira ampla (e um tanto circular), preocupa-se com o comportamento inteligente em artefatos. O comportamento inteligente, por sua vez, envolve percepção, raciocínio, aprendizado, comunicação e atuação em ambientes complexos. A IA tem como um de seus objetivos de longo prazo o desenvolvimento de máquinas que podem fazer essas coisas tão bem quanto os humanos, ou possivelmente até melhor. Outro objetivo da IA é entender esse tipo de comportamento, seja em máquinas ou em humanos ou outros animais. Assim, a IA tem ambos objetivos, de engenharia e científicos." NILSSON, Nils J. *Artificial intelligence*: a new synthesis. San Francisco: Morgan Kaufmann Publishers, 1998. Por um viés técnico, entende-se que *"Artificial Intelligence is the field of computer science aimed at developing hardware and/or software systems (more generally, computational models) capable of performing functions which have been traditionally considered unique and exclusive of human cognition. Among those capabilities, we can mention natural language and speech processing, expert reasoning and problem solving, such as diagnosis and design, vision, and learning."* Tradução livre: "Inteligência Artificial é o campo da ciência da computação voltado para o desenvolvimento de sistemas de hardware e/ou software (geralmente, modelos computacionais) capazes de executar funções tradicionalmente consideradas únicas e exclusivas da cognição humana. Entre essas funções, podemos citar o processamento natural de linguagem e fala, raciocínio especializado e solução de problemas, como diagnóstico e design, visão e aprendizado." TASSO, C. An introduction to artificial intelligence and to the development of knowledge-based systems. *In:* TASSO, Carlo; OLIVEIRA, Edoardo R. Arantes e (orgs.). *Development of knowledge-based systems for engineering*. Vienna: Springer Vienna, 1998. p. 11-26. p. 11. Disponível em: http://link.springer.com/10.1007/978-3-7091-2784-1_2 Acesso em: 23 abr. 2021.

[67] *"Machine learning can be broadly defined as computational methods using experience to improve performance or to make accurate predictions. Here,* experience *refers to the past information available to the learner, which typically takes the form of electronic data collected and made available for analysis. This data could be in the form of digitalized human-labeled training sets, or other types of information obtained via interaction with the environment. In all cases, its quality and size are crucial to the success of the predictions made by the learner."* Tradução livre: "*Machine learning* pode ser amplamente definido como métodos computacionais que utilizam a experiência para melhorar o desempenho ou fazer previsões precisas. Aqui, a *experiência* se refere às informações passadas disponíveis para o aprendiz, que geralmente assumem a forma de dados eletrônicos coletados e disponibilizados para análise. Esses dados podem estar na forma de conjuntos de treinamento digitalizados, classificados manualmente, ou outros tipos de informações obtidas por meio da interação com o ambiente. Em todos os casos, sua qualidade e tamanho são cruciais para o sucesso das previsões feitas pelo aprendiz." MOHRI, M.; ROSTAMIZADEH A.; TALWALKAR A. *Foundations of machine learning*. 2 ed. Cambridge: The MIT Press, 2018. p. 1.

learning[68], além de Redes Neurais Artificiais (RNA)[69], importantes para o desenvolvimento, aprimoramento e, sobretudo, expansão dos usos do reconhecimento facial. Por meio do d*eep learning,* tem-se avançado na solução de grandes problemas da inteligência artificial, mostrando-se acertado em descobrir estruturas complexas em dados de alta dimensão, batendo recordes de aplicação em reconhecimento de imagem - gênero do qual o reconhecimento facial é espécie.[70]

É manifesto que os avanços tecnológicos levam a cenários de resolução de problemas, ao passo que outros surgem. A capacidade de reconhecer imediatamente um indivíduo por meio de suas características faciais, coletando e acessando significativas quantidades de dados - inclusive sensíveis -, remete a preocupações sobre o direito à proteção de dados, bem como, de proteção à privacidade.[71]

O direito à privacidade, contemporaneamente, de forma genérica, pode ser compreendido como um conceito amplo que engloba a proteção à privacidade, à vida privada, à intimidade e a inviolabilidade de dados pessoais.[72] Originalmente, a proteção da privacidade surgiu com o próprio conceito, quando, nos anos 1890, o cenário norte americano de fotografias instantâneas e jornais iniciou uma invasão dos recintos da vida privada e doméstica.[73]

O que tem gerado significativas controvérsias teóricas e jurídicas é a existência de um direito à privacidade em locais públicos. Reflexos dessa celeuma diversas vezes chegaram à Corte Europeia de Direitos Humanos (após longas discussões nos tribunais da Alemanha e da Inglaterra, por exemplo) e também aos tribunais brasileiros. Embora, em uma primeira impressão, não se vislumbra um direito à privacidade em ambientes públicos, o tema merece considerações.

Inicialmente, vale ressaltar que ter direito à privacidade não é o mesmo que ter privacidade; um pode inteiramente existir sem o outro. Por exemplo, quem oculta atividades criminosas possui privacidade, mas não possui o direito à privacidade, ao passo que alguém pode ter direito à privacidade, mas não a possuir, por alguém ter violado tal direito.[74] Em uma sociedade vigiada, proteger o direito à privacidade com vista a garantir a privacidade, é um cenário imbricado.

A proteção à privacidade pode ser observada sob duas condições: a formal e a material. Sob a condição formal, são elencadas as normas legais, constitucionais ou não, que visam a tutela da privacidade. Por outro

---

[68] *"To summarize, deep learning [...] is an approach to AI. Specifically, it is a type of machine learning, a technique that allows computer systems to improve with experience and data. [...] machine learning is the only viable approach to building AI systems that can operate in complicated, real-world environments. Deep learning is a particular kind of machine learning that achieves great power and flexibility by learning to represent the world as a nested hierarchy of concepts and representations, with each concept defined in relation to simpler concepts, and more abstract representations computed in terms of less abstract ones.".* Tradução livre: "Resumindo, o *deep learning* [...] é uma abordagem para a IA. Especificamente, é um tipo de *machine learning*, uma técnica que permite que os sistemas de computador melhorem com experiência e com dados. [...] o aprendizado de máquina é a única abordagem viável para a construção de sistemas de IA que podem operar em ambientes complicados do mundo real. O *deep learning* é um tipo particular de *machine learning* que alcança grande poder e flexibilidade, aprendendo a representar o mundo como uma hierarquia aninhada de conceitos e representações, com cada conceito definido em relação a conceitos mais simples, e representações mais abstratas computadas em termos de menos abstratas uns." GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. *Deep Learning*. Cambridge: MIT Press, 2017. p. 8.

[69] "Redes neurais artificiais são sistemas de computação vagamente inspirados pelas redes neurais biológicas que constituem os cérebros animais. A rede neural em si não é um algoritmo, mas a estrutura de muitos algoritmos diferentes de aprendizado de máquina para trabalhar juntos e processar entradas de dados complexas. Tais sistemas aprendem a executar tarefas considerando exemplos, sem serem programados com regras específicas de tarefas. Por exemplo, no reconhecimento de imagem, as redes neurais podem aprender a identificar imagens que contenham gatos analisando exemplos que tenham sido rotulados manualmente como "gato" ou "não gato" e, em seguida, usar os resultados para identificar gatos em outras imagens. As redes neurais fazem isso sem qualquer conhecimento prévio sobre gatos, por exemplo, que eles têm pele, rabo, bigode e cara de gato. Em vez disso, eles identificam automaticamente as características do material de aprendizagem que processam." FALCÃO, João Vitor Regis *et al.* Redes Neurais Deep Learning com Tensorflow. *RE3C - Revista Eletrônica Científica de Ciência da Computação*, v. 14, n. 1, 2019. Disponível em: http://revistas.unifenas.br/index.php/RE3C/article/view/232. Acesso em: 24 abr. 2021.

[70] LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. *Nature,* [s.l.], v. 521, n. 7553, p. 436-444, maio 2015, p. 436. Springer Science and Business Media LLC. DOI: http://dx.doi.org/10.1038/nature14539. Disponível em: https://www.nature.com/articles/nature14539. Acesso em: 27 mar. 2021.

[71] MILLIGAN, Christopher S. Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal*, v. 9, p. 295-334, 1999. p. 307.

[72] FORTES, Vinícius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Rio de Janeiro: Lumen Juris, 2016. p. 108.

[73] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 192-220, dez. 1890. p. 195. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf Acesso em: 5 abr. 2021.

[74] REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 32.

lado, a condição material expressa a realidade física que impede a invasão da privacidade.[75] Essa última é constantemente enfraquecida pelos avanços tecnológicos, dos quais o reconhecimento facial é exemplo.

Todas as pessoas possuem classificação própria, que, em sua base, é compartilhada por uma mesma sociedade, daquilo que pode ser denominado hierarquias da privacidade. Assim, algumas particularidades da vida da pessoa são compartilhadas, apenas, com a família, outras com amigos próximos, outras com profissionais da saúde e semelhantes e, por fim, outros assuntos compartilhados com o total de estranhos.[76]

Mesmo em lugares públicos, determinados aspectos da vida de um indivíduo não são revelados às demais pessoas que compartilham, com ele, do lugar. Isso porque há um quesito volitivo em escolher o que e quanto da vida da pessoa é que será exposta ao público. O desejo volitivo, portanto, resume-se em um aspecto de concessão de acesso[77] desse próprio indivíduo aos demais.[78]

Outro ponto que fundamenta a existência de um direito à privacidade em lugares públicos é que a exposição escolhida pelo indivíduo se dá justamente em função das condições do lugar no qual a pessoa está exposta. Contudo, a partir do momento em que esse indivíduo passa a ser vigiado, especialmente com coleta de imagens, um público mais amplo pode acessá-lo, inclusive, em momentos posteriores (futuro), sem que o indivíduo tenha conhecimento ou tenha aquiescido com essa exposição consequente[79].[80]

Ainda que não haja um clássico e consubstanciado direito à privacidade em locais públicos, indivíduos possuem uma "razoável expectativa de privacidade"[81], que a sociedade deve reconhecer como legítima.[82] O nó górdio apresenta-se em como essa razoável expectativa de privacidade pode sobreviver a uma sociedade que se torna, crescentemente, em *surveillance*.

