REVISTA DE DIREITO E ATUALIDADES

INSTRUMENTOS DE RECONHECIMENTO FACIAL E OS CONTORNOS DA LEI GERAL DE PROTEÇÃO DE DADOS ANTE A PRIVACIDADE NAS CIDADES (IN)INTELIGENTES.

Guilherme Ornelas Monteiro[1]

Resumo: O presente artigo analisou se a implementação de sistemas de reconhecimento facial em cidades pode significar abandono ao direito de proteção de dados. Desse modo, o artigo apresenta uma síntese da literatura acadêmica acerca das cidades inteligentes, destacando como tecnologias de reconhecimento de dados biométricos faciais são comumente utilizados pelo poder público. O artigo cobriu as fragilidades do uso desse sistema, analisando pesquisas e estudos que evidenciam a imprecisão dessas soluções e seu potencial efeito discriminatório aos grupos vulneráveis quando adotados pelo Estado. Norteando esses desafios, o presente artigo investigou como a Lei Geral de Proteção de Dados recepciona a utilização dessas soluções e garante legitimidade para que o Poder Público possa implementá-las. Além disso, investigou-se como a Autoridade Nacional de Proteção de Dados pode se espelhar em experiências de autoridades internacionais de proteção de dados para garantir o usufruto dessas soluções no Brasil. Do ponto de vista teórico, o estudo entende que a não priorização do direito de proteção de dados ante a utilização dessas tecnologias pelo poder público pode ter efeitos discriminatórios em sociedade, ao passo que deslegitima sua utilização e torna a cidade ininteligente. Na conclusão, o estudo demonstra possíveis cenários em que a adoção de tecnologias de reconhecimento facial pelo Poder Público possa ocorrer em conformidade com a lei de proteção de dados pessoais.

Palavras-chave: Lei Geral de Proteção de Dados; Reconhecimento facial; Cidade inteligente; RGPD; dados pessoais sensíveis.

---

[1] Graduando em Direito pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Membro do grupo de Direito e Ciência Comportamental (IDP/CNPq). Integrante da Clínica de Direitos Humanos IDP.

REVISTA DE
DIREITO E
ATUALIDADES

FACIAL RECOGNITION SYSTEMS AND THE LEGAL IMPLICATIONS OF THE BRAZILIAN GENERAL DATA PROTECTION LAW IN SMART CITIES.

Abstract: *The purpose of this article is to analyze whether the implementation of facial recognition systems in cities could mean abandoning personal data protection rights. This article attempts to provide an overview of the academic literature about smart cities, highlighting how facial recognition technologies are commonly and widely used by the government. This article covers the weaknesses of using facial recognition systems by analyzing studies that show the low level of facial recognition accuracy and its potential to involve discriminatory bias, particularly against vulnerable groups. In this context, this article investigates how the Brazilian General Data Protection Law guarantees legitimacy for the government to implement these facial recognition systems. In addition, this article addresses how The Brazilian National Data Protection Authority can adopt and follow the legal parameters of international data protection authorities to guarantee the proper application of facial recognition systems in Brazil. From a theoretical point of view, this article concludes that not prioritizing the right to privacy when adopting facial recognition technologies to be used in the public sphere may have harmful effects on society, particularly against civil liberties, meaning that smart cities do not work in our best interests. The study concludes by demonstrating possible scenarios for the adoption of facial recognition technologies in accordance with the Brazilian General Data Protection Law.*

Keywords: *Brazilian General Data Protection Law; Facial Recognition; smart city; GDPR; Sensitive Personal Data.*

1. INTRODUÇÃO

A rápida urbanização e novos desafios de promoção e alocação de bens e serviços podem tornar ineficiente a gestão pública. Novas tecnologias de informação e comunicação (TICs) surgem como instrumentos alternativos e promissores para tornar a administração de serviços urbanos mais célere e sustentável (JOH, 2019).

A integração desses sistemas é aplicável na esfera de vigilância estatal para fins de tutela da saúde e incolumidade física dos cidadãos. Em âmbito nacional, por exemplo, o município de Vitória, no Espírito Santo, desenvolveu o Dispositivo de Segurança Preventiva (DSP) conhecido como "botão do pânico", com a finalidade de oferecer instrumento de segurança para proteger mulheres vítimas de violência doméstica. Mulheres sob medida protetiva que observavam o agressor não respeitando o distanciamento legal, situação indicativa de grave ameaça, podiam notificar a patrulha policial mais próxima[2] por meio de acionamento desse mecanismo eletrônico. Em Santa Catarina, o Laboratório de Inovação do Governo (NIDUS) desenvolve instrumentos de realidade aumentada para a atuação das ocorrências policiais[3].

As soluções podem ser integradas, ainda, para variados setores: (i) situações de emergência como pedidos de socorro podem ser detectados por sensores de áudio espalhados pela cidade (IM CHO, 2012); (ii) sensores sonoros são aptos a detectar barulho de disparos de armas de fogo (WELSH; ROY, 2017); (iii) *machine learning* e *big data* viabilizam o rastreio de crimes financeiros (SADGALI; SAEL; BENABBOU, 2018); e (iv) técnicas de reconhecimento

---

[2] Botão do pânico, dispositivo de segurança que ajuda a proteger mulheres vítimas de violência doméstica, completa 6 anos. I**mprensa e Comunicação Social do Tribunal de Justiça do Espírito Santo.** 17 abr. 2019. disponível em: http://www.tjes.jus.br/botao-do-panico-dispositivo-de-seguranca-que-ajuda-a-proteger-mulheres-vitimas-de-violencia-domestica-completa-6-anos/. acesso em: 21 nov. 2020.

[3] Laboratório Nidus auxilia órgãos do Governo a solucionarem desafios com uso de tecnologia e inovação. 04 ago. 2020. Disponível em: https://www.sc.gov.br/noticias/temas/institucional/laboratorio-nidus-auxilia-orgaos-do-governo-a-solucionarem-desafios-com-uso-de-tecnologia-e-inovacao?highlight=WyJyZWNvbmhlY2ltZW50byIsImZhY2lhbCIsInJlY29uaGVjaW1lbnRvIGZhY2lhbCJd. Acesso em: 22 nov. 2020.

de gestos, falas, expressões faciais e corporais podem detectar e prevenir tentativas de suicídio em metrôs, de modo a avaliar a propensão de uma pessoa se suicidar (THODORIS ANAGNOSTOPOULOS, 2014).

