“SMART CITY”: entre os riscos da celebração antecipada da computação ubíqua e as liberdades individuais

“SMART CITY”: between the risks of the early celebration of ubiquitous computing and individual freedoms

Alex Mecabô[1]

Pedro Teixeira Gueiros[2]

Recebido/Received: 24.02.2023/Feb 24th, 2023

Aprovado/Approved: 11.04.2023/Apr 11th, 2023

> Uma vez que o espaço se desenvolve na época global sobretudo de maneira digital, ocorre também a localização digital. Para a formação e ampliação do poder seria preciso então uma apropriação digital de terras, um ganho digital de espaço. Em relação à lógica do poder, não há diferença essencial entre localização terrestre e digital” (HAN, 2019, p. 174).

RESUMO: Os fascínios em torno das soluções implementadas em cidades inteligentes encontram abrigo na ideia de uso progressivo e intenso das tecnologias para melhorar a qualidade de vida humana. Mas em que medida estas soluções incutidas em processos tecnológicos foram programadas para, efetivamente, aderir à legislação e à proteção das liberdades individuais? No ecossistema urbano, diversos são os exemplos eloquentes quanto os impactos que a digitalização repercurte sobre ambientes densamente povoados. O presente artigo se propõe a investigar os possíveis riscos decorrentes da utilização de tecnologias avançadas empregadas nas denominadas *smart cities*, particularmente, no tocante à proteção dos dados pessoais e potenciais repercussões discriminatórias provocadas pelo uso de aprendizado de máquina. Conclui-se, ao fim, que para que seja funcional, a inteligência projetada às cidades deve ser precedida, além de uma regulação eficaz, de mecanismos de conformidade e adequação desde a concepção, de modo a garantir um diálogo harmonioso entre o oportuno progresso técnico-científico e a proteção de direitos fundamentais.

PALAVRAS-CHAVE: smart city; algoritmos; proteção de dados pessoais; privacidade; discriminação.

[1] Mestre em Direito das Relações Sociais pela UFPR. MBA em Business Law pela FGV. Graduado pela Faculdade de Direito de Curitiba. Membro do Grupo de Estudos de Direito Autoral e Industrial – GEDAI/UFPR. Advogado. Currículo Lattes: http://lattes.cnpq.br/6771160643840272. E-mail: aleex.m@hotmail.com

[2] Mestre em Direito Civil Contemporâneo e Prática Jurídica pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio). Bolsista de mestrado pela Fundação alemã Konrad Adenauer no Brasil. Advogado Orientador do Núcleo de Prática Jurídica (NPJ) do Ibmec-RJ. Pesquisador de Direito e Tecnologia no Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio). Integrante do Legalite (PUC-Rio). Graduado em Direito pelo Ibmec-RJ. Advogado. Currículo Lattes: http://lattes.cnpq.br/3185404403050883. E-mail: pedrogueiros@uol.com.br

ABSTRACT: The fascination around the solutions implemented in smart cities finds shelter in the idea of progressive and intense use of technologies to improve the quality of human life. But to what extent were these solutions embedded in technological processes programmed to effectively adhere to legislation and the protection of individual freedoms? In the urban ecosystem, there are several eloquent examples of the impacts that digitization has on densely populated environments. This article proposes to investigate the possible risks arising from the use of advanced technologies employed in the so-called smart cities, particularly with regard to the protection of personal data and potential discriminatory repercussions caused by the use of machine learning. In the end, it is concluded that, in order to be functional, the intelligence designed for cities must be preceded, in addition to effective regulation, by conformity and adequacy mechanisms from conception, in order to guarantee a harmonious dialogue between timely technical-scientific progress and the protection of fundamental rights.
KEYWORDS: smart city; algorithms; personal data protection; privacy; discrimination.

INTRODUÇÃO

Em meio ao intenso progresso técnico-científico dos últimos anos, a tônica em torno das atuais soluções tecnológicas parece estar sendo progressivamente alterada. Sob um franco desenvolvimento da computação ubíqua[1], os objetos passaram a estar cada vez mais conectados, interoperáveis e, sobretudo, *smarts*. A sofisticação dos recursos movidos à Inteligência Artificial (IA), em um contexto de Internet das Coisas (IoT)[2], pretexta tornar a vida humana mais facilitada do ponto de vista micro ao macro, como se constata em (i) geladeiras que elaboram listas de itens em falta e automaticamente encaminham solicitações de compra ao supermercado; (ii) relógios que monitoram dados calóricos, quilometragens percorridas e informações cardíacas do usuário; (iii) casas conectadas (*smart homes*), controladas à distância por comandos de celulares; e (iv) até verdadeiras cidades "inteligentes".