Em um período pré-computacional, a proteção da privacidade teve como grande aliado não as normas constitucionais, mas a própria perspectiva prática. Todavia, com a atual possibilidade de reconhecimento facial presente em locais públicos e o acesso a dados pessoais, faz-se intrincada a proteção do anonimato, inclusive em meio a grandes multidões.[83]

As associações entre privacidade e anonimato não são novas, sendo que há teorias que reconhecem o ano-

[75] REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 43.

[76] CALOYANNIDES, M. Society cannot function without privacy. *Ieee Security & Privacy*, v. 1, n. 3, p. 84-86, maio 2003. DOI: http://dx.doi.org/10.1109/msecp.2003.1203230. Disponível em: https://ieeexplore.ieee.org/document/1203230. Acesso em: 20 abr. 2021.

[77] *"By* privacy*, I understand the condition in which other people are deprived of access to either some information about you or some experience of you. For the sake of economy, I will shorten this and say that privacy is the condition in which others are deprived of access to you."*. Tradução livre: "Por privacidade, entendo a condição em que outras pessoas são privadas de acesso a algumas informações sobre você ou de alguma experiência sua. Por uma questão de economia, reduzirei isso e direi que privacidade é a condição na qual os outros estão privados de acesso a você." REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 30.

[78] MOREHAM, N. A. Privacy in public places. *The Cambridge Law Journal*, v. 65, n. 3, p. 606–635, 2006. p. 617-618.

[79] MOREHAM, N. A. Privacy in public places. *The Cambridge Law Journal*, v. 65, n. 3, p. 606–635, 2006. p. 618.

[80] *"[…] it is theoretically sound to say that people can have a reasonable expectation of privacy in a public place: first because people can choose how much or how little of themselves they reveal in public and secondly, because it is always possible to disseminate an image of a person to a much wider audience than the one to which he or she was originally exposed. In other words, it does not follow from the fact that an individual is happy for some aspects of him- or herself to be observed by some members of the public in some contexts, that he or she must be prepared to have all aspects of him- or herself observed by the public at large in any context."* Tradução livre: "[...] é teoricamente correto dizer que as pessoas podem ter uma expectativa razoável de privacidade em um local público: primeiro, porque as pessoas podem escolher quanto ou quão pouco de si mesmas revelam em público e, em segundo lugar, porque sempre é possível disseminar a imagem de uma pessoa para um público muito maior do que aquele a que ela foi originalmente exposta. Em outras palavras, não decorre do fato de que um indivíduo está feliz por alguns aspectos dele serem observados por alguns membros do público em alguns contextos, que ele ou ela deve estar preparado para ter todos os aspectos dele ou ela mesma observados pelo público em geral em qualquer contexto." MOREHAM, N. A. Privacy in public places. *The Cambridge Law Journal*, v. 65, n. 3, p. 606–635, 2006. p. 620.

[81] No original, "*reasonable expectation of privacy*". MOREHAM, N. A. Privacy in public places. *The Cambridge Law Journal*, v. 65, n. 3, p. 606–635, 2006; REIDENBERG, Joel. Privacy in Public. *University of Miami Law Review*, v. 69, p. 141, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2493449 Acesso em: 11 abr. 2021.

[82] REIDENBERG, Joel. Privacy in Public. *University of Miami Law Review*, v. 69, p. 141, 2014. p. 144. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2493449 Acesso em: 11 abr. 2021.

[83] REIDENBERG, Joel. Privacy in Public. *University of Miami Law Review*, v. 69, p. 141, 2014. p. 148-149. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2493449 Acesso em: 11 abr. 2021.

nimato como um dos estados da privacidade.[84] *"The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance."*[85]

Garantir o anonimato significa que o indivíduo pode estar realizando qualquer atividade em público, compartilhando espaços com outras pessoas, tendo plena consciência de que está sendo observado por outros. No entanto, a não ser que se trate de uma pessoa pública, não espera que seja identificado e reconhecido, mantendo um comportamento que não segue todas as normas sociais que seriam desejadas caso fosse reconhecido por quem o observa.[86]

Por sua vez, com o reconhecimento facial em uso, o anonimato entra completamente em xeque, uma vez que essa tecnologia se destina, justamente, a identificar indivíduos. O fato de saber, ou ao menos temer[87], estar sob sistêmica observação em locais públicos tolhe a sensação de relaxamento e liberdade que os indivíduos buscam, especialmente nos locais públicos e abertos, como praças, parques e similares[88].[89]

Os efeitos de uma *surveillance* envolvem, exemplificativamente, a exposição de laços afetivos, abrangidos por uma razoável expectativa de privacidade, ao tolhimento do anonimato dos indivíduos envolvidos. Para além disso, uma sociedade panóptica pode trazer riscos, sendo: perda extrínseca da liberdade, perda intrínseca da liberdade, riscos simbólicos e risco de metamorfose psicopolítica.[90]

O risco da perda extrínseca da liberdade envolve as formas nas quais a perda da privacidade acarreta tornar pessoas vulneráveis a terem seu comportamento moldado. Caracteriza-se por uma pressão social, que se destina a coibir determinados comportamento indesejados, com a promessa de penalização. Ressalta-se que esse mecanismo de coibição, também, é aplicado às manifestações políticas impopulares, que não são ilícitas ou imorais.[91]

O risco da perda intrínseca da liberdade abrange as maneiras pelas quais a negação da privacidade importa diretamente na limitação da liberdade das pessoas, ou seja, consiste que a privacidade não é apenas modo de proteção da liberdade, mas que ela mesma se constitui, de diversas maneiras, na própria liberdade. Ainda, na medida em que, cada vez mais, as ações humanas vão sendo gravadas, por meio de coletas de dados, ocorre uma perda da liberdade individual de agir espontaneamente.[92]

[84] Desse modo, os estados da privacidade são: primeiro, solidão; segundo, intimidade; terceiro, anonimato; quarto e mais sutil, criação de barreiras psicológicas contra invasões indesejadas. WESTIN, A. F. *Privacy and freedom*. New York: Ig Publishing, 1967. p. 54-55.

[85] Tradução livre: "O terceiro estado de privacidade, anonimato, ocorre quando o indivíduo está em locais públicos ou pratica atos públicos, mas ainda procura e encontra-se livre da identificação e da vigilância." WESTIN, A. F. *Privacy and freedom*. New York: Ig Publishing, 1967. p. 55.

[86] WESTIN, A. F. *Privacy and freedom*. New York: Ig Publishing, 1967. p. 55.

[87] Basta tomar como exemplo as webcams dos notebooks em geral. O simples temor de existir uma possibilidade de estar sendo vigiado (nesse caso, tendo a privacidade invadida) provoca a reação de colocar adesivos ou outras maneiras de bloquear a webcam.

[88] WESTIN, A. F. *Privacy and freedom*. New York: Ig Publishing, 1967. p. 55. p. 55.

[89] "Daí decorre o efeito mais importante do Panóptico: induzir no recluso um estado consciente e permanente de visibilidade, que assegura o funcionamento automático do poder. Fazer de maneira a que a vigilância seja permanente nos seus efeitos, ainda que seja descontínua na sua ação; que a perfeição do poder tenda a tornar inútil a atualidade do seu exercício; que este aparelho arquitectónico seja uma máquina de criar e sustentar uma relação de poder independente de quem o exerce; em suma, que os reclusos estejam presos numa situação de poder de que eles próprios são os portadores. Para isso, é simultaneamente de mais e de menos que o prisioneiro seja incessantemente observado por um vigilante: de menos, porque o essencial é que saiba que está a ser vigiado; de mais, porque não precisa efetivamente de ser vigiado. Foi por isso que Bentham formulou o princípio segundo o qual o poder deve ser visível e inverificável. Visível: o recluso terá incessantemente diante de si a alta silhueta da torre central, de onde é espiado. Inverificável: o recluso nunca deve saber se está realmente a ser observado; mas deve ter a certeza de que pode estar sempre a ser vigiado. Para tornar inverificável a presença ou a ausência do vigilante, para que os prisioneiros, na sua cela, não possam ver uma sombra ou uma contraluz, Bentham previu não só persianas nas janelas da sala central de vigilância, mas também, no interior, tabiques que a cortam em ângulo reto e, para passar de uma sala para outra, não portas, mas biombos: é que um mínimo ruído, uma luz entrevista, uma claridade numa reentrância denunciariam a presença do guardião. O Panóptico é uma máquina de dissociar o par ver-ser visto: no anel periférico, os indivíduos são totalmente vistos, sem nunca verem; na torre central, vê-se tudo, sem nunca se ser visto." FOUCAULT, Michel. *Vigiar e Punir*. Lisboa: Almedina, 2013. p. 156.

[90] REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 34.

[91] REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 35.

[92] REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 37-38.

No risco simbólico, compreende-se que, mesmo quando a invasão da privacidade não causa nenhum dano, tal invasão constitui, por si própria, um insulto à dignidade e à soberania individual. São questões sutis, mas que, em uma sociedade em *surveillance*, vão desconstituindo a soberania individual, transportando-a para o exterior do indivíduo.[93]

Por fim, o risco de metamorfose psicopolítica, consequência da perda da autonomia individual, capaz de reduzir a criatividade e a diversidade, tornado pessoas em "homens unidimensionais"[94]. *"Unless people can form their own views, democratic voting becomes mere ratification of conventionality, and individual freedom mere voluntary conformity."*[95] Aqui, proteger a privacidade implica, também, assegurar os mecanismos democráticos e a liberdade de crítica, essenciais à superação de um estado vigilante.

Retomando a concepção da proteção da privacidade sob condições formais e materiais, registre-se que as condições formais nunca podem garantir a privacidade quando as condições materiais para invadir a privacidade estão à disposição. As condições materiais possuem uma espécie de poder que - ainda - não é alcançado pelas condições formais.[96]

A existência de bancos de dados sempre maiores, a capacidade de coleta e processamento de dados a grandes velocidades, aliados ao uso do reconhecimento facial, promovem condições materiais inéditas para a invasão da privacidade. *"One has to be very optimistic indeed about the power of rules, to think that formal guarantees of privacy will protect us."*[97]

Análises profundas sob a utilização do reconhecimento facial nas *smart cities são importantes*, na medida em que se deve atentar em como esses elementos são ferramentas agregadoras da evolução fenomenológica da vigilância em *surveillance*. Também, por essa razão, o crescente emprego de soluções tecnológicas nas *smart cities* devem ser equiponderadas mediante os seus reflexos à privacidade individual, mesmo em lugares públicos.