Diante desse cenário, a adoção de soluções integradas de TICs vocacionados a tornar setores urbanos mais inteligentes pelos atores urbanos (governo, cidadãos, órgãos públicos, instituições privadas e públicas) acentua-se. Driblar problemas que obstaculizam o fornecimento mais eficiente de bens e serviços, seja pela alocação inteligente de carros em ruas, digitalização de serviços governamentais ou mesmo pela atividade policial, torna-se uma tendência: é a resposta da cidade para a urbanização e a revolução digital (CUNHA et al., 2016). Essas tecnologias, no entanto, são vulneráveis à ataques cibernéticos que podem comprometer o funcionamento das cidades. Por vezes, esses sistemas carecem de mecanismos sólidos de segurança o que torna necessário a produção de novos estudos que se debrucem sobre essas tecnologias que em primeiro momento externalizam benesses, mas serão cada vez mais vulneráveis à ataques (CUI et al., 2018).

A partir desse cenário, em que as cidades se tornam inteligentes, instrumentos de reconhecimento facial também servem como alternativas para tornar factível a tutela da saúde e proteção dos cidadãos. A adoção desses sistemas aumenta a capacidade de vigilância em setores urbanos e oportuniza um poder de polícia mais efetivo.

Essa adoção de mecanismos de reconhecimento facial, contudo, merecem notada atenção, pois ao passo que mais câmeras de reconhecimento facial aumentam, a privacidade diminui. A partir dessa perspectiva, a utilização dessas técnicas pressupõe o tratamento massivo de dados pessoais sensíveis que, como será visto, merecem notada atenção posto seu potencial poder discriminatório. É nesse sentido que as leis e regulamentos sobre proteção de dados são dispositivos legais essenciais para contornar a aplicação desses sistemas.

O presente artigo discutiu se a adoção de instrumentos de reconhecimento facial é compatível com a Lei Geral de Proteção de Dados. Noutras palavras, o objetivo principal do artigo foi analisar e questionar a ressignificação do direito de proteção de dados em cidades inteligentes. A partir do objetivo principal, o artigo delineou três áreas de estudo: (i) apresentou-se algumas ponderações sobre *smart cities* e os fatores que influenciam na adoção de instrumentos de TICs para soluções inteligentes de gestão urbana; (ii) analisou-se como a Lei

Geral de Proteção de Dados pode recepcionar instrumentos de reconhecimento facial, quais são os dispositivos jurídicos que legitimam seu uso e os desafios inerentes que podem resultar em efeitos disruptivos sobre a sociedade; e (iii) observou-se, a partir de uma perspectiva comparada, a recepção das tecnologias de reconhecimento facial.

A metodologia adotada compreendeu uma revisão bibliográfica sobre a Lei Geral de Proteção de Dados (LGPD), o Regulamento Geral de Proteção de Dados da União Europeia (GDPR), sobre a literatura acerca de *smart city,* investigações e estudos empíricos sobre a eficiência de modelos de TICs integrados em setores urbanos e sobre a discriminação algorítmica (*machine bias).* Além disso, a partir de um panorama exploratório, estudou-se o posicionamento de autoridades internacionais de proteção de dados sobre o uso de sistemas de reconhecimento facial pelo poder público.

Dessa forma, o estudo se divide em quatro partes. Primeiramente, apresentou-se o que pode ser considerado uma cidade inteligente, os fatores que tornam a aceitação de conjuntos de TICs uma necessidade e o potencial crescimento de seu uso.

Na segunda parte, o artigo destacou como a LGPD recepciona os instrumentos de reconhecimento facial, evidenciando o que são os dados sensíveis, as hipóteses em que pode ocorrer o tratamento de dados biométricos e as salvaguardas indispensáveis para seu uso. Ainda na segunda parte, o artigo destacou os desafios para o usufruto eficiente do sistema de reconhecimento facial, evidenciando a possibilidade que essa ferramenta tem de discriminar grupos vulneráveis e aumentar a assimetria informacional entre cidadão e Estado.

Na terceira parte, a partir de um panorama exploratório em uma perspectiva comparada, mostrou-se como a GDPR também recepciona o tema, as recomendações e decisões de autoridades de proteção de dados estrangeiras e o que a Agência Nacional de Proteção de Dados (ANPD) pode se espelhar nessas instruções. Por fim, a conclusão.

2. SMART CITIES: UMA TENDÊNCIA INEVITÁVEL

O avanço estrutural de novos mecanismos de tratamento de dados nas cidades inteligentes, que a literatura inglesa se refere como *smart cities,* acentua-se na medida em que o crescimento populacional também aumenta.

O que difere uma cidade ordinária para uma inteligente se amostra ao passo que soluções tecnológicas são integradas à administração pública para a superação de desafios

administrativos. Métodos criativos para resolver dificuldade de gestão surgem em consonância com a urbanização e tendências digitais, mas se defrontam com a perspectiva do cidadão e seus direitos de privacidade e proteção de dados pessoais.

Em estudo coordenado pelo Centro de Estudos em Administração Pública e Governo da Fundação Getúlio Vargas[4], os pesquisadores delinearam o que chamam de estágios de evolução para uma efetiva implementação de uma cidade inteligente: fase vertical, fase horizontal, fase conectado e fase inteligente.

A fase vertical é o estágio em que a administração pública adota, com vistas a manter serviços de infraestrutura (energia, abastecimento, água, iluminação), mecanismos de tecnologia; a fase horizontal é a integração dos serviços urbanos em uma plataforma transversal; a fase conectada ocorre quando a gestão dos serviços verticais se concentra e se correlaciona em uma plataforma de gestão; e o estágio inteligente é a possibilidade de todos esses serviços serem conduzidos simultaneamente, de modo que o cidadão, o estado e as empresas se tornam partes interessadas nas soluções advindas da aplicação de tecnologia em âmbito de gestão[5] (CUNHA et al., 2016).

Esses estágios de desenvolvimento se alicerçam em um conceito de cidade inteligente que agregue fatores de "visão holística ou global", "meio para melhorar a qualidade de vida", "a tecnologia como fator disruptivo" e "um novo modelo de relações"[6] (CUNHA et al., 2016).

A visão holística se caracteriza por considerar a cidade inteligente como a que aplica inteligência em todos os setores e assuntos urbanos, de forma a não priorizar setores em detrimento de outros. A cidade também deve buscar enriquecer a qualidade de vida dos indivíduos a partir de adoção de práticas sustentáveis, de um setor produtivo moderno e concorrente que seja atrativo para a captação de capital (CUNHA et al., 2016).

A tecnologia como fator disruptivo é o elemento em que a cidade utiliza mecanismos para coletar massivamente dados com vistas a permitir interoperabilidade na cidade com serviços e setores urbanos, tais como de energia, de saúde, de transporte, por exemplo. A tecnologia

---

[4] ALEXANDRA CUNHA, Maria; PRZEYBILOVICZ, Erico; FERNANDA MEDINA MACAYA, Javiera; BURGOS, Fernando. SMART CITIES: Transformação digital de cidades. **Fundação Getulio Vargas, FGV-EAESP**, ano 2016, ed. 1ª edição, p. 1-164, 4 jan. 2016. Disponível em: https://ceapg.fgv.br/sites/ceapg.fgv.br/files/u60/smart_cities_bra_versao_final.pdf. Acesso em: 20 nov. 2020.