Embora não se tenha uma definição exata do que venha a ser uma "cidade inteligente", estas podem ser identificadas como o lugar onde redes, sistemas e serviços se tornam mais eficientes por meio do uso de soluções digitais em benefício

[1] O termo "computação ubíqua" foi originalmente cunhado pelo cientista da computação Mark Weiser em 1991, para descrever o potencial do aperfeiçoamento de computadores com conexão onipresente, que chegariam ao ponto de serem mais universais, menos perceptíveis e mais integrados à vida humana.

[2] Acrônimo em inglês para *Internet of Things*. O termo foi originalmente cunhado pelo pesquisador Kevin Ashton do *Massachusetts Institute of Technology* (MIT), em 1999, para descrever uma série de objetos físicos dotados de sensores que poderiam ser interconectados por meio da Internet.

dos habitantes e negócios (EUROPEAN COMMISSION). Ao contrário do que o senso comum possa inferir, cidades inteligentes não são exemplos distópicos ou futuristas. Em maior ou menor escala, elas já existem e são capazes de inovar a governança de tecidos urbanos, por meio da eficiência, resiliência e sustentabilidade de setores como educação, moradia, transporte, saúde, segurança, dentre tantos outros tantos aspectos nucleares à existência nos grandes centros (KITCHIN, 2015). Casos bem-sucedidos revelam como os investimentos trouxeram melhorias socioeconômicas a diversas localidades[1].

Para entender o universo de possibilidades para a construção de uma cidade inteligente, examina-se a seguir alguns exemplos adjetivados como soluções *smarts*. Como será observado, grandes avanços nessa seara implicam em responsabilidades igualmente notórias, especialmente em se tratando de ambientes plurais, diversos e complexos, como todo centro urbano. A forma com que as tecnologias avançadas são manejadas pode refletir no desenvolvimento efetivo da formação de cidades, não apenas mais "espertas" do ponto de vista técnico, como também funcionais à pessoa humana.

Sob essas circunstâncias, o presente artigo apresentará um paranoma acerca dos riscos, desafios e oportunidades decorrentes da pretensa acepção de tornar as cidades *smart*. No primeiro tópico, será apresentado um conceito de *smart city*, consignando alguns exemplos extraídos do relatório anual produzido pelo *Institute for Management Development* em parceria com a *Singapore University for Technology and Design* (SUTD).

No segundo e terceiro tópicos, já sob um olhar dos possíveis riscos decorrentes da hiperconectidade, serão abordados os contornos da *black box* algortímica, como um fenômeno de vigilância on-line promovido a partir da coleta e manipulação de dados pessoais diversos. Na sequência, no quarto e quinto tópicos, serão indicados alguns exemplos de danos à segurança, inclusive física, em que a conectividade irrestrita de equipamentos do dia a dia pode causar. No sexto tópico, aborda-se a problemática da conduta potencialmente discriminatória do uso de Inteligências Artificiais (IAs), de modo a revelar como prejuízos consideráveis são experimentados pela população em geração, particularmente em razão da

[1] Ilustrativamente, Curitiba aparece como verdadeira capital ecológica, possuindo diversos parques com áreas verdes em diversos pontos. A capital paranaense também é destaque como cidade inteligente, pois possui sistema de coleta seletiva que fomenta a separação de lixo, oferecendo programas de reciclagem (DORE, 2020).

implementação afoita de tecnologias de hiperconexão sem um arcabouço regulatório eficaz.

1 O QUE TORNA UMA CIDADE INTELIGENTE

Diante de tantos fatores aptos a tornar uma cidade inteligente, não faltam iniciativas voltadas à parametrização sobre quais localidades promovem realmente uma associação *smart* entre a tecnologia e a vivência urbana. O relatório anual produzido pelo *Institute for Management Development* em parceria com a *Singapore University for Technology and Design* (SUTD) classifica cidades como inteligentes, com base em dados econômicos e tecnológicos, levando também em conta as percepções de seus habitantes.