4 O desenvolvimento de *smart cities* no Brasil e a proteção aos direitos fundamentais de privacidade e proteção de dados pessoais

Por um lado, o uso do reconhecimento facial complica em potenciais violações à privacidade de pessoas, mesmo em lugares públicos. Entretanto, os riscos dessas tecnologias podem se estender à seara intrínseca dos dados pessoais. Isso porque o reconhecimento facial utiliza, em seu processo, características/informações, que são classificadas como dados pessoais. Então, a indagação: quais os parâmetros de uso de dados pessoais por sistemas de reconhecimento facial nas *smart cities* em face do dever de observância dos direitos fundamentais de privacidade e proteção de dados pessoais?

A adoção da China como objeto de análise do fenômeno de utilização de reconhecimento facial nas *smart cities* se dá não apenas em razão da exponencialidade dessas tecnologias nas cidades chinesas, mas também pelos usos singulares e diferentes, que decorrem da própria disseminação das tecnologias. Além disso, o país sedia empresas que são superpotências em relação ao desenvolvimento de tecnologias de reconhecimento fa-

[93] REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 38-40.

[94] *One-dimensional man*, ideia desenvolvida por Herbert Marcuse, no livro de mesmo nome, como crítica a sociedade capitalista, que opera com poder uniformizador do comportamento humano. *"Thus emerges a pattern of one-dimensional thought and behavior in which ideas, aspirations, and objectives that, by their content, transcend the established universe of discourse and action are either repelled or reduced to terms of this universe. They are redefined by the rationality of the given system and of its quantitative extension."* Tradução livre: "Assim, emerge um padrão de pensamento e comportamento unidimensional em que ideias, aspirações e objetivos que, por seu conteúdo, transcendem o universo estabelecido de discurso e ação são repelidos ou reduzidos a termos desse universo. Eles são redefinidos pela racionalidade do sistema fornecido e por sua extensão quantitativa." MARCUSE, Herbert. *One-dimensional man*: studies in the ideology of advanced industrial society. London: Routledge, 2007. p. 14.

[95] Tradução livre: "A menos que as pessoas possam formar seus próprios pontos de vista, o voto democrático se torna mera ratificação da convencionalidade e a liberdade individual, mera conformidade voluntária." REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 42.

[96] REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995. p. 43-44.

[97] Tradução livre: "É preciso ser realmente muito otimista quanto ao poder das regras, para pensar que garantias formais de privacidade nos protegerão." REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995.

cial e inteligência artificial, competindo com o Vale do Silício.[98] Ainda, alguns usos de reconhecimento facial no Brasil são resultado da importação dessas tecnologias da China, o que demonstra a traslado da tecnologia.

O Brasil tem demonstrado, há tempos, interesse nas tecnologias de reconhecimento facial. No âmbito legislativo, o Projeto de Lei n.º 3.372/2004 propôs a instituição de mecanismos de características biométricas para credenciamento e autenticação de usuários, como requisito para permitir alterações de informações em bancos de dados dos setores de pessoal, pagamentos e arrecadação de tributos, da administração pública direta, indireta e fundacional.[99]

Entre outros mecanismos citados diretamente pelo projeto, tem-se o reconhecimento facial, além da impressão digital e o reconhecimento de íris. Apesar de arquivado em 2008, o projeto, que tramitou na Câmara dos Deputados, recebeu aprovação pela Comissão de Trabalho, Administração e Serviço Público (CTASP), além de parecer pela aprovação na Comissão de Ciência e Tecnologia, Comunicação e Informática (CCTCI).[100]

Em 2018, a Câmara dos Deputados recebeu outras duas proposições legislativas, que tramitam simultaneamente, a fim de implementar a utilização de reconhecimento facial no âmbito do sistema penitenciário.[101] O Projeto de Lei n.º 9.736/2018 propõe que a guia de recolhimento do apenado seja complementada, mediante identificação biométrica por reconhecimento facial.[102] Por sua vez, o Projeto de Lei n.º 11.140/2018 estabelece que custodiados, servidores públicos, prestadores de serviços e visitantes deverão realizar identificação biométrica para acesso aos estabelecimentos penais.[103]

Para além do poder legislativo, o Brasil conta, desde 2011, com a utilização de reconhecimento facial, implantado como projeto piloto em Ilhéus, na Bahia, visando coibir fraudes no transporte público. Nada obstante, o uso dessas tecnologias se tornou popular a partir de 2018. Ao todo, já são mais de quarenta e oito implantações, somente pelo poder público, respectivamente nos setores de transporte, segurança pública, controle de fronteiras, educação, além de outras aplicações[104].[105]

Na Bahia[106], a Secretaria de Segurança Pública utiliza sistema de reconhecimento facial, desde 2018.[107] Em 2019, o uso da tecnologia na Micareta de Feira de Santana, capturou o rosto de mais de 1,3 milhão de foliões.[108] Em 2020, o reconhecimento facial no Carnaval

[98] MILLIGAN, Christopher S. Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal*, v. 9, p. 295-334, 1999. p. 319.

[99] KAI-FU LEE. *AI superpowers*: China, Silicon Valley, and the new world order. New York: Houghton Mifflin, 2018.

[100] BRASIL. Câmara dos Deputados. *Projeto de Lei nº 3.372/2004*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=248978. Acesso em: 01 abr. 2021.

[101] Ambos projetos visam alterar a Lei nº 7.210, de 11 de julho de 1984 (Lei de Execução Penal – LEP). O Projeto de Lei nº 9.736/2018 visa acrescentar o "Art. 107-A. As informações constantes da guia de recolhimento serão complementadas pela identificação biométrica por reconhecimento facial, quando o custodiado for recolhido a um estabelecimento penal." BRASIL. Câmara dos Deputados. *Projeto de Lei nº 9.736/2018*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011. Acesso em: 15 abr. 2021. Já o Projeto de Lei nº 11.140/2018 visa inserir o "Art. 109-A. Todos os custodiados, servidores públicos, prestadores de serviços e visitantes deverão ser identificados pelo sistema biométrico para ter acesso aos estabelecimentos penais." BRASIL. Câmara dos Deputados. *Projeto de Lei nº 11.140/2018*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2188455. Acesso em: 18 abr. 2021. Esse último, apesar de não citar expressamente o reconhecimento facial, entende-se ser essa uma técnica que pode ser utilizada.

[102] BRASIL. Câmara dos Deputados. *Projeto de Lei nº 9.736/2018*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011. Acesso em: 15 abr. 2021.

[103] BRASIL. Câmara dos Deputados. *Projeto de Lei nº 11.140/2018*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2188455. Acesso em: 18 abr. 2021.

[104] INSTITUTO IGARAPÉ. *Infográfico reconhecimento facial no Brasil*. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/ Acesso em: 15 mar. 2021.

[105] As implantações concentram-se em quinze estados da federação, além do Distrito Federal, estando presentes em trinta cidades. INSTITUTO IGARAPÉ. *Infográfico reconhecimento facial no Brasil*. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/ Acesso em: 15 mar. 2021.

[106] O reconhecimento facial utilizado no Estado da Bahia é da empresa chinesa Huawei, sediada em Shenzhen, onde, em 14 de maio de 2019, a empresa convidou o governador Rui Costa a apresentar as experiencias citadas, durante o Fórum Smart City. O governador afirmou que: "estamos felizes com o resultado inicial, mas nosso objetivo é avançar e proporcionar mais segurança aos baianos, por isso estamos licitando este serviço para 55 cidades. Também contrataremos softwares para educação e saúde, áreas que considero fundamental o uso da tecnologia para melhorar e ampliar a oferta de serviços à população.". BAHIA. Secretaria de Estado de Segurança Pública. *Bahia apresenta resultado do Reconhecimento Facial na China*. 2019. Disponível em: http://www.ssp.ba.gov.br/2019/05/5695/Bahia-apresenta-resultado-do-Reconhecimento-Facial-na-China.html. Acesso em: 17 mar. 2021.

[107] MARAUX, Alberto. *SSP amplia cobertura do reconhecimento facial no carnaval*. 2020. Disponível em: http://www.ssp.ba.gov.br/modules/noticias/article.php?storyid=7236. Acesso em: 17 abr. 2021.

[108] NASCIMENTO, Silvânia. *Reconhecimento facial resulta nas prisões de 33 pessoas*. 2019. Disponível em: http://www.ssp.ba.gov.br/2019/04/5613/Reconhecimento-Facial-resulta-nas-prisoes-de-33-pessoas.html Acesso em: 17 mar. 2021.

de Salvador permitiu a contagem do número de foliões, chegando a 11,7 milhões.[109] O número aponta a quantidade de pessoas que foram submetidas à tecnologia, não sendo divulgada nenhuma medida de proteção aos dados pessoais coletados e, ainda, sem o claro conhecimento pelos cidadãos.

Em 2019, a Companhia do Metropolitano de São Paulo (METRÔ) realizou processo licitatório (Licitação Pública Internacional n.º 10014557) a fim de conceber sistema de monitoração eletrônica nas linhas de metrô. O detalhamento técnico que acompanha a licitação evidencia o objetivo de implantação de reconhecimento facial de todos os usuários do metrô.[110]

Em decorrência disso, em fevereiro de 2020, ajuizou-se Ação de Produção Antecipada de Provas, a fim de que fossem demonstrados os detalhamentos dos procedimentos de segurança a serem adotados em relação ao banco de dados do sistema.[111] A demanda foi deferida a fim de que a Companhia do Metropolitano de São Paulo (METRÔ) apresentasse documentação hábil a comprovar a segurança do banco de dados utilizado para realizar o reconhecimento facial[112].[113]

A utilização de tecnologias de detecção facial[114] vai

[109] MARAUX, Alberto. *Reconhecimento Facial captura 42 foragidos na folia*. 2020. Disponível em: http://www.ssp.ba.gov.br/2020/02/7296/Reconhecimento-Facial-captura-42-foragidos-no-Carnaval-de-Salvador.html Acesso em: 17 abr. 2021.