[5] Ibdem p.10

[6] Ibdem p.29

assume papel de facilitador, promove a digitalização como componente essencial para o tratamento de dados pessoais (CUNHA et al., 2016).

Por fim, a cidade, na medida em que adota tais critérios, modifica as relações sociais – os atores urbanos (cidadãos, órgãos públicos, empresas, governo, turistas, investidores) passam a integrar uma economia colaborativa: a gestão e o oferecimento de bens e serviços são construídos com a participação de todos os atores urbanos com a contribuição das TICs (CUNHA et al., 2016).

Esses ciclos de desenvolvimento, no entanto, não se expressam de modo homogêneo, uma vez que os fatores que potencializam essas fases (urbanização e desenvolvimento tecnológico, por exemplo) tendem a crescer em conformidade com as especificidades de desenvolvimento social de cada cidade. A título de exemplo, em âmbito internacional, na França, a cidade de Paris atém em média 30% da economia do país e, no Brasil, a cidade de São Paulo se evidencia com quase 11,4% da economia do país[7] (CUNHA et al., 2016). É nesse sentido que, nessas cidades, os estágios de desenvolvimento tendem a se concretizar de modo mais célere do que outras.

Em termos de crescimento populacional, ainda que não seja determinante, também influencia na passagem para uma cidade inteligente, mas demonstra ser um fator irregular. Em relatório de 2019 do *United Nations Department of Economic and Social Affairs*[8], a China e a Índia ocupam a categoria dos países mais populosos do mundo, com 1.43 bilhão e 1.37 bilhão de cidadãos, respectivamente.

A irregularidade se revela quando a projeção de aumento populacional para 2050 posiciona a Índia como o país mais populoso do mundo. Essa inconstância, ainda, concentrará mais da metade da população em somente nove países: Índia, Nigéria, Paquistão, República Democrática do Congo, Etiópia, Tanzânia, Indonésia, Egito e Estados Unidos[9].

O crescimento populacional, econômico e a urbanização[10] aceleraram o processo de

---

[7] Ibdem p.21

[8] DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS POPULATION DIVISION. World Population Prospects 2019. **United Nations**, [*S. l.*], p. 1-46, 7 jan. 2019. Disponível em: https://population.un.org/wpp/Publications/Files/WPP2019_Highlights.pdf. Acesso em: 20 nov. 2020.

[9] Ibdem p.12; *'' India is expected to add nearly 273 million people between 2019 and 2050, while the population of Nigeria is projected to grow by 200 million. Together, these two countries could account for 23 per cent of the global population increase to 2050''*

adoção de mecanismos tecnológicos para cuidar dos serviços urbanos, afinal, quanto maior a população em cidades, maior será a necessidade de gerir os serviços de infraestrutura. No entanto, como mencionado, esse crescimento se relaciona com as características de cada país e não podem ser interpretados como fenômenos homogêneos.

No Brasil, pesquisa do Instituto Brasileiro de Geografia e Estatística (IBGE) evidenciou que a população dos municípios brasileiros teve crescimento de 0,77% em comparação com o ano de 2019[11]. Com efeito, o crescimento populacional evidente propulsiona a hiperconectividade: as cidades se tornam polos de inovação, pois a tecnologia assume papel disruptivo na gestão administrativa para contornar problemas de gestão e de oferecimento de bens e serviços (CUNHA et al., 2016).

Problemas de infraestrutura e organização social obstaculizam uma completa reunião dos estágios de desenvolvimento de uma cidade inteligente, de maneira que a aplicabilidade de tecnologias emergentes nesses problemas reflete um novo modelo de cidade.

A definição proposta pela União Europeia de cidade inteligente é a que busca solucionar problemas estruturais com a adoção de tecnologias da informação e comunicação (TICs) sobre o viés de colaboração e participação plural de áreas municipais (EUROPEAN UNION, 2014). Essa definição aponta para a adoção de tecnologias em seis setores: *smart governance*, *smart economy, smart mobility*, *smart environment*, *smart people* e *smart living.*

O primeiro ângulo exige que o governo promova serviços de integração com organizações públicas e privadas, serviços estes baseados em infraestruturas de TICs. Economia inteligente é agregar valor para os atores urbanos, recepcionando novos modelos de negócios (*e-business* e *e-commerce)* a fim de que haja maior interconexão de bens e serviços. A mobilidade inteligente busca aumentar serviços logísticos e de transporte em uma abordagem sustentável e que se comunique com serviços de tecnologia. O ângulo do meio ambiente, analogamente, é a

---

[10] Relação entre o aumento e progresso das cidades ante fatores como dimensão territorial, industrialização, população e migração.

[11] IBGE. IBGE divulga estimativa da população dos municípios para 2020. **Instituto Brasileiro de Geografia e Estatística**, Agência IBGE, p. S.I, 27 ago. 2020. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/28668-ibge-divulga-estimativa-da-populacao-dos-municipios-para 2020#:~:text=IBGE%20divulga%20estimativa%20da%20popula%C3%A7%C3%A3o%20dos%20munic%C3%ADpios%20para%202020,-Editoria%3A%20Estat%C3%ADsticas%20Sociais&text=O%20IBGE%20divulga%20hoje%20as,77%25%20em%20rela%C3%A7%C3%A3o%20a%202019. Acesso em: 20 nov. 2020.

construção de uma cidade baseada em consumo de energia, bens e serviços sustentáveis. *Smart people* é o engajamento dos cidadãos com os mecanismos de tecnologia, é dizer que a educação se debruça sobre a possibilidade de os indivíduos adquirirem educação digital. A última tecnologia – o *smart living* – inclui oportunizar estilos de vida, comportamentos e espaços seguros para o exercício da cidadania em coadjuvação com as TICs.

Partindo dessas características, em 2011, na União Europeia, constatou-se que o maior número de cidades inteligentes se concentrava no Reino Unido, Itália e Espanha. As cidades não contemplavam os seis pilares propostos pela União Europeia de o que seria uma cidade inteligente, mas continham pelo menos uma delas.

Das 480 cidades da União Europeia com pelo menos 100.000 habitantes, 240 cidades possuíam uma das características elencadas (EUROPEAN UNION, 2014, p.32). As características mais comuns entre elas são o meio ambiente e mobilidade inteligentes - 33% e 21% das cidades respectivamente.

As outras quatro características se encontram em somente 10% das outras cidades. Esses dados evidenciam que não há como valorar uma cidade inteligente partindo do pretexto de que a cidade oportunizará que todos os setores urbanos adotem sistemas de TICs. Em outros termos, as iniciativas ocorrem em ângulos isolados, por vezes adotando as TICs em somente um setor, o que já oportuniza a criação de ponte necessária para uma cidade transitar rumo ao conceito de cidade inteligente.