Singapura constantemente encabeça a listagem. A Cidade-Estado insular tem uma população envelhecida e um governo focado em desenvolver tecnologias digitais e iniciativas para aumentar a produtividade da economia. Isso incluiu a implantação de sistema de saúde digital - normalizando as consultas médicas por vídeo antes mesmo das tendências introduzidas pela crise epidemiológica causada pela Covid-19 -, bem como a há a popularização de dispositivos IoT para monitorar pacientes remotamente. O país asiático é densamente povoado e sua visão *smart* visa coletar informações diversas usando sensores capazes de parametrizar e monitorar desde a limpeza de uma determinada área até a lotação de um evento (NEC, 2022).

Oslo é uma outra cidade inteligente, bastante focada na criação de um ambiente sustentável e ecologicamente correto. Com mais de 650.000 luzes LED conectadas a estações de processamento, a iluminação na capital norueguesa oscila conforme a necessidade da região, reduzindo, ao fim, o consumo energético. Além disso, o governo local monitora carros usando pequenos detectores de placas para entender o fluxo de tráfego pela cidade e desenvolver melhores práticas e orientações para gestão do congestionamento (NEC, 2022).

Em Nova York, centenas de sensores inteligentes foram colocados em diferentes distritos como parte de um projeto piloto de cidade inteligente. O programa coleta volumosas quantidades de dados para ajudar a gerenciar serviços essenciais em toda a região, incluindo coleta de resíduos. A cidade também está melhorando a conectividade para os cidadãos, substituindo cabines telefônicas por

estações de carregamento que também são habilitadas com redes Wi-Fi (NEC, 2022).

Sob a ótica da segurança pública, o departamento de polícia da maior cidade estadunidense testou um polêmico[1] software (HunchLab) que cruza e avalia dados históricos de crimes, informações geográficas das áreas e outros elementos para prever e responder a eventuais delitos. O teste produziu resultados com uma redução acentuada em ações violentas (NEC, 2022).

Já no campo da otimização de soluções burocráticas, Nova York também trouxe bons exemplos. A Organização Não-Governamental (ONG) 596 Acre[2] oferece um programa com mapas interativos e em tempo real que compila dados de terrenos públicos existentes, sua utilização, destinação e sob qual órgão está sendo administrado. Em uma das cidades mais ricas e densamente povoadas do mundo, erguida sob um contexto de intensa gentrificação e marginalização de comunidades mais pobres[3], a medida parece ser acertada.

Na cidade de São Paulo, o ambicioso projeto GeoSampa oferece propostas semelhantes em torno dos imóveis existentes (PREFEITURA DE SÃO PAULO). Por meio da publicização de dados cadastrais junto ao Imposto Territorial e Predial Urbano (IPTU), disponibilizam-se informações relativas ao nome dos proprietários, metragem, tipo de construção, uso etc. A perspectiva se mostrou eficaz na verificação de corrupção e identificação de crimes como lavagem de dinheiro em contratos de compra e venda da capital paulista (ANTONIALLI; KIRA, 2020, p. 7).

---

[1] De acordo com informações: “In two law review articles I have detailed the distorting effects of predictive policing and big data on the Fourth Amendment and have come to the conclusion that insufficient attention has been given at the front end to these constitutional questions. New York has the chance now to address these issues before the adoption of the technology and should be encouraged by the same civil libertarians and ordinary citizens who challenged the stop and frisk policies. Progress is good. Police obtaining more information to stop and solve crimes is a social good. But questions need to be asked and answered to make sure worthwhile predictive innovations have adequate transparency, accountability, and process protections built into the system. As the NYPD rolls out this new plan, I hope those tasked with implementing the policy do not replace one legally discredited practice of hunch-based stops with an automated HunchLab system only to find themselves facing similar legal challenges to the fairness and effectiveness of this policing strategy” (FERGUSON, 2016).

[2] A teor dos objetivos desenvolvidos: “596 Acres builds tools to help neighbors see vacant lots as opportunities and create needed green spaces that become focal points for community organizing and civic engagement. We turned our original online map into a sophisticated interactive organizing tool, Living Lots NYC, which provides information about vacant land across NYC and is supported by signs and other print materials. These materials go hand in hand with our ongoing organizing and advocacy work” (596 ACRES).

[3] A título de ilustração, como se verifica de reportagem investigativa da Vox, nota-se que o célebre Central Park em Nova York foi construído em 1853 sob um bairro periférico ocupado pela população negra, conhecido como Seneca Village, destruído sem qualquer justa indenização ou reparação histórica (CHAKRABORTY, 2020).