[110] SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (1. Vara da Fazenda Pública). *Ação de Produção Antecipada de Provas nº 1006616-14.2020.8.26.0053*. Relator: Juíza Renata Barros Souto Maior Baião, 02 de fevereiro de 2020. Disponível em: https://www.jusbrasil.com.br/processos/252983937/processo-n-1006616-1420208260053-do-tjsp Acesso em: 17 abr. 2021.

[111] SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (1. Vara da Fazenda Pública). *Ação de Produção Antecipada de Provas nº 1006616-14.2020.8.26.0053*. Relator: Juíza Renata Barros Souto Maior Baião, 02 de fevereiro de 2020. Disponível em: https://www.jusbrasil.com.br/processos/252983937/processo-n-1006616-1420208260053-do-tjsp Acesso em: 17 abr. 2021.

[112] SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (1. Vara da Fazenda Pública). *Ação de Produção Antecipada de Provas nº 1006616-14.2020.8.26.0053*. Relator: Juíza Renata Barros Souto Maior Baião, 02 de fevereiro de 2020. Disponível em: https://www.jusbrasil.com.br/processos/252983937/processo-n-1006616-1420208260053-do-tjsp Acesso em: 17 abr. 2021.

[113] A decisão judicial determinou a apresentação da seguinte documentação: "1) Prova documental de confiabilidade e eficiência do sistema de monitoração eletrônica objeto do processo de licitação LPI n.º 10014557, tendo em vista a pretensão de sua aplicação sobre todos os usuários do Metrô; 2) Prova documental sobre análise de impacto de proteção de dados, contendo quais dados serão coletados e tratados, a base legal para essa coleta (art. 7º, LGPD), a finalidade desse tratamento, análise à luz do princípio da minimização e da proporcionalidade, se há dentre os dados que serão coletados algum que seja definido como sensível pela LGPD, o período de retenção dos dados, o grau de risco e finalmente as ações para a mitigação do risco envolvido. Na sua ausência, prova documental com i) descrição do processo de tratamento de dados pessoais que podem gerar riscos aos titulares e que possam impor restrições não previstas em lei aos usuários de serviços públicos, conforme previsto na LGPD e decorrente do sistema normativo protetor dos consumidores e dos usuários de serviços públicos (art. 6º, I e III, do CDC; Art. 5º, inc. IV, CDUSP; art. 7º, V, da Lei Estadual 10.294/1999; ii) medidas e mecanismos voltados a mitigar os riscos identificados; 3) Prova documental sobre o já existente banco de dados a ser utilizado no sistema de monitoração eletrônica, contendo: i) a data de criação do banco de dados; ii) a forma de aquisição do banco de dados (se foi criação própria, comprado, emprestado); iii) quais informações de usuários do metrô compõem esse banco de dados; iv) qual consentimento foi dado, pelos usuários, para uso de suas informações; v) a forma e frequência de atualização de referido banco de dados; vi) quem terá acesso aos dados pessoais coletados e quais serão os graus de privilégios de acesso; 4) Prova documental sobre como o Metrô obterá consentimento de pais ou responsáveis para obtenção, guarda e uso de dados pessoais de crianças e adolescentes, nos termos do Estatuto da Criança e do Adolescente; 5) Prova documental sobre como será observada a anonimização e a guarda dos dados Pessoais; 6) Prova documental sobre análise de impacto financeiro de eventuais falhas e vazamentos na atividade de monitoração eletrônica, considerando como potencialmente afetados todos os usuários do metrô; 7) Prova documental sobre a governança do futuro banco de dados decorrente desta contratação, incluindo detalhamento de seu controlador, critérios de segurança do armazenamento, usos, formas de acesso e mecanismos de controle social da sua utilização com fundamento e base legal nas finalidades indicadas; 8) Prova documental da proposta de compartilhamento da base de dados com outras entidades estatais e/ou privadas e das hipóteses de tratamento antevistas, permitidas e almejadas, uma vez que a pretensa base legal refere-se à segurança pública e a finalidade institucional da entidade licitante não se relaciona a esse objetivo de política pública, também em virtude dos requisitos mínimos previstos no item 6.9.6 no anexo CS983MEXX7XX001 do edital; 9) Atas de reunião dos órgãos e gestão da Ré aprovando as análises de impacto de proteção de dados e de impacto financeiro do sistema de monitoração eletrônica, nos termos exigidos pelos artigos 1º e 9º da Lei 13.303 de 2016. 10) Prova documental do ato administrativo que elucide a motivação pública do procedimento licitatório em questão, sendo considerados os riscos, custos e eventuais benefícios da contratação pretendida." SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (1. Vara da Fazenda Pública). *Ação de Produção Antecipada de Provas nº 1006616-14.2020.8.26.0053*. Relator: Juíza Renata Barros Souto Maior Baião, 02 de fevereiro de 2020. Disponível em: https://www.jusbrasil.com.br/processos/252983937/processo-n-1006616-1420208260053-do-tjsp Acesso em: 17 abr. 2021.

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

além da área de segurança pública. Em abril de 2018, a empresa ViaQuatro (Concessionária da Linha 4 do Metrô de São Paulo S. A.) realizou instalação de portas interativas digitais, em algumas estações do metrô de São Paulo. A tecnologia consiste na implantação de câmeras com sensores capazes de contabilizar a quantidade de pessoas que passam em frente às telas de publicidade. Além da captação da presença humana, há a coleta de dados da face (detecção facial) que, após processados pelo software, interpretam as expressões faciais, classificando-as em quatro tipos de emoções: feliz, insatisfeito, surpreso e neutro.[115] [116]

Mediante análise da estatura da pessoa, o sistema é capaz de classificá-la como criança, jovem ou adulto, além de, a partir do formato do rosto, haver a identificação do gênero da pessoa, em masculino ou feminino.[117] A coleta dos dados biométricos dos usuários não se destina à segurança do metrô, mas à análise da reação destes aos anúncios de publicidade veiculados nos painéis, alimentando preceitos de otimização publicitária. Em razão disso, o Instituto de Defesa do Consumidor (IDEC) ajuizou Ação Civil Pública, com Tutela de Urgência, que foi deferida, determinando-se o desligamento das portas interativas digitais.[118]

Em cada uma das fases do processo de reconhecimento facial, quantidades significativas de dados são coletadas e processadas. Exemplificativamente, a etapa de coleta de dados pode ser realizada em diversas fontes, sendo possível o reconhecimento de pessoas por meio de imagens que são obtidas exclusivamente na internet.[119] O panorama é agravado com a possibilidade de combinação de conjuntos de dados, que podem ser originados de diferentes bases, mas que criam valiosos banco de dados, mesmo que anonimizados.[120]

É preciso registrar, também, que os dados utilizados para o reconhecimento facial são considerados aparentes. Significa dizer que tais dados pessoais podem ser capturados de qualquer pessoa, em público ou em qualquer outro local, sem o consentimento ou, sequer, o conhecimento da pessoa.[121] Diante desse cenário, o anonimato e a autonomia individual são postos em perigo. Ainda, a proteção insuficiente às imagens (dados pessoais) coletadas podem contribuir para a expansão de fenômenos potencialmente lesivos, como os *deepfakes,*[122]

O direito à proteção de dados pessoais e o direito à da privacidade não estão, nesses termos, previstos no âmbito constitucional brasileiro.[123] Apesar disso, uma rá-

115 SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (37. Vara Cível). *Ação Civil Pública nº 1090663-42.2018.8.26.0100*. Relator: Juíza Patrícia Martins Conceição, 30 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/processos/202658044/processo-n-1090663-4220188260100-do-tjsp Acesso em: 17 abr. 2021.

116 Explica o presidente da ViaQuatro, Harald Zwetkoff, que "as portas de plataforma interativas são uma tecnologia inovadora desenvolvida pela ViaQuatro para aprimorar transmissão de informações aos passageiros da Linha 4-Amarela. Essa nova ferramenta na área de comunicação e marketing, com recursos sofisticados, pode colaborar na criação de novas estratégias para públicos específicos, visando mais efetividade na troca de mensagens importantes ou mesmo o incremento em vendas." SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (37. Vara Cível). *Ação Civil Pública nº 1090663-42.2018.8.26.0100*. Relator: Juíza Patrícia Martins Conceição, 30 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/processos/202658044/processo-n-1090663-4220188260100-do-tjsp Acesso em: 17 abr. 2021.

117 SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (37. Vara Cível). *Ação Civil Pública nº 1090663-42.2018.8.26.0100*. Relator: Juíza Patrícia Martins Conceição, 30 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/processos/202658044/processo-n-1090663-4220188260100-do-tjsp Acesso em: 17 abr. 2021.

118 SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (37. Vara Cível). *Ação Civil Pública nº 1090663-42.2018.8.26.0100*. Relator: Juíza Patrícia Martins Conceição, 30 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/processos/202658044/processo-n-1090663-4220188260100-do-tjsp Acesso em: 17 abr. 2021.

119 KINDT, Els J. *Privacy and data protection issues of biometric applications*: a comparative legal analysis. Dordrecht: Springer, 2013. p. 121.

120 CUMBLEY, Richard; CHURCH, Peter. Is "Big Data" creepy? *Computer Law & Security Review*, v. 29, n. 5, p. 601-609, out. 2013. DOI: http://dx.doi.org/10.1016/j.clsr.2013.07.007 Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364913001349. Acesso em: 10 mar. 2021.

121 KINDT, Els J. *Privacy and data protection issues of biometric applications*: a comparative legal analysis. Dordrecht: Springer, 2013. p. 399.

122 *Deepfake* consiste em uma técnica de manipulação de vídeo que permite a substituição da face de uma pessoa em um vídeo por uma face de uma segunda pessoa, mantendo-se as demais características do vídeo original. Para isso, basta que haja uma grande quantidade de imagens de ambas as pessoas. Esses vídeos, conhecidos como *deepfakes*, ganharam popularidade na mídia devido a utilização de rostos de atrizes e políticos famosos, que foram *deepfaked* em vídeos pornográficos. MATSAKIS, Louise. Gfycat uses artificial intelligence to fight deepfakes porn. *Wired,* fev. 2018. Disponível em: https://www.wired.com/story/gfycat-artificial-intelligence-deepfakes/ Acesso em: 17 mar. 2021.