Essas implicações conceituais que visam categorizar uma cidade em inteligente carecem de se debruçar sobre os perfis de políticas públicas de segurança que podem ser adotadas em coadjuvação com as TICs (LAUFS; BORRION; BRADFORD, 2020). Uma abordagem digital à procura de soluções maximizadoras de bem-estar social em que o governo assume papel atuante na promoção de setores urbanos tecnológicos não poderia ignorar o desenvolvimento inteligente do poder de polícia (JOH, 2019).

3. CÂMERAS DE RECONHECIMENTO FACIAL

Uma das várias aplicações que viabilizam um rendimento maior da vigilância é por meio da adoção de instrumentos de reconhecimento facial. Em Santa Catarina, o uso dessa técnica já é usado no aeroporto de Florianópolis[12], também estudado para ser aplicado na gestão

de cadastro de aposentados e pensionistas em sistema de previdência, de modo que não precisariam se deslocar aos órgãos públicos para realizar seu recadastramento, bastaria o reconhecimento facial[13] e, ademais, aplicado em vigilância policial, inclusive com uma eficácia que resultou em prisões de criminosos foragidos[14]. São exemplos, também, o Estado da Bahia, que a cobertura do reconhecimento facial resultou na captura de quarenta e dois foragidos[15], a cidade do Rio de Janeiro[16] também trabalha na adoção do sistema para segurança pública e o Governo do Distrito Federal[17] idem.

No entanto, essas novas perspectivas de adoção de instrumentos de TICs realizam o tratamento de dados pessoais (coleta, armazenamento, distribuição, avaliação, processamento, entre outros) que devem ser compreendidos à luz da LGPD.

Não é dizer que as leis de privacidade surgem como fatores inibidores do desenvolvimento urbano, mas é pensar na adoção desses sistemas em uma perspectiva que os dados pessoais que serão tratados por esses mecanismos estejam resguardados e socorridos ante práticas arbitrárias e deletérias que possam surgir a partir de uma má gestão desses recursos. Necessário, portanto, entender como as leis de proteção de dados pessoais recepcionam essas tendências e quais são os desafios inerentes a elas.

---

[12] Governo Federal realiza teste de embarque por reconhecimento facial no aeroporto de Florianópolis. **Globo.** 8 out. 2020. Disponível em: https://g1.globo.com/sc/santa-catarina/noticia/2020/10/08/governo-federal-realiza-teste-de-embarque-por-reconhecimento-facial-no-aeroporto-de-florianopolis.ghtml. Acesso em: 22 nov. 2020.

[13] Prova de vida de inativos e pensionistas de Santa Catarina será com reconhecimento facial. 12 ago. 2020. Disponível em: https://www.sc.gov.br/noticias/temas/ciencia-e-tecnologia/prova-de-vida-de-inativos-e-pensionistas-de-santa-catarina-sera-com-reconhecimento-facial?highlight=WyJyZWNvbmhlY2ltZW50byIsImZhY2lhbCIsInJlY29uaGVjaW1lbnRvIGZhY2lhbCJd. Acesso em: 22 nov. 2020.
Ver também a utilização da técnica em âmbito federal: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/agosto/reconhecimento-facial-pelo-aplicativo-meu-gov-br-e-a-primeira-etapa-da-prova-de-vida-dos-aposentados. Acesso em 25 nov 2020.

[14] SC tem primeiras prisões indicadas por sistema de câmeras de monitoramento**. Governo de Santa Catarina.** 12 jun. 2019. Disponível em: https://www.sc.gov.br/index.php/noticias/temas/seguranca-publica/sc-tem-as-primeiras-prisoes-indicadas-por-sistema-utilizado-em-cameras-de-monitoramento-da-secretaria-de-estado-da-seguranca-publica. Acesso em: 22 nov. 2020.

[15] Reconhecimento Facial captura 42 foragidos na folia. **Governo do Estado da Bahia.** 26 fev. 2020. Disponível em: http://www.ssp.ba.gov.br/2020/02/7296/Reconhecimento-Facial-captura-42-foragidos-na-folia.html. Acesso em: 22 nov. 2020.

[16] Município estende Rio+Seguro à Zona Oeste com câmeras de reconhecimento facial. **Prefeitura da Cidade do Rio de Janeiro.** 22 jan. 2020. Disponível em: https://prefeitura.rio/cidade/municipio-estende-rioseguro-a-zona-oeste-com-cameras-de-reconhecimento-facial. Acesso em: 22 nov. 2020.

[17] Segurança Pública usará reconhecimento facial e drones no Carnaval. **Governo do Distrito Federal.** 12 fev. 2020. Disponível em: http://www.ssp.df.gov.br/seguranca-publica-usara-reconhecimento-facial-e-drones-no-carnaval/. Acesso em: 22 nov. 202

4. CONTORNOS DA LEI GERAL DE PROTEÇÃO DE DADOS E DESAFIOS

Os dados pessoais são fragmentos de informações que possibilitam a identificação de uma pessoa. A identificação pode ser direta ou indireta, pois os fragmentos podem ser disciplinados e correlacionados para autenticar a identidade de um indivíduo.

O dado, como unidade básica da informação, deve ser relacionado com outros fatores para se tornar pessoal. A partir de uma interpretação extensiva, em que o dado pessoal é o dado que direta ou indiretamente se relaciona a uma pessoa natural abarca nome, dados bancários, fotos, orientação sexual, religião, endereço de e-mail, dados médicos e histórico de compras, por exemplo.

À vista de uma interpretação extensiva, a LGPD considera dado pessoal como a informação "relacionada a pessoa natural identificada ou identificável" (art. 5, I, LGPD).

Para além dos dados pessoais, a LGPD disciplina o conceito de dados pessoais sensíveis que são os dados que potencializam discriminação (DONEDA, 2019). Os dados pessoais sensíveis estão intrinsecamente relacionados às características da personalidade e honra de uma pessoa: dado genético, dado biométrico, opinião política, origem racial ou ética, dados de caráter religioso ou filosófico (art. 5º, II, LGPD). Esse dispositivo legal busca conferir proteção privilegiada aos dados pessoais sensíveis, uma vez que o tratamento errôneo desses fragmentos pode se tornar um instrumento discriminatório.

O especial zelo para o tratamento dos dados sensíveis deve partir de uma interpretação expansiva do art. 11 §1º da LGPD, cuja essência é a de evitar que o manuseio desses dados que, numa análise rasa, poderiam ser considerados não sensíveis, mas, se relacionados com outros fragmentos puderem expor informações sensíveis sobre um indivíduo, deverão ser tratados com as mesmas salvaguardas que o tratamento de dados pessoais sensíveis requer desde o início.