Não é demais sublinhar que, especialmente no tocante à regulação do uso e destinação da propriedade privada, o ecossistema das cidades inteligentes pode ser capaz de projetar mudanças essenciais à transparência e à gestão de terrenos e logradouros, públicos e privados (PARENTI; NOORI; JANSSEN, 2022).

Alimentada pela corrida regulatória de implementação do 5G no Brasil, nota-se uma verdadeira expansão destas soluções em potenciais cidades inteligentes brasileiras. As medidas, que vão desde as mais arrojadas, até mais simples, parecem encontrar terrenos férteis, impulsionadas pelas promessas da qualidade de sinal 5G, dentre elas, a melhora na velocidade de Internet, conexão massiva de dispositivos e baixa latência do sinal de transmissão. Sob esse prospero cenário, o universo de aparelhos inteligentes se torna ainda mais acessíveis e com menores custos (EXAME, 2021).

A despeito desses benefícios prometidos ou já introduzidos nas cidades, há se destacar, todavia, a existência de graves riscos e prejuízos com a popularização da computação ubíqua. À luz de tais circunstâncias, passa-se ao exame das principais preocupações observadas na tendência de uso progressivo de novas tecnologias e soluções nas cidades, traçando seus impactos à qualidade de vida da população.

2 AS ADVERSIDADES POR DETRÁS DE ALGUMAS CIDADES INTELIGENTES

Em 2017, o Washington Post informou que 70% dos dispositivos de armazenamento que registravam dados de câmeras de vigilância da polícia de Washinton D.C. haviam sido infectados com *ransomwares*. O ataque cibernético deixou a polícia local incapaz de gravar grande parte dos perímetros da cidade entre os dias 12 e 15 de janeiro daquele ano, na medida em que a invasão do sistema afetou 123 dos 187 gravadores de vídeo em rede municipal, com danos diretos à segurança pública local (WILLIAMS, 2017).

No mesmo ano, o USA Today publicou que as telas de exibição de informações na estação de metrô da capital estadunidense haviam sido hackeadas. Em razão disso, foram reproduzidos vídeos com conteúdos pornográficos durante a hora do *rush* – em um local público também frequentado por crianças e adolescentes. Ao ser constatada a invasão hacker, os monitores foram rapidamente

desligados, mas as autoridades não compartilharam detalhes sobre a extensã, tampouco as razões do incidente de violação de segurança (MUNTEAN, 2017).

Em outro caso ainda mais grave, um grupo de pesquisadores universitários descobriu a facilidade de hackear carros autônomos. Os acadêmicos analisaram a classificação de imagens de algoritmos usada por sistemas de visão em carros autônomos e, em seguida, manipularam placas de rua usando adesivos para enganar os modelos de aprendizado. Em um teste, o sistema de visão interpretou um sinal de “pare” como uma indicação de velocidade máxima de 45 milhas por hora. As consequências de um ataque cibernético tão simples podem ser devastadoras no mundo real, especialmente em um momento de estímulo à utilização de condução semiautônoma em muitos veículos rodoviários (SNYDER, 2017).

Infere-se a partir desses breves exemplos que a irrefreável transformação em curso para que cidades inteligentes sejam implementadas exige cautela, testagem e ponderação. Procedimentos e adoção de medidas preventivas dessa natureza são elementares para que a convergência entre digitalização e urbanização se opere em alinho à proteção dos direitos individuais e segurança coletiva.

Sob essas circunstâncias, minudenciam-se, adiante, alguns riscos e reflexões prévias a quaisquer operações envolvendo a coleta e gestão de dados pessoais, em especial sob contextos de massa como no caso de cidades inteligentes. Tendências e soluções por mais inovadoras e arrojadas que sejam, sem o devido processo de adequação e conformidade à tutela dos dados pessoais são capazes de alavancar fenômenos deletérios, a exemplo da *black box* algorítmica, ao provocar o desconhecimento dos parâmetros usados para formação do aprendizado de máquina nas Ias (BRAUNEIS; GOODMAN, 2018).

3 *BIG DATA* E A *BLACK BOX* ALGORÍTMICA NAS CIDADES

Como citado, para que a sustentabilidade e o progresso permaneçam inerentes ao desenvolvimento das cidades inteligentes, deve-se ter atenção e cautela à curadoria e organização das novas formas de tecnologia empregadas[1].