123 Registre-se que, em março de 2019, foi apresentada Proposta de Emenda à Constituição (PEC) n.º 17/2019 no Senado Federal. O projeto original da PEC acrescentava ao artigo 5º o inciso "XII-A – é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais.", bem como, acrescentava ao artigo 22 (competência privativa da União para legislar sobre) o inciso "XXX – proteção e tratamento de dados pessoais.". Na Comissão de Constituição de Justiça (CCJ), a referida PEC recebeu e aprovou a Emenda de Redação n.º 1, a fim de que não fosse incluída a alteração constitucional ao artigo 5º por meio de dispositivo autônomo (inciso XII-A), mas que houvesse o acréscimo do texto

pida exegese do artigo 5º, inciso X[124], torna plenamente plausível tal dedução, também em virtude da adoção de um conceito amplo de privacidade. Para além disso, o inciso XII[125] do mesmo artigo 5º trata da inviolabilidade de dados e do respetivo direito ao sigilo.[126] [127]

Seja por serem extraídos do artigo 5º (inserido no "Título II − Dos Direitos e Garantias Fundamentais", no "Capítulo I − Dos Direitos e Deveres Individuais e Coletivos") da Constituição Federal do Brasil, seja pelo avanço da doutrina nacional, e também internacional, sobre o tema, certo é que tais direitos são considerados direitos fundamentais[128]. Concernente à privacidade, "o ordenamento jurídico brasileiro contempla a proteção da pessoa humana como seu valor máximo e a privacidade como um direito fundamental".[129] No que diz respeito aos dados pessoais,

> [...] o direito à proteção de dados não deve ser considerado subordinado a nenhum outro direito. Significa que devemos ir além de uma simples análise balanceada de fatores, porque a própria proteção de dados é um 'direito fundamental.[130]

Do mesmo modo, o Supremo Tribunal Federal, no julgamento conjunto[131] de Referendo em Medida Cautelar nas Ações Diretas de Inconstitucionalidade (ADIs) n.º 6.387, n.º 6.388, n.º 6.389, n.º 6.390 e n.º 6.393, ratificou o entendimento de que a proteção de dados pessoas e a privacidade encontra-se sob os auspícios dos direitos fundamentais.[132] Nesse sentido, observa-se uma

ao inciso "XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.". A PEC, aprovada unanimemente nos dois turnos no Senado Federal, foi encaminhada à Câmara dos Deputados, por meio do Ofício n.º 521, de 03 de julho de 2019. BRASIL. Senado Federal. *Proposta de Emenda à Constituição nº* 17/2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso em: 18 abr. 2021. Na Câmara dos Deputados, a PEC 17/2019 foi recebida com parecer de admissibilidade pela CCJ e, após constituída Comissão Especial para análise da proposta, a mesma foi aprovada, com alteração substancial do texto. Ao artigo 5º, acrescenta-se o inciso "LXXIX – é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais;"; ao artigo 21 (competência da União), acrescenta-se o inciso "XXVI – organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei, que disporá sobre a criação de um órgão regulador e outros aspectos institucionais."; ao artigo 22, acrescenta-se o inciso "XXX – proteção e tratamento de dados pessoais.", mantendo-se, nesse item, a redação original da PEC proposta no Senado Federal. Além disso, a PEC traz um artigo 4º, dispondo que "para os efeitos do inciso XXVI do art. 21, na redação dada pelo art. 2º desta Emenda, o órgão regulador será entidade independente, integrante da administração pública federal indireta, submetida a regime autárquico especial.". A PEC aguarda deliberação pelo Plenário da Câmara dos Deputados. BRASIL. Câmara dos Deputados *Proposta de Emenda à Constituição nº 17/2019*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 18 abr. 2021.

[124] Art. 5º: "X − são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;". BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 abr. 2021.

[125] Art. 5º: "XII − é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;". BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 abr. 2021.

[126] BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 abr. 2021.

[127] Ainda, o artigo 5º, em seu parágrafo §2º, é expresso ao estabelecer que "os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.". BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 abr. 2021.

[128] "Direitos fundamentais são direitos público-subjetivos de pessoas (físicas ou jurídicas), contidos em dispositivos constitucionais e, portanto, que encerram caráter normativo supremo dentro do Estado, tendo como finalidade limitar o exercício do poder estatal em face da liberdade individual." DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 41.

[129] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 27-28.

[130] RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 18.

[131] Todas as ações possuem como objeto de impugnação o inteiro teor da Medida Provisória n.º 954/2020, que "dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei n.º 13.979, de 6 de fevereiro de 2020." BRASIL. Presidência da República. *Medida Provisória nº 954/2020*. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 18 abr. 2021. Na ocasião, entendeu o Supremo Tribunal Federal pela suspensão da eficácia do referido ato normativo. BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade.** *ADI nº 6.387/DF*. Medida cautelar em ação direta de inconstitucionalidade [...]. Relatora: Min. Rosa Weber, 07 de maio de 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165 Acesso em: 18 abr. 2021.

[132] BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Di-**

mudança de paradigma, evoluindo-se de um cenário de simples proibição de intervenção, para uma premissa de proteção positiva desses direitos fundamentais.

Os direitos fundamentais não se revestem de absolutismo, havendo situações que é possível, legitimamente, limitar o exercício dos direitos fundamentais. Nesse sentido, o Estado pode intervir (intervenção estatal), limitando o exercício de um direito fundamental, em detrimento de um interesse estatal ou para impor um interesse difuso coletivo não individualizável, também conhecido como transindividual.[133] [134]

Desse modo, a área de proteção[135] de um direito fundamental pode ser invadida por uma intervenção estatal, assim considerada como aquela que engloba

> [...] praticamente toda e qualquer ação ou omissão estatal com um mínimo de relevância em face do direito fundamental que é o parâmetro constitucional utilizado para o exame da intervenção (intervenção estatal "em sentido amplo").[136]

Na seara das intervenções estatais, tem-se as consideradas intervenções permitidas, que ocorrem quando há "justificação constitucional da intervenção na área de proteção de direito fundamental".[137] Uma dessas intervenções justificadas ocorre quando há a colisão entre um direito fundamental individual e um princípio de interesse geral, sendo, inclusive, hipótese de uma intervenção administrativa.[138]

Considerando-se o presente caso em estudo, está-se a analisar se o uso do reconhecimento facial para o contexto das *smart cities* configura-se como uma intervenção estatal justificada aos direitos fundamentais de privacidade e proteção de dados pessoais. Para isso, anote-se que a possibilidade de limitar o exercício de um direito fundamental, mesmo que por meio de uma intervenção justificada, não é ilimitada, havendo balizas a serem observadas. "Isso indica que é proibido proibir o exercício do direito fundamental além do necessário, conforme ensina a doutrina dos *limites dos limites* (*Schranken-Schranken*) elaborada no direito constitucional alemão".[139] [140]

Os limites aos limites dos direitos fundamentais exercem a função de limitar a restrição aos direitos fundamentais. Operam, assim, como barreiras aos processos de restringibilidade, a fim de garantir a máxima eficácia desses direitos. Em decorrência disso, sob a lógica do controle material desses limites, busca-se proteger o núcleo essencial dos direitos fundamentais, também chamado de conteúdo essencial.[141]

reta de Inconstitucionalidade. *ADI nº 6.387/DF*. Medida cautelar em ação direta de inconstitucionalidade [...]. Relatora: Min. Rosa Weber, 07 de maio de 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165 Acesso em: 18 abr. 2021.

133 DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 141.

134 "De forma esquemática, a dogmática dos direitos fundamentais tem como início e como ponto de chegada o choque de interesses causado pela concretização de direitos fundamentais. Inicia com a constatação de um choque de interesses entre titulares de direitos fundamentais, ou entre um titular e interesses gerais que constitucionalmente têm o condão de limitá-los, e dá uma resposta final ao conflito indicando aquilo que cada envolvido pode ou não pode fazer.". DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 143.

135 É necessário distinguir os conceitos de área de regulamentação e área de proteção de um direito fundamental. A área de regulamentação "[...] refere-se ao *tema* tratado pelo constituinte. Como esse tema mereceu a atenção do constituinte, dizemos genericamente que ele o regulamentou. Tratou dele com uma norma definidora de direito fundamental, razão pela qual o verbo "regulamentar" nesse contexto não é idêntico à regulamentação infraconstitucional ou muitas vezes infralegal de um direito comum com vistas à sua aplicabilidade ou viabilização de exercício." DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 134. Por sua vez, "a área de proteção será menor que a área de regulamentação toda vez que o constituinte retirou daquele recorte da realidade social no qual incide a norma (área de regulamentação) um comportamento ou situação não contemplados pela norma. Dito de outra forma: o constituinte recorta de todos os comportamentos e situações tematizados pela norma de direito fundamental somente aqueles que pretende proteger. Em muitos casos isso não ocorre, havendo equivalência entre os dois círculos que representam a área de regulamentação e a área de proteção. Nos demais casos, a área de proteção de cada direito é resultado da subtração da área de regulamentação daqueles casos e situações que a Constituição não protegeu." DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 135-136.

136 DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 145.

137 DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 148.

138 DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 150.

139 DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 167.

140 "Na Alemanha, o art. 19, II, GG, traz uma limitação formal que é de difícil concretização e deu azo a teorias particularmente problemáticas. Segundo esse dispositivo, "em caso algum pode um direito fundamental ser atingido em seu conteúdo essencial". O *conteúdo essencial* funciona como limite, isto é, como "obstáculo" de determinadas restrições aos direitos fundamentais (na terminologia alemã: "óbice do conteúdo essencial" – *Wesensgehaltssperre*)." DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 168.

141 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 6. ed. São Paulo: Saraiva, 2017. p. 408-409.