Mecanismos de reconhecimento facial realizam o tratamento[18] de dados sensíveis, pois coletam, armazenam, acessam, transmitem, processam, avaliam dado biométrico (dado referente às características fisiológicas de uma pessoa). Nesse sentido, o consentimento do titular dos dados, que deve ser uma manifestação livre, informada e inequívoca, deve também ser sempre

[18] Nos termos da LGPD, art. 5º, X, tratamento de dados é "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração."

solicitado à vista de uma finalidade específica (art.5, XII, LGPD). O titular dos dados, assim, necessita ter conhecimento sobre o motivo, finalidade e quais os procedimentos que estão sendo aplicados aos seus dados, isto é, há de se ter transparência acerca dos tratamentos (art. 9 e 6 LGPD).

O ato do consentimento deve ser exercido de modo substancial, ao passo que o titular possa gozar da autodeterminação informativa (posto como fundamento da lei), que concede o direito de o titular requisitar informações, a exclusão de seus dados, ou seja, decidir sobre os limites pelos quais os seus dados serão tratados (art. 2, II).

O consentimento se torna um ato em que o titular confere às instituições privadas e públicas a possibilidade de realizarem o tratamento de seus dados para uma finalidade específica e não significa, portanto, que o titular renunciou sua custódia sobre suas informações. O consentimento é um ato que representa a autonomia individual e não seu abandono (MENDES, 2014).

O consentimento, porém, é relativizado quando o tratamento dos dados pessoais sensíveis corresponde às hipóteses do inciso II, do art. 11 da LGPD. O consentimento elencado pela lei, que obriga as instituições requisitarem a anuência do titular para o tratamento de seus dados, pode ser desnecessário em certas circunstâncias, mas somente quando se trata de interesse público. Para ilustrar essa assertiva, quando o tratamento de dados pessoais sensíveis for necessário para a proteção da vida física do titular e terceiro, aplicação de políticas públicas previstas em leis ou regulamentos (inclusive quando necessário o compartilhamento pela administração pública), prevenir fraudes em sistemas eletrônicos, cumprimento de obrigação legal ou regulatória pelo controlador, o Estado está legitimado a dispensar o instituto do consentimento (art. 11, II, LGPD).

Para além do consentimento (salvo as hipóteses explicadas), o controlador e operador de dados (art. 5, VI e VII, LGPD) deverá, sempre que possível, aplicar procedimento de anonimização aos dados pessoais sensíveis, em vista de seu potencial poder discriminatório. Os dados anonimizados não viabilizam a identificação direta ou indireta do seu titular, como são, a título de exemplo, os dados estatístico e agregado.

Para um dado perder sua capacidade de associação ao seu titular, deve ser submetido a um processo que retire seu poder identificador: processo de anonimização (art., 5, III, LGPD).

Ainda que nenhum processo de anonimização seja completamente invulnerável, deve-se buscar aplicar técnicas e procedimentos que não permitam que com esforços razoáveis o processo de anonimização possa ser revertido e identificar seu titular, ou seja, o processo não pode ser incipiente.

A LGPD, nesse sentido, dispõe que se o processo de anonimização for obsoleto, as instituições não poderão afirmar que o dado é anônimo, pelo contrário, o dado será considerado pessoal desde o início de seu tratamento (art. 12, LGPD).

Desse modo, mesmo que nas hipóteses do artigo 11 o consentimento seja desnecessário, os princípios e fundamentos da lei ainda são imprescindíveis para a legalidade do tratamento de dados em âmbito governamental, de modo que a sua não observação acarretaria uma violação à lei.

O tratamento de dado biométrico deve se valer do princípio da não discriminação, é dizer, o seu tratamento não pode ser utilizado para objetivos ilícitos, discriminatórios ou abusivos (art. 9, IX, LGPD). Esse parece ser um dispositivo que ameaça a efetividade de muitos experimentos de reconhecimento facial.

Sistemas de reconhecimento facial utilizam decisões automatizadas realizados por mecanismos de *machine-learning system.* Essas soluções, por vezes, não necessitam de uma interpretação humana para sua execução, o próprio programa é apto a realizar sua função detectando, agindo e eventualmente replicando padrões da sociedade. A problemática surge quando diversos padrões sociais são discriminatórios e podem ser internalizados por instrumentos tecnológicos. Decisões automatizadas podem prejudicar os grupos mais vulneráveis e, portanto, uma interpretação humana na valoração dessas decisões, sobretudo quando adotada pelo Estado, pode ser uma alternativa para mitigar possíveis externalidades negativas (EUBANKS, 2018). Não é dizer que o programa é propositalmente construído para se tornar um meio discriminatório, mas ele passa a aprender e parodiar o que se analisa.

A rede social *Twitter*, por exemplo, foi acusada de adotar um conjunto de algoritmo discriminatório, em que postagens de fotos de pessoas negras tendiam a ser minimizadas no *feed* da rede social. Melhor explicando: em uma foto de várias pessoas, brancas e negras, postada na rede social, a foto quando exposta no *feed* de notícias dos usuários somente expunha as pessoas

brancas, de modo que a foto minimizada desprivilegiava a exposição das pessoas negras, tornando sua visibilidade somente possível quando o usuário clicasse na foto para expandi-la.

Conquanto a empresa alegue que não encontrou indícios discriminatórios nos algoritmos de reconhecimento facial, dezenas de usuários relataram o mesmo problema[19]. As decisões automatizadas de tecnologias refletem potenciais perigos discriminatórios: algoritmos alicerçados em métricas que excluem o estudo de demografia, estarão propensos a produzir falsas conclusões em suas decisões automatizadas.

Nos Estados Unidos, departamentos de polícia utilizam, sem o consentimento, fotos de metade dos adultos estadunidenses para a identificação de suspeitos em sistemas de reconhecimento facial. A precisão desses instrumentos é irregular e tende a apresentar piores resultados em análise de grupos demográficos de indivíduos do sexo feminino, negros e jovens (NAJIBI, 2020).

Alex Najibi, em publicação em portal da universidade de Harvard, destaca o estudo *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* das pesquisadoras Timnit Gebru e Joy Buolamwini que analisaram três conjuntos de algoritmos de classificação de gênero. As pesquisadoras trabalharam com os algoritmos categorizando o grupo de indivíduos em quatro classificações: “mulheres de pele mais escura”, “homens de pele mais escura”, “mulheres de pele mais clara” e “homens de pele mais clara”.