[1] Particularmente com relação aos atores privados, Piovesan e Gonzaga destacam como a responsabilidade empresarial atual envolve por essência a efetiva adoção de direitos humanos: “Em uma arena cada vez mais complexa, fundamental é avançar na afirmação da responsabilidade das

A *International Data Corporation* estima que haverá no mundo 55,7 bilhões de dispositivos IoT conectados até 2025, gerando quase 80 bilhões de zettabytes (ZB) de dados (IDC, 2021).

Por essa razão, em primeiro lugar, é imprescindível observar o tratamento adequado de dados pessoais existentes em meio ao intenso fluxo informacional das cidades inteligentes. Afinal, a coexistência das esferas públicas e privadas depende essencialmente da respectiva exposição ou ocultação de aspectos da vida humana (ARENDT, 2004, p. 84). A perspectiva de massiva coleta e compartilhamento de dados pessoais, recrudescida por sistemas avançados de IAs, como câmeras de reconhecimento facial, carros autônomos e programas de autenticação biométrica são capazes de gerar espaços de maior monitoramento e vigilância.

Em outras palavras, o estímulo à descomedida digitalização nas cidades somado à extensa (e pontecialmente vulgarizada) coleta e compartilhamento em rede de dados pessoais, pontecializa a criação de uma vigilância duradoura e progressiva. A partir disso, inseridas sobre o universo de IoT e por demais tecnologias utilizadas para viabilizar cidades inteligentes), são patentes os elevados riscos ao exercício das liberdades individuais, ameaçando a necessária democratização do acesso a direitos básicos.

Na China, a título ilustrativo, vigora denominado *Social Credit System*. Trata-se de um ambicioso projeto voltado verdadeiramente categorizar e ranquear coletivamente pessoas naturais e jurídicas, estimulado especialmente pelas informações eminentemente pessoais coletadas diuturnamente nas cidades inteligentes[1]. Inclusive, o sucesso no combate em tempo recorde dos casos de contaminação durante a pandemia da Covid-19, esteve diretamente associado ao uso obrigatório de um aplicativo de celular, que rotulava indivíduos como

empresas em matéria de direitos humanos, a compor uma nova arquitetura, capaz de responder aos desafios da agenda contemporânea, da nova dinâmica de poder e da necessária transformação da cultura corporativa com a incorporação do *human rights approach*, em um crescente quadro de responsabilidades compartilhadas" (PIOVESAN; GONZAGA, 2018, p. 110).

[1] Sobre o processo de funcionamento do sistema de crédito social chinês, "é possível identificar três pontos nevrálgicos de sua funcionalidade sistêmica. Primeiramente, há um massivo compartilhamento de dados, compilados a uma base central. A seguir, tem-se as subjetivas avaliações sociocomportamentais de indivíduos, de modo a classificá-los em dicotômicas listas, boas e ruins. Por fim, consoante as rotulações estabelecidas nas listas, aplicam-se os instrumentos de punições e recompensas, regulando a efetiva participação e acesso de indivíduos à cidadania. O sistema se retroalimenta por constantes coletas e requalificações dos dados, angariados sem quaisquer consentimentos, deforma aleatória e difusa. Subsiste uma temerária tentativa chinesa em definir conceitos obscuros de boa cidadania. Como resultado, tem-se a uma sociedade de desempenho voltada à autoexploração dos indivíduos" (RITO; GUEIROS, 2020, p. 203).

possivelmente infectdos ou não com o vírus SARS-CoV-2. A despeito das diversas denúncias de erro e falta de acuracidade dos algoritmos empregados no *App*, cidadãos eram estigmatizados com cores (verde, amarelo e vermelho) em alusão aos semáforos de trânsito, definindo se poderiam ou não sair de casa (MOZUR; KROLIK, 2021).

4 O ATUAL ESTADO DE VIGILÂNCIA NO CONTEXTO NACIONAL

No Brasil, como bem estabelece a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD), sabe-se que os dados pessoais devem ser tratados nas expressas bases legais definidas na normativa[1], em atenção à existência de dados pessoais sensíveis, bem como observando os pressupostos quanto à tutela de crianças e adolescentes[2]. A normativa também aponta para a exigência de documentos jurídicos relevantes ao *compliance* de dados, como o Mapeamento dos Registros das Operações de Tratamento (RoPA)[3], o Relatório de Impacto à Proteção de Dados (RIPD)[4] e a Avaliação dos Riscos do Legítimo Interesse (LIA)[5].