Mesmo onde as constituições não introduziram, expressamente, a ideia de um conteúdo essencial dos direitos fundamentais - como é o caso do Brasil -, entende-se que há um núcleo que deve ser protegido, evitando-se que os direitos fundamentais se esvaziem de conteúdo.[142] Entretanto, com o intuito de compreender o que compõe esse conteúdo essencial, surgem duas teorias: a absoluta, com a defesa de um núcleo duro; e a relativa, com a defesa de um núcleo flexível dos direitos fundamentais.[143] [144]

Para a teoria absoluta, o núcleo duro é abstratamente fixado e irrestringível, de modo que "[...] o núcleo essencial é uma posição subjetiva de tal modo indisponível que não pode ser relativizada por qualquer direito ou interesse contraposto.".[145] Por sua vez, para a teoria relativa

> [...] o núcleo essencial é o resultado de um processo de ponderação, constituindo aquela parte do direito fundamental que, em face de outros direitos ou bens constitucionalmente protegidos e com ele colidentes, acaba por ser julgada prevalecente e consequentemente subtraída à disposição do legislador.[146] [147]

A doutrina apresenta divergências em relação ao tema. Nada obstante, há unanimidade ao afirmar a existência de um núcleo essencial, e que a proteção a esse núcleo instransponível é elemento indeclinável dos direitos fundamentais.[148] E é nesse sentido que, na legislação infraconstitucional, a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n.º 13.709, de 14 de agosto de 2018 – disciplina a matéria. Tanto assim o é, que o artigo 1º, tem como objetivo, justamente, "[...] proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.".[149]

No que tange aos fundamentos da proteção de dados pessoais, pode-se extrair do referido diploma legal, como pertinentes ao tema do reconhecimento facial, "o respeito à privacidade" (artigo 2º, inciso I), "a inviolabilidade da intimidade, da honra e da imagem" (artigo 2º, inciso IV), "o desenvolvimento econômico e tecnológico e a inovação" (artigo 2º, inciso V) e "os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais" (artigo 2º, inciso VII).[150]

---

142 BARCELLOS, Ana Paula de. *Ponderação, racionalidade e atividade jurisdicional*. Rio de Janeiro: Renovar, 2005. p. 139-140.

143 BARCELLOS, Ana Paula de. *Ponderação, racionalidade e atividade jurisdicional*. Rio de Janeiro: Renovar, 2005. p.142-143.

144 As teorias também são abordadas por DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014. p. 168; CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. 7. ed. Coimbra: Almedina, 2003. p. 459-461. Como pressupõe a coerência, adota-se a teoria relativa do núcleo essencial dos direitos fundamentais.

145 CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. 7. ed. Coimbra: Almedina, 2003. p. 460.

146 CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. 7. ed. Coimbra: Almedina, 2003. p. 460.

147 A controvérsia da doutrina também se estende na medida que examina o significado do princípio da proteção do núcleo, ou seja, em relação ao objeto de proteção do núcleo essencial dos direitos fundamentais. "Existem aqui duas teorias em confronto. A *teoria objectiva* considera dever referir-se a proteção do núcleo essencial ao direito fundamental como norma objectiva e não como direito subjectivo individual. Por outras palavras: o objecto de protecção do preceito é a garantia geral e abstracta prevista na norma e não a posição jurídica concreta do particular. A *teoria subjectiva* toma como 'referente' a proteção do núcleo essencial do direito fundamental na sua dimensão de direito subjetivo do indivíduo. De acordo com a primeira teoria, visa-se assegurar a eficácia de um direito fundamental na sua globalidade; de acordo com a segunda, pretende-se afirmar que, em caso algum, pode ser sacrificado o direito subjetivo de uma pessoa, a ponto de, para ele, esse direito deixar de ter qualquer significado.". CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. 7. ed. Coimbra: Almedina, 2003. p. 459.

148 E essa é, também, a posição do Supremo Tribunal Federal. Quando do julgamento do *Habeas Corpus* 82.424-RS, conhecido como Caso Ellwanger, o Ministro Celso de Mello registrou que "[...] a superação dos antagonismos existentes entre princípios constitucionais há de resultar da utilização, pelo Supremo Tribunal Federal, de critérios que lhe permitam ponderar e avaliar, *'hic et nunc'*, em função de determinado contexto e sob uma perspectiva axiológica concreta, qual deva ser o direito a preponderar no caso, considerada a situação de conflito ocorrente, desde que, no entanto, a utilização do método da ponderação de bens e interesses não importe em esvaziamento do conteúdo essencial dos direitos fundamentais, tal como adverte o magistério da doutrina.". BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Habeas Corpus. *HC nº 82.424/RS*. Habeas-corpus. Publicação de livros: anti-semitismo [...]. Relator: Min. Moreira Alves, 17 de setembro de 2003. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=2052452 Acesso em: 18 abr. 2021. Além desse julgamento emblemático, o tema do conteúdo essencial dos direitos fundamentais na jurisprudência do Supremo Tribunal Federal pode ser encontrado nos julgamentos do Inquérito 1.957, Mandado de Segurança 24.369, *Habeas Corpus* 84.862, *Habeas Corpus* 82.959, *Habeas Corpus* 85.867, Mandado de Segurança 24.045, Recurso Extraordinário 427.339 e Recurso Extraordinário 431.121.

149 BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 abr. 2021.

150 BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 abr. 2021.

A Lei Geral de Proteção de Dados Pessoais apresenta, também, o conceito de dado pessoal, sendo a "informação relacionada a pessoa natural identificada ou identificável".[151] Para além disso, a lei cria uma subcategoria, os dados pessoais sensíveis, assim denominados por apresentarem um grau superior de importância ao indivíduo, sendo, desse modo, merecedores de proteção especial. De acordo com a lei, trata-se de

> Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.[152]

Legalmente, dado biométrico é considerado dado pessoal, e ainda, de natureza sensível. No entanto, a lei é silente quanto ao que compõe um dado biométrico. Por isso a literatura especializada, que define dados biométricos como aqueles que

> *[...] (a) are based on the unique or distinctive biological and/or behavioral characteristics of human beings, (b) are processed in whole or in part by automated means, and (c) allow specific use of these characteristics, in particular identification or verification of the identity or of a claim.*[153]

Sob tal proteção legal, os processos de reconhecimento facial constituem-se potencialmente lesivos aos direitos fundamentais de privacidade e proteção de dados pessoais dos indivíduos a eles submetidos. Tais direitos fundamentais, envoltos no princípio (amplo) de proteção à privacidade, contraporem-se ao princípio da supremacia do interesse público, em que se encontram os preceitos de garantia da segurança pública[154] e do interesse geral. Nesse sentido, a fim de apontar possíveis elucidações a esse imbróglio, utiliza-se da proporcionalidade.[155]

O emprego da proporcionalidade envolve a aplicação das regras de adequação, necessidade e proporcionalidade em sentido estrito, nessa sequência. Concisamente, a regra da adequação impõe a análise do meio empregado e sua contribuição para alcançar o objetivo almejado. Por sua vez, a regra da necessidade objetiva verificar a gravidade do meio empregado em relação ao objetivo perquirido. Por fim, a proporcionalidade, em sentido estrito, consiste na ponderação recíproca entre os bens envolvidos, ou seja, tanto os que justificam os limites, quando os que são afetados por eles.[156] [157]

Indissociáveis, portanto, os conceitos de conteúdo essencial[158] e proporcionalidade, na medida em que as "restrições a direitos fundamentais que passam no teste da proporcionalidade não afetam o conteúdo essen-

---

[151] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 abr. 2021.

[152] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 abr. 2021.

[153] Tradução livre: "[...] (a) se baseiam nas características biológicas e/ou comportamentais únicas ou distintivas dos seres humanos; (b) são processados total ou parcialmente por meios automatizados; e (c) permitem o uso específico dessas características, em particular identificação ou verificação da identidade ou de uma reivindicação." KINDT, Els J. *Privacy and data protection issues of biometric applications*: a comparative legal analysis. Dordrecht: Springer, 2013. p. 148.

[154] O artigo 4º, inciso III, alínea a, da Lei Geral de Proteção de Dados Pessoais excepciona sua aplicação no tratamento de dados pessoais para, entre outros, fins exclusivos de segurança pública. "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] III − realizado para fins exclusivos de: a) segurança pública." Nada obstante, estabelece o §1º do mesmo artigo que "o tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei." BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 abr. 2021.

[155] Registre-se, por necessário, que o presente estudo não visa esgotar matéria da proporcionalidade alexyana, nem o desenvolvimento da fórmula elaborada pelo autor, e tampouco adentrar na discussão da aplicação da teoria pelos tribunais brasileiros. Objetiva-se, apenas, destacar a aplicação da teoria aos princípios suscitados, demonstrando-se a comprovação dos resultados, quando aplicada a proporcionalidade.

[156] ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros, 2008. p. 116-120.

[157] Nesse sentido, a máxima da proporcionalidade em sentido estrito, de que "quanto maior for o grau de não-satisfação ou de afetação de um princípio, tanto maior terá que ser a importância da satisfação do outro.". ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros, 2008. p. 593.

[158] "[...] o objeto de análise, 'o conteúdo essencial dos direitos fundamentais', deve ser encarado como um fenômeno complexo, que envolve uma série de problemas interrelacionados. Esses problemas, que são, na sua complexidade, o objeto da tese, já foram analisados até aqui e são, sobretudo, aqueles ligados: (a) à análise daquilo que é protegido pelas normas de direitos fundamentais; (b) à relação entre o que é protegido e suas possíveis restrições; e (c) a como fundamentar tanto o que é protegido como as suas restrições. O que se disse anteriormente pode e deve ser retomado aqui: é da relação dessas variáveis - e de todos os problemas que as cercam - que se define, na visão do trabalho que aqui se resume, o conteúdo essencial dos direitos fundamentais.". SILVA, Luís Virgílio Afonso da. O conteúdo essencial dos direitos fundamentais e a eficácia das normas constitucionais. *RDE: Revista de Direito do Estado*, Rio de Janeiro, v. 1, n. 4, p. 23-51, 2006. p. 41.

cial dos direitos restringidos.".[159] Ademais, importante destacar a adequação e a necessidade como situação de análise das possibilidades fáticas, enquanto a proporcionalidade em sentido estrito coteja as possibilidades jurídicas.[160]

Parte-se à regra de adequação. O uso do reconhecimento facial para monitoramento, pode ser considerado como meio adequado para satisfazer interesses de segurança pública. É certo que, no monitoramento, a possibilidade de identificar grandes quantidades de pessoas em questões de segundos, contribui para a apuração de fatos nocivos às pessoas e à coletividade. Todavia, no mencionado caso das portas interativas digitais, a adequação se mostra menos evidente, na medida em que a finalidade do emprego da detecção facial não é expressamente demonstrada.