As pesquisadoras observaram que a tecnologia de reconhecimento facial demonstrou piores resultados de precisão na categoria de “mulheres de pele mais escura” – os três conjuntos de algoritmos priorizavam os outros grupos de pessoas (BUOLAMWINI; GEBRU, 2018). O sistema, que apresentou erro de 34,7% de precisão em identificar mulheres negras, deixava de as detectar. A partir disso, uma instituição (pública ou privada) não poderia delegar a avaliação de um serviço para um sistema de reconhecimento facial que exclui mulheres negras por sua imprecisão. Embora as pesquisadoras não identificassem o motivo pelo qual os sistemas de reconhecimento facial não detectavam mulheres de pele mais escura, há sugestões que podem estar intrínsecas à construção do próprio sistema. Um sistema de reconhecimento facial que foi treinado a partir de um banco de dados somente com fotos de homens de pele clara em

[19] Twitter investigates racial bias in image previews. **BBC NEWS.** 21 set. 2020. Disponível em: https://www.bbc.com/news/technology-54234822. Acesso em: 22 nov. 2020.

detrimento de homens e mulheres de pele mais escura, não estará apto a identificar a biometria destes indivíduos. Como as autoras apontam, são necessários mais estudos que revelem de fato as causas dessas imprecisões, ao passo que é necessário o comprometimento das empresas em revelar as métricas e parâmetros que subsidiaram a construção das tecnologias, isto é, que haja transparência.

A *Microsoft*[20]*, Amazon*[21] *e Ibm*[22] já alertaram que esses sistemas têm potencial impacto deletério para a sociedade, ressaltando a necessidade de os modelos de reconhecimento facial, que articulam com a inteligência artificial, serem alicerçados em uma perspectiva não discriminatória, que incluam revisões periódicas de riscos e potenciais abusos.

Desse modo, não há como valorar, ainda, um sistema eficaz e invulnerável às projeções discriminatórias (*machine bias*) e aos falsos positivos. No Brasil, para ilustrar, o reconhecimento facial utilizado no Rio de Janeiro pela Polícia Militar errou na identificação correta e implicou que uma mulher fosse detida por policiais[23].

Para além de distorções que podem ser automatizadas, deve-se pensar que a adoção dos modelos de reconhecimento facial, por parte do governo, carece de notada atenção, posto que o uso arbitrário dessas tecnologias pode dificultar garantias individuais. Uma intepretação deformada de que o uso desses instrumentos serve unicamente para preservar a segurança pública pode justificar uma maior vigilância e repressão para grupos vulneráveis que reivindicam seus direitos por meio de protestos civis: ao passo que essa visão prejudica grupos vulneráveis, a privacidade as empodera – esses sistemas não podem ser utilizados para inibir a privacidade como direito fundamental.

Os fundamentos da LGPD, notadamente o respeito à privacidade, à liberdade de expressão, de informação e opinião, aos direitos humanos e quanto ao exercício da cidadania (art. 2º), obstam o uso abusivo de instrumentos de reconhecimento facial. Ao garantir o direito à

---

[20] Facial recognition: It's time for action. **Microsoft.** 06 oct. 2018. Disponível em: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action. Acesso em: 22 nov. 2020.

[21] Some Thoughts on Facial Recognition Legislation. **Amazon.** 07 fev. 2019. Disponível em: https://aws.amazon.com/pt/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/. Acesso em: 22 nov. 2020.

[22] Mitigating Bias in AI Models. **IBM** 06 oct. 2018. Disponível em: https://www.ibm.com/blogs/research/2018/02/mitigating-bias-ai-models/. Acesso em: 22 nov. 2020.

[23] Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **Globo**. 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 22 nov. 2019

autodeterminação informativa, a transparência surge como um elemento que possibilita o titular dos dados, além de requisitar a exclusão, saber como ocorre o tratamento de suas informações. O artigo 20 da lei espelha a autodeterminação informativa: o titular dos dados usufrui do direito de solicitar a revisão de decisões automatizadas feitas por esses instrumentos de *machine-learning system,* é dizer, o controlador deverá fornecer informações suficientes para que o titular dos dados possa saber como essa decisão automatizada afeta seus interesses.

Esses dispositivos legais implicam em inibir vieses discriminatórios na construção desses sistemas, além de expor como estão sendo aplicados, seja por instituições privadas ou públicas. É evitar, assim, que os novos mecanismos de tecnologia adotados se tornem indecifráveis e intricados, em que não se sabe como se dão suas construções, aplicações, critérios de decisão e os efeitos de seu uso (PASQUALE, 2015).

Quando adotadas pelo Poder Público, no Brasil, para além da LGPD, o Estado deve observar os princípios constitucionais que norteiam sua atuação, principalmente a impessoalidade, a publicidade, a eficiência, a razoabilidade, a igualdade, a supremacia do interesse público, a proporcionalidade, com vistas a resguardar os fundamentos e princípios da LGPD.

5. PERSPECTIVA COMPARADA: O QUE O BRASIL PODE APRENDER?

Em âmbito internacional, não há regulamentos específicos que abordam o tratamento de dados biométricos faciais por parte de instituições públicas e privadas. O Regulamento Geral sobre a Proteção de Dados, da Europa, assim como a LGPD, garante especial proteção aos dados pessoais sensíveis, de modo que os dados biométricos representam risco para os direitos e liberdades fundamentais GDPR, (51).

Na Suécia, a agência governamental de proteção de dados, "*Datainspektionen",* aplicou multa administrativa de 20.000 euros a um município por violação à lei de dados europeia[24]. Uma escola pública, em Skelleftea, decidiu utilizar um sistema de reconhecimento facial como uma forma de contabilizar a presença e assiduidade dos estudantes na escola. O sistema, que ainda se encontrava em fase de teste, foi utilizado em uma das classes durante três semanas, realizando o

[24] Facial recognition in school renders Sweden's first GDPR fine. **Datainspektionen**. 21 ago. 2019. Disponível em: https://www.datainspektionen.se/nyheter/2019/facial-recognition-in-school-renders-swedens-first-gdpr-fine/. Acesso em: 22 nov. 2019

tratamento de dados biométricos faciais de 22 alunos. A escola requereu o consentimento explícito dos pais das crianças, ao passo que estes concederam.

No entanto, a agência entendeu que embora a escola tenha requisitado aos responsáveis pelas crianças a anuência para que pudesse manusear os dados, não houve preenchido os requisitos necessários para o gozo do instituto jurídico de modo substancial (consentimento como um ato informado, inequívoco, livre e para uma finalidade específica. art. 6º, §1, a; e art. 4º, §11, GDPR). Além disso, dado a assimetria informacional entre o controlar dos dados (poder público, haja vista se tratar de escola pública municipal) e o titular dos dados, o aludido consentimento não exerceu sua função de decisão informada, nos termos da GDPR (43). O consentimento não se pode valer como condição formal para que instituições públicas se projetem para realizar o tratamento indiscriminado dos dados, na verdade o consentimento deve ser exercido de modo substancial a fim de que essa assimetria de poder entre indivíduo e Estado seja mitigada.

O que tornou a ação da escola ilegal e incoerente com a lei europeia se encontra também na falta de conformidade com os princípios da lei. O princípio da adequação que circunscreve o tratamento de dados para uma finalidade pertinente e limitada ao que seja necessário para cumprir sua função, isto é, que haja minimização dos dados, não foi comprovado pela escola (art. 5º, §1º, c e §2º GDPR). Pelo contrário, instalar um sistema de reconhecimento facial que resultara no tratamento de dados sensíveis unicamente para garantir a assiduidade dos alunos é uma medida desproporcional que não obedeceu ao princípio. Melhor explicando: outros meios menos invasivos podem ser cogitados para garantir a presença dos alunos na escola.

A autoridade de proteção de dados francesa, *Commission nationale de l'informatique et des libertés*, publicou relatório em que traça alguns parâmetros para que agentes públicos possam utilizar o reconhecimento facial paralelamente assegurando a proteção de dados. Por exemplo, a autoridade indica que se o sistema for utilizado de modo experimental, só se justifica o uso se houver importante necessidade e comprovação de que as técnicas utilizadas pelo referido sistema guardam precisão para identificar dados biométricos faciais. Além disso, o controlador dos dados deve respeitar estritamente a lei europeia, requisitando o consentimento para cada tratamento de dado a ser usado; e o tratamento deve propender a minimizar os dados sob uma metodologia rigorosa[25].

A assimetria de poder que é apta a surgir na utilização de instrumentos de tratamento de dados pelo poder público pode prejudicar liberdades civis. O correto uso do sistema de reconhecimento facial deve estar alicerçado em uma construção que incida em aplicações éticas, *privacy by design*[26], que compreenda que o tratamento de dados deve estar à vista do princípio da minimização dos dados (em grosso modo, utilizar a menor quantidade possível e garantir a anonimização dos dados), além de oferecer medidas de *accountability*, de modo que a prestação de contas e a transparência quanto à aplicação dessas tecnologias se torne factível.

Dispositivos legais, medidas técnicas e valores éticos surgem como norteadores das futuras cidades inteligentes. O papel do Direito é valorar novos sistemas que possam produzir externalidades em sociedade, positivos ou negativos, mas sempre de modo a respeitar novos entendimentos e visões.

Essa perspectiva é fundamental para evitar ações precipitadas que possam causar efeitos deletérios ao mercado como ocorreu nos Estados Unidos. As cidades de São Francisco, Somerville e Oakland baniram o uso de sistemas de reconhecimento facial por parte do poder público[27], Boston[28] e Portland (que inclusive estendeu a proibição para empresas privadas que utilizam em espaços públicos[29]) também decidiram no mesmo sentido.

Essas ações súbitas, cuja consequência a longo prazo não foi substancialmente considerada, podem impedir frutíferos resultados do uso dessas aplicações para os setores urbanos, na medida que novas pesquisas e resultados surgem. Tecnologias emergentes devem ser reguladas e balizadas pelo Poder Legislativo e pelas agências reguladoras, isto é, o Direito deve se empenhar em obstaculizar as externalidades negativas e não inibir as novas tecnologias de tal forma que as externalidades positivas não consigam se projetar.

---

[25] *Facial Recognition: for a debate living up to the stakes.* **CNIL.** 15 nov 2019. Disponível em: https://www.cnil.fr/en/facial-recognition-debate-living-challenges. Versão em Francês: https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf. Acesso em: 25 nov 2020

[26] Entendimento de que a privacidade deve ser aplicada desde o início da formulação de aplicativos. Medidas de transparência devem estar intrínsecas à engenharia do programa. (CAVOUKIAN, 2012)

[27] Oakland Becomes Third U.S. City to Ban Facial Recognition. **VICE**. 17 jul. 2019. Disponível em: https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz. Acesso em: 22 nov. 2019

[28] Boston City Council votes to ban facial-recognition technology. 24 jun. 2020. Disponível em: https://www.bostonherald.com/2020/06/24/boston-city-council-votes-to-ban-facial-recognition-technology/. Acesso em 25 nov. 2020

[29] Portland passes broadest facial recognition ban in the US. Disponível em: https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html. Acesso em 25 nov 2020.

O Brasil, como previamente mencionado, já utiliza instrumentos de reconhecimento facial com vistas a desenvolver o poder de polícia. Esses instrumentos projetaram externalidades positivas (como a captura de dezenas de criminosos e um melhor oferecimento de cadastro de previdência aos aposentados, por exemplo), ao passo que também são passíveis de projetar externalidades negativas (como o caso do Rio de Janeiro que uma mulher foi detida por erro do sistema).

A LGPD, contudo, garante que essas aplicações sejam observadas, de modo a preservar a autonomia do indivíduo. A utilização do reconhecimento facial pode ser efetiva respeitando os princípios da lei, em especial a não discriminação, adequação e necessidade. Embora a lei não se debruce estritamente sobre a utilização dessas técnicas, já dispõe sobre o tratamento de dados pessoais sensíveis que, com observado, são os dados em que sistemas de reconhecimento facial realizam tratamento (dados biométricos). Esse tratamento deverá adotar técnicas de anonimização que, embora não sejam completamente seguras, devem servir a fim de que não deixam que com esforços razoáveis possam se detectar seus titulares

A Agência Nacional de Proteção de Dados (ANPD), em suas prerrogativas, pode dispor sobre quais os melhores parâmetros e técnicas que podem ser adotados no processo de anonimização dos dados (art.12, § 3º, LGPD), assim como promover ações sobre a publicidade das operações que envolvam o tratamento de dados pessoais sensíveis (art. 55-J, X, LGPD), editando relatórios de impacto sobre o risco do tratamento dos dados biométricos – recomendando a avaliação humana após decisão automatizada, por exemplo – (art. 55-J, XII, LGPD) e inclusive fiscalizando o poder público sobre o uso das técnicas de reconhecimento facial (art. 55-J, XI, LGPD).

O art. 4º da LGPD necessita de notada atenção, pois preconiza que, em algumas hipóteses, a lei não resguardará o tratamento de dados, como naquela em que o tratamento de dados pessoais ocorra para fins exclusivos de segurança pública, defesa nacional ou segurança do Estado. A vigência da ANPD (que ainda não está oficialmente implementada) é de extrema importância para garantir melhor entendimento sobre o dispositivo legal, isto é, se o uso de reconhecimento facial por agentes públicos poderia se valer desse artigo para estar além do alcance da LGPD.

Não significa, porém, que, se o uso do sistema estiver compatível com o artigo 4º da lei, o poder público poderá realizar o tratamento indiscriminado dos dados pessoais sensíveis dos cidadãos: a inviolabilidade da intimidade, da vida privada, honra e imagem dos indivíduos é prerrogativa constitucional (art. 5º, X, Constituição da República Federativa do Brasil de 1988).