No tocante à necessidade, o seu exame denota que a utilização do reconhecimento facial pode ser substituída por técnicas menos danosas. Isso porque, conforme mencionado, o reconhecimento facial acarreta a coleta de grandes quantidades de dados pessoais (biométricos), classificados como sensíveis. Todavia, o uso de outras técnicas, como a identificação por impressão digital e escaneamento de íris, podem ser utilizadas - para utilizar um exemplo aqui mencionado - em casos de identificação de pessoas para acesso a estabelecimentos penitenciários, de modo menos gravoso, eis que quantidades substancialmente menores de dados pessoais são coletadas.

Por fim, a proporcionalidade em sentido estrito. Considerando-se o princípio de proteção à privacidade, verifica-se que o emprego do reconhecimento facial afeta, profundamente, esse princípio, na medida que há coleta de dados pessoas sensíveis e ocorre a perturbação da autonomia e do anonimato, mesmo em locais públicos. Por outro lado, os preceitos de segurança nacional e interesse geral, abarcados no princípio da supremacia do interesse público, podem ser satisfeitos por medidas outras. O reconhecimento facial, portanto, não se caracteriza como técnica imprescindível para garantir a segurança pública, tampouco do interesse geral.

A proteção aos direitos fundamentais de privacidade e proteção de dados pessoais, mediante a limitação do uso do reconhecimento facial, não impede a realização, por parte do poder público, de garantir a segurança pública. Com relação ao caso das portas interativas digitais do metrô de São Paulo, é latente que a proteção a esses direitos fundamentais não limita, ou sequer impede, a difusão publicitária. Daí porque rememorar paradigma da *surveillance*, ao passo que se encontra rotineiramente incrustada em situações sutis na vida de todos os dias.

Considerando-se a potencial violação a direitos fundamentais, as justificativas para uso dessas tecnologias para os casos chineses apresentados - a rememorar o uso do reconhecimento facial para identificar uigures e nos banheiros públicos de Pequim - parecem não subsistir. A utilização dessa tecnologia, como explicitado, importa em infringir o princípio de proteção à privacidade, fomentando processos de *surveillance*. A adoção, portanto, do modelo de *smart cities* em vigor na China não é recepcionada pela ordem jurídico-constitucional brasileira, de modo que sua utilização não é dissociada de violações aos direitos e garantias fundamentais de privacidade e de proteção de dados pessoais.

5 Considerações finais

Os impactos das tecnologias de reconhecimento facial são os limites analíticos do estudo desenvolvido. Assim, destaca-se que uma gama de outras tecnologias empregadas pelas *smart cities*, como geolocalização, *data minig* e *IoT*, também são potencialmente transgressoras a direitos e garantias fundamentais, inclusive para além daqueles aqui referidos.

Os objetivos geral e específicos são alcançados, na medida em que as situações de uso de reconhecimento artificial na *smart cities* chinesas - apresentados no capítulo primeiro - são substanciosas para a compreensão de dois aspectos: de um lado, que a evolução do modelo de *smart cities* na China torna-se o horizonte a partir do qual há uma incipiente circulação desse modelo de *smart cities* para o ocidente, incluindo o Brasil; por outro, que utilizar do reconhecimento facial para solver problemáticas é uma aposta dúbia, na medida que essas próprias tecnologias compõem o núcleo da *surveillance* - e que esta possui consequências ainda não compreendidas, dada sua permanente transformação.

[159] SILVA, Luís Virgílio Afonso da. O conteúdo essencial dos direitos fundamentais e a eficácia das normas constitucionais. *RDE: Revista de Direito do Estado*, Rio de Janeiro, v. 1, n. 4, p. 23-51, 2006. p. 43.
[160] ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros, 2008. p. 118.

O capítulo segundo, ao apresentar e descrever tecnicamente os processos de reconhecimento facial, apontam para a capacidade dessa tecnologia em coletar dados pessoais e, em tratando-os, utilizá-los para além da verificação e identificação de pessoas. Outrossim, denota a potencialidade de interferência da liberdade individual, como consequência de inviabilizar o anonimato e a autonomia dos indivíduos e, além disso, em como a privacidade é fragilizada diante das tecnologias de reconhecimento facial.

O capítulo terceiro aponta o interesse do Brasil para adoção do modelo chinês de *smart cities*, especificamente que tange ao uso do reconhecimento facial na segurança pública e para além dela. No entanto, considerando-se que o ordenamento jurídico-constitucional brasileiro assegura a privacidade e a proteção aos dados pessoais sob o prisma de direitos fundamentais, há uma não recepção de tal modelo. Em razão disso, o problema de pesquisa apresentado mostra-se atendido.

Apesar de a supremacia do interesse geral ser princípio legítimo norteador da atividade estatal, e que, ordinariamente, se sobrepõe aos interesses individuais, a limitação aos direitos individuais, especialmente aos de índole fundamental, não pode ser irrestrita, sob pena de sua anulação. Por isso os direitos fundamentais de privacidade e a proteção de dados pessoais, encontrados no princípio da privacidade, devem operar como limites à *surveillance*, e não serem, por ela, esvaziados.

Referências

ALEXY, Robert. *Teoria dos direitos fundamentais*. São Paulo: Malheiros, 2008.

AMAZON. *We are implementing a one-year moratorium on police use of Rekognition*. 2020. Disponível em: https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition Acesso em: 10 mar. 2021.

AMY QIN. Chinese city uses facial recognition to shame pajama wearers. *The New York Times*, jan. 2020. Disponível em: https://www.nytimes.com/2020/01/21/business/china-pajamas-facial-recognition.html?searchResultPosition=13 Acesso em: 11 abr. 2021.

ARENDT, Hannah. *Origens do totalitarismo*. São Paulo: Companhia das Letras, 1989.

BAHIA. Secretaria de Estado de Segurança Pública. *Bahia apresenta resultado do Reconhecimento Facial na China*. 2019. Disponível em: http://www.ssp.ba.gov.br/2019/05/5695/Bahia-apresenta-resultado-do-Reconhecimento-Facial-na-China.html. Acesso em: 17 mar. 2021.

BARCELLOS, Ana Paula de. *Ponderação, racionalidade e atividade jurisdicional*. Rio de Janeiro: Renovar, 2005.

BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In: ENCYCLOPEDIA of Electrical and Electronics Engineering*. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257 Acesso em: 13 abr. 2021.

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

BOTSMAN, Rachel. Big data meets Big Brother as China moves to rate its citizens. *Wired,* 2017. Disponível em: https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion. Acesso em: 29 mar. 2021.

BOWYER, Kevin W.; CHANG, Kyong; FLYNN, Patrick. A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition. *Computer Vision and Image Understanding*, v. 101, n. 1, p. 1-15, jan. 2006. Disponível em: https://www.sciencedirect.com/science/article/pii/S1077314205000822 Acesso em: 14 abr. 2021.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 abr. 2021.

BRASIL. Câmara dos Deputados *Proposta de Emenda à Constituição nº 17/2019*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 18 abr. 2021.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 11.140/2018*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2188455. Acesso em: 18 abr. 2021.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 3.372/2004*. Disponível em: https://www.camara.leg.

br/proposicoesWeb/fichadetramitacao?idProposicao=248978. Acesso em: 01 abr. 2021.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 9.736/2018*. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011. Acesso em: 15 abr. 2021.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 abr. 2021.

BRASIL. Presidência da República. *Medida Provisória nº 954/2020*. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 18 abr. 2021.

BRASIL. Senado Federal. *Proposta de Emenda à Constituição nº* **17/2019.** Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594 Acesso em: 18 abr. 2021.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade.** *ADI nº 6.387/DF*. Medida cautelar em ação direta de inconstitucionalidade [...]. Relatora: Min. Rosa Weber, 07 de maio de 2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165 Acesso em: 18 abr. 2021.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Habeas Corpus. *HC nº 82.424/RS*. Habeas-corpus. Publicação de livros: anti-semitismo [...]. Relator: Min. Moreira Alves, 17 de setembro de 2003. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=2052452 Acesso em: 18 abr. 2021.

BUCKLEY, Chirs; MOZUR, Paul; RAMZY, Austin. How China turned a city into a prision: a surveillance state reaches new Heights. *The New York Times*, 04 abr. 2019. Disponível em: https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html. Acesso em: 01 abr. 2021.

BUCKLEY, Chirs; MYERS, Steven Lee. Battered but resilient after China's Crackdown. The New York Times, 18 jan. 2020. Disponível em: https://www.nytimes.com/2020/01/18/world/asia/china-uighurs-xinjiang-yarkand.html. Acesso em: 01 abr. 2021.

CALOYANNIDES, M. Society cannot function without privacy. *Ieee Security & Privacy*, v. 1, n. 3, p. 84-86, maio 2003. DOI: http://dx.doi.org/10.1109/msecp.2003.1203230. Disponível em: https://ieeexplore.ieee.org/document/1203230. Acesso em: 20 abr. 2021.

CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da constituição*. 7. ed. Coimbra: Almedina, 2003.

CREEMERS, Rogier. China's Social Credit System: an evolving practice of control. *Ssrn Electronic Journal*, p. 1-32, maio 2018. DOI: http://dx.doi.org/10.2139/ssrn.3175792 Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3175792 Acesso em: 15 mar. 2021.

CUMBLEY, Richard; CHURCH, Peter. Is "Big Data" creepy? *Computer Law & Security Review*, v. 29, n. 5, p. 601-609, out. 2013. DOI: http://dx.doi.org/10.1016/j.clsr.2013.07.007 Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0267364913001349. Acesso em: 10 mar. 2021.

DIMOULIS, Dimitris; MARTINS, Leonardo. *Teoria geral dos direitos fundamentais*. 5. ed. São Paulo: Atlas, 2014.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

DONG-HEE SHIN. Ubiquitous city: urban technologies, urban infrastructure and urban informatics. *Journal of Information Science*, v. 35, n. 5, p. 515-526, set. 2009. DOI: http://dx.doi.org/10.1177/0165551509100832 Disponível em: https://journals.sagepub.com/doi/10.1177/0165551509100832 Acesso em: 27 mar. 2021.

DUDLEY, Lauren. China's Ubiquitous Facial Recognition Tech Sparks: Privacy Backlash Privacy concerns remain largely unaddressed in proposed Chinese facial recognition standards. *The Diplomat*, mar. 2020. Disponível em: https://thediplomat.com/2020/03/chinas-ubiquitous-facial-recognition-tech-sparks-privacy-backlash/ Acesso em: 01 abr. 2021.