6. CONCLUSÃO

A discussão iniciada buscou traçar os fatores pelos quais potencializam a transição de uma cidade ordinária para uma cidade inteligente. A despeito disso, a literatura aponta uma série de fatores que fomentam essa característica, de modo que o presente artigo não buscou esgotá-la, mas objetivou adotar a posição da União Europeia que preconiza que uma cidade inteligente busca recepcionar, em uma relação plural com todos os atores urbanos, sistemas de TICs para a solução de gestão.

Depreende-se, desse primeiro objetivo, que uma cidade não pode ser considerada inteligente somente quando todos os setores urbanos estão integrados em uma utilização de serviços de tecnologia da informação e comunicação. Do contrário, os serviços de TICs podem ser aplicados somente a um setor específico.

Diante desse panorama exploratório, observou-se que esses instrumentos são aplicados pelo setor público desempenhando função de polícia, isto é, a partir de sistemas de reconhecimento facial, a vigilância estatal resulta em fatores positivos, mas têm potencialidade de causar lesões sociais.

A utilização desses mecanismos requer necessariamente o tratamento de dados biométricos que são dados sensíveis, cujo manuseio tem capacidade de servir como meio discriminatório com grupos vulneráveis da sociedade, pois podem parodiar padrões sociais discriminatórios e não há comprovação de que são totalmente eficazes.

As bases normativas da LGPD não obstam o uso dessas soluções pelo setor público ou privado, pelo contrário, o Estado poderá inclusive realizar o tratamento de dados biométricos sem o consentimento de seu titular para fins de proteção da vida dos cidadãos ou para o exercício de políticas públicas, por exemplo.

Argumentar-se-ia, a partir do artigo 4º do dispositivo legal, que a utilização de sistemas de reconhecimento facial se enquadraria na hipótese do inciso II, alínea b, da lei, de modo que não se aplicaria a LGPD nesses casos. Tal diploma deve ser compreendido à luz dos direitos

fundamentais estabelecidos na Constituição Federal, de forma que a aplicação do sistema não poderá violar direitos e garantias fundamentais.

A viabilidade de tal proposta, a fim de que se garanta maior relevância à privacidade dos cidadãos, deve dar prioridade para a anonimização e menor utilização dos dados pessoais em consonância com os princípios da adequação e necessidade.

Por fim, a ANPD deve indicar quais as melhores técnicas de anonimização dos dados que os governos estaduais e federal podem se valer para garantir, sempre que possível, o anonimato dos dados biométricos, ao passo que a ANPD poderá fiscalizará sua utilização. Nesse sentido, o Brasil pode se espelhar nas autoridades de dados sueca e francesa para dispor como o governo brasileiro pode adotar os mecanismos de reconhecimento facial com vistas a evitar utilizações desnecessárias e abusivas da técnica, que, inclusive, a depender do uso equivocado, leva uma cidade a transitar de um potencial em desenvolvimento para uma condição de ininteligência.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRA CUNHA, Maria; PRZEYBILOVICZ, Erico; FERNANDA MEDINA MACAYA, Javiera; BURGOS, Fernando. SMART CITIES: Transformação digital de cidades. **Fundação Getulio Vargas, FGV-EAESP**, ano 2016, ed. 1ª edição, p. 1-164, 4 jan. 2016. Disponível em: https://ceapg.fgv.br/sites/ceapg.fgv.br/files/u60/smart_cities_bra_versao_final.pdf. Acesso em: 20 nov. 2020.

BRASIL. Constituição da República Federativa do Brasil de 1988. Constituição Federal de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 25 nov. 2020

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: 22 nov. 2020.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Gender Shades, Conference on Fairness, Accountability, and

Transparency, p. 1-15, 2018. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 22 nov. 2020.

Cavoukian, Ann "Privacy by Design [Leading Edge]," in IEEE Technology and Society Magazine, vol. 31, no. 4, pp. 18-19, winter 2012, doi: 10.1109/MTS.2012.2225459.

CUI, Lei; GAO, Longxiang; XIE, Gang; QU, Youyang; YANG, Yunyun. Security and Privacy in Smart Cities: Challenges and Opportunities. **IEEE Access.** Vol 6, 2018. Doi: 10.1109/ACCESS.2018.2853985.

Directorate General For Internal Policies. Mapping Smart Cities In The EU. **European Union, p.** 1-200, 2014. Disponível em: Https://www.europarl.europa.eu/regdata/etudes/etudes/join/2014/507480/IPOL-ITRE_ET(2014)507480_EN.Pdf. Acesso em: 21 nov. 2020.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados. São Paulo: Revista dos Tribunais, 2019.

E. JOH, Elizabeth. Policing the smart city. **International Journal of Law in Context**, 2019. Cambridge University Press 2019, p. 177-182. Doi:10.1017/S1744552319000107.

Eubanks, Virginia. Automating Inequality**:** How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press, 2018.

EUROPEAN UNION LAW. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 25 nov. 2020

IM CHO, Young. Designing Smart Cities: Security Issues. In: Cortesi A., Chaki N., Saeed K., Wierzchoń S. (eds) Computer Information Systems and Industrial Management., Lecture Notes in Computer Science, v. 7564. 2012. https://doi.org/10.1007/978-3-642-33260-9_2

LAUFS, Julian; BORRION, Hervé; BRADFORD, Ben. Security and the smart city: A systematic review. **Sustainable Cities and Society** v. 55, n. 2020, p. 1-18, abr. 2020. DOI https://doi.org/10.1016/j.scs.2020.102023.

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

NAJIBI, Alex. Racial Discrimination in Face Recognition Technology. **Harvard University**, [*S. l.*], p. S.I, 24 out. 2020. Disponível em: http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/. Acesso em: 22 nov. 2020.

Pasquale, Frank. **The Black Box Society:** The Secret Algorithms That Control Money and Information. Cambridge, Massachusetts. London, Harvard University Press, 2015.

SADGALI, Imane; SAEL, Nawal; BENABBOU, Faouzia. Detection of credit card fraud: State of art. **International Journal of Computer Science and Network Security.** Vol. 18 No.11. P. 76 - 83. 2018.

THODORIS ANAGNOSTOPOULOS, Theodoros. 2014. A Surveillance System for Preventing Suicide Attempts in Urban Metro Stations. In Proceedings of the 18th Panhellenic Conference on Informatics. Association for Computing Machinery. 1–6. https://doi.org/10.1145/2645791.2645806

WELSH, David; ROY, Nirmalya. Smartphone-based Mobile Gunshot. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops, pp. 244-249, Kona, HI, doi: 10.1109/PERCOMW.2017.7917566.