FALCÃO, João Vitor Regis *et al*. Redes Neurais Deep Learning com Tensorflow. *RE3C - Revista Eletrônica Científica de Ciência da Computação*, v. 14, n. 1, 2019. Disponível em: http://revistas.unifenas.br/index.php/RE3C/article/view/232. Acesso em: 24 abr. 2021.

FORTES, Vinícius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet*. Rio de Janeiro: Lumen Juris, 2016.

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

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. *Deep Learning*. Cambridge: MIT Press, 2017.

HIRANAND, Ravi. Jaywalk in Shenzhen get fined on WeChat: Shenzhen's jaywalkers get scolded on WeChat and shamed on public screens. *Abacus,* mar. 2018. Disponível em: https://www.abacusnews.com/future-tech/shenzhens-jaywalkers-get-scolded-wechat-and-shamed-public-screens/article/2138928 Acesso em: 01 abr. 2021.

HONG XU; XUEXIAN GENG. People-centric service intelligence for smart cities. *Smart Cities*, v. 2, n. 2, p.135-152, abr. 2019. DOI: http://dx.doi.org/10.3390/smartcities2020010 Disponível em: https://www.mdpi.com/2624-6511/2/2/10/xml Acesso em: 15 mar. 2021.

HU, Richard. Planning for economic development. *In:* HEIN, Carola. *The Routledge Handbook of Planning History*. London; New York: Routledge, 2017. p. 313-324.

HU, Richard. The state of smart cities in China: the case of Shenzhen. *Energies*, v. 12, n. 22, p.4375-4393, nov. 2019. DOI: http://dx.doi.org/10.3390/en12224375 Disponível em: https://www.mdpi.com/1996-1073/12/22/4375 Acesso em: 29 mar. 2021.

INSTITUTO IGARAPÉ. *Infográfico reconhecimento facial no Brasil*. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/ Acesso em: 15 mar. 2021.

JANE LI. China's facial-recognition giant says it can crack masked faces during the coronavirus. *Quartz,* fev. 2020. Disponível em: https://qz.com/1803737/chinas-facial-recognition-tech-can-crack-masked-faces-amid-coronavirus/ Acesso em: 01 abr. 2021.

KAI-FU LEE. *AI superpowers*: China, Silicon Valley, and the new world order. New York: Houghton Mifflin, 2018.

KINDT, Els J. *Privacy and data protection issues of biometric applications*: a comparative legal analysis. Dordrecht: Springer, 2013.

KOSTOFF, Ronald N.; BOYLAN, Robert; SIMONS, Gene R. Disruptive technology roadmaps. *Technological Forecasting and Social Change*, v. 71, n. 1-2, p. 141-159, jan. 2004. DOI: http://dx.doi.org/10.1016/s0040-1625(03)00048-9 Disponível em: https://www.sciencedirect.com/journal/technological-forecasting-and-social-change/vol/71/issue/1 Acesso em: 15 abr. 2021.

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

LECUN, Yann; BENGIO, Yoshua; HINTON, Geoffrey. Deep learning. *Nature,* v. 521, n. 7553, p. 436-444, maio 2015. DOI: http://dx.doi.org/10.1038/nature14539 Disponível em: https://www.nature.com/articles/nature14539 Acesso em: 27 mar. 2021.

LIANG, Fan *et al*. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, v. 10, n. 4, p.415-453, ago. 2018. DOI: http://dx.doi.org/10.1002/poi3.183 Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.183 Acesso em: 05 abr. 2021.

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

MA ZHENHUAN. Park alters entry rules following facial recognition tech lawsuit. *China Daily,* nov. 2019. Disponível em: http://global.chinadaily.com.cn/a/201911/07/WS5dc38381a310cf3e35575f3a.html. Acesso em: 01 abr. 2021.

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

MANN, Steve; NOLAN, Jason; WELLMAN, Barry. Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, v. 1, n. 3, p. 331-355, set. 2002. DOI: http://dx.doi.org/10.24908/ss.v1i3.3344 Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3344 Acesso em: 15 abr. 2021.

MARAUX, Alberto. *Reconhecimento Facial captura 42 foragidos na folia*. 2020. Disponível em: http://www.ssp.ba.gov.br/2020/02/7296/Reconhecimento-Facial-captura-42-foragidos-no-Carnaval-de-Salvador.html Acesso em: 17 abr. 2021.

MARAUX, Alberto. *SSP amplia cobertura do reconhecimento facial no carnaval*. 2020. Disponível em: http://www.ssp.ba.gov.br/modules/noticias/article.php?storyid=7236. Acesso em: 17 abr. 2021.

MARCUSE, Herbert. *One-dimensional man*: studies in the ideology of advanced industrial society. London: Routledge, 2007.

MARX, Gary T. What's new about the "new surveillance"?: classifying for change and continuity. *Knowledge, Technology & Policy*, v. 17, n. 1, p. 18-37, mar. 2004. DOI: http://dx.doi.org/10.1007/bf02687074 Disponível em: https://link.springer.com/article/10.1007/BF02687074 Acesso em: 15 abr. 2021.

MATSAKIS, Louise. Gfycat uses artificial intelligence to fight deepfakes porn. *Wired,* fev. 2018. Disponível em: https://www.wired.com/story/gfycat-artificial-intelligence-deepfakes/ Acesso em: 17 mar. 2021.

MENEZES NETO, Elias Jacob de. *Surveillance, democracia e direitos humanos*: os limites do Estado na era do big data. 2016. Tese (Doutorado em Direito) - Universidade do Vale do Rio dos Sinos - UNISINOS, São Leopoldo, 2016.

MILLIGAN, Christopher S. Facial recognition technology, video surveillance, and privacy. *Southern California Interdisciplinary Law Journal*, v. 9, p. 295-334, 1999.

MOHRI, M.; ROSTAMIZADEH A.; TALWALKAR A. *Foundations of machine learning*. 2 ed. Cambridge: The MIT Press, 2018.

MOREHAM, N. A. Privacy in public places. *The Cambridge Law Journal*, v. 65, n. 3, p. 606–635, 2006.

NASCIMENTO, Silvânia. *Reconhecimento facial resulta nas prisões de 33 pessoas*. 2019. Disponível em: http://www.ssp.ba.gov.br/2019/04/5613/Reconhecimento-Facial-resulta-nas-prisoes-de-33-pessoas.html Acesso em: 17 mar. 2021.

NILSSON, Nils J. *Artificial intelligence*: a new synthesis. San Francisco: Morgan Kaufmann Publishers, 1998.

O'MEARA, Sarah. New app rates Shanghai Citizens' Honesty: pilot ideas for nationwide social credit system are rolled out in China's biggest city. *Sixth Tone,* nov. 2016. Disponível em: http://www.sixthtone.com/news/1554/new-app-rates-shanghai-citizens%20-honesty Acesso em: 01 abr. 2021.

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

POLLARD, Martin. Even mask-wearers can be ID'd, China facial recognition firm says. *Reuters,* mar. 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL Acesso em: 01 abr. 2021.

POWELL, Walter W.; SNELLMAN, Kaisa. The knowledge economy. *Annual Review of Sociology*, v. 30, n. 1, p. 199-220, ago. 2004. DOI: http://dx.doi.org/10.1146/annurev.soc.29.010202.100037 Disponível em: https://www.annualreviews.org/doi/full/10.1146/annurev.soc.29.010202.100037 Acesso em: 27 mar. 2021.

REIDENBERG, Joel. Privacy in Public. *University of Miami Law Review*, v. 69, p. 141, 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2493449 Acesso em: 11 abr. 2021.

REIMAN, J. Driving to the panopticon: a philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara High Technology Law Journal*, v. 11, n. 1, p. 27, jan. 1995.

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

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (1. Vara da Fazenda Pública). *Ação de Produção Antecipada de Provas nº 1006616-14.2020.8.26.0053*. Relator: Juíza Renata Barros Souto Maior Baião, 02 de fevereiro de 2020. Disponível em: https://www.jusbrasil.com.br/processos/252983937/processo-n-1006616-1420208260053-do-tjsp Acesso em: 17 abr. 2021.

SÃO PAULO. Tribunal de Justiça do Estado de São Paulo (37. Vara Cível). *Ação Civil Pública nº 1090663-42.2018.8.26.0100*. Relator: Juíza Patrícia Martins Conceição, 30 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/processos/202658044/processo-n-1090663-4220188260100-do-tjsp Acesso em: 17 abr. 2021.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*. 6. ed. São Paulo: Saraiva, 2017.

SILVA, Luís Virgílio Afonso da. O conteúdo essencial dos direitos fundamentais e a eficácia das normas constitucionais. *RDE: Revista de Direito do Estado*, Rio de Janeiro, v. 1, n. 4, p. 23-51, 2006.

STAN Z. LI *et al.* (orgs.). *Handbook of Face Recognition*. London: Springer London, 2011.

STEPHEN CHEN. China to build giant facial recognition database to identify any citizen within seconds. *South China Morning Post*, 12 out. 2017. Disponível em: https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any. Acesso em: 01 abr. 2021.

TASSO, C. An introduction to artificial intelligence and to the development of knowledge-based systems. *In:* TASSO, Carlo; OLIVEIRA, Edoardo R. Arantes e (orgs.). *Development of knowledge-based systems for engineering*. Vienna: Springer Vienna, 1998. p. 11-26. Disponível em: http://link.springer.com/10.1007/978-3-7091-2784-1_2 Acesso em: 23 abr. 2021.

TURING, A. M. Computing machinery and intelligence. *Mind,* v. 54, n. 236, p. 433-460, 1950.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, v. 4, n. 5, p. 192-220, dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf Acesso em: 5 abr. 2021.

WESTIN, A. F. *Privacy and freedom*. New York: Ig Publishing, 1967.

XI JIPING. *Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with chinese characteristics for a new era*. 2017. Disponível em: http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf. Acesso em: 26 mar. 2021.

XINHUA. *Across China*: facial recognition, new watchdog of Beijing public rental neighborhoods. 2019. Disponível em: http://www.xinhuanet.com/english/2019-07/22/c_138247731.htm Acesso em: 01 abr. 2021.

XINHUA. *Chinese company develops 3D facial recognition system*. 2020. Disponível em: http://www.xinhuanet.com/english/2020-03/04/c_138842757.htm Acesso em: 01 abr. 2021.