Mas será que a simples previsão quanto à obrigação legal seria capaz de mitigar os riscos decorrentes de uma coleta irrestrita de dados pessoais, sobretudo em ambientes públicos? Ademais, como operacionalizar um tratamento aderente às hipóteses previstas nos arts. 7º e 11 da LGPD, em contextos de hiperconexão e popularização das cidades inteligentes? Essas indagações têm desafiado o Poder Judiciário.

Recentemente, o Supremo Tribunal Federal (STF) julgou a Ação Direta de Inconstitucionalidade (ADI) n. 6649, ajuizada pela Ordem dos Advogados do Brasil e pelo Partido Socialista Brasileiro, que sustentavam a inconstitucionalidade do Decreto n. 10.046/19. Em apertada síntese, a medida instituída pela Administração Pública federal visava criar o Cadastro Base do Cidadão, capaz de instituir um massivo banco de dados da população brasileira, de certa forma, similar ao que já existe na China. As finalidades não apenas não eram claras e objetivas, como

[1] A teor dos arts. 7º e 11, LGPD.
[2] Consoante art. 14, LGPD.
[3] Nos termos do art. 37, LGPD.
[4] Conforme arts. 5º, XVII e 38, LGPD.
[5] Com base nas recomendações do art. 10, §2º, LGPD.

pretendiam compilar uma série de informações pessoais complexas, inclusive sensíveis, como atributos biométricos[1].

Nos termos da decisão proferida em sessão plenária da Corte, conduzida pelo voto do Min. Relator Gilmar Mendes, julgou-se parcialmente procedente as alegações de que o Decreto permitiria a instauração de uma vigilância massiva de dados (SUPREMO TRIBUNAL FEDERAL). A Corte Suprema, na oportunidade, reconheceu que para que se tenha o compartilhamento de dados necessários à criação do Cadastro Base, os órgãos da Administração Pública precisam adotar propósitos legítimos, específicos e explícitos ao tratamento de dados. Além disso, devem limitar o compartilhamento ao mínimo necessário e atendendo a todos os pressupostos dispostos na LGPD.

Outro caso relevante quanto às fronteiras entre espaço público e uso de dados é observado no caso envolvendo o metrô de São Paulo. O Tribunal de Justiça de São Paulo (TJSP) reconheceu, na Ação Civil Pública n. 1090663-42.2018.8.26.0100, a dificuldade de adaptação de uma tutela da proteção de dados pessoais em contextos de IoT. Na demanda, o IDEC (Instituto Brasileiro de Defesa do Consumidor) litigava com a Concessionária da Linha 4 do Metrô de São Paulo, por conta da implantação de portas de plataforma interativas, dotadas de sensores que reconhecem o gênero, a faixa etária e as emoções dos usuários expostos à publicidade veiculada, inclusive comercial[2].

O caso esboça como a problemática relativa ao uso de dados pessoais tem assumido uma postura sistêmica, com peculiaridades que diferem da acepção clássica de proteção dos espaços privados e liberdades individuais. As câmeras, equipamentos eletrônicos comuns (utilizados até mesmo por motivos de segurança, por exemplo), adquirem funcionalidades extraordinárias, gerindo dados que foram captados sem qualquer consentimento - ou até mesmo percepção - do usuário. A

[1] Para fins do disposto no art. 2º, II, do Decreto n. 10.046/19, atributos biométricos envolvem "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar".

[2] Nas palavras do próprio Instituto "O sensor é sempre posicionado acima de uma propaganda publicitária, para que a identificação da emoção ocorra quando o usuário do transporte público passa por ela, sendo possível captar os efeitos que ela produz sobre a população em geral. A prática, espécie de 'pesquisa de mercado automatizada' sem autorização do participante, permite a obtenção de receita a partir da venda desses dados para terceiros, que podem então direcionar suas estratégias de publicidade a partir das reações identificadas. De acordo com informações da própria Ré, mais de 350.000 pessoas acessam a Linha Amarela por meio das estações de metrô que possuem o sistema de 'portas interativas" (BRASIL, 2018).

ação, proposta perante a 37ª Vara Cível de São Paulo/SP, foi julgada procedente, com base nas normativas consumeristas, no Marco Civil da Internet e no direito à privacidade (MECABÔ, 2021):

> A situação exposta no caso concreto é muito diferente da captação de imagens por sistemas de segurança com objetivo de melhoria na prestação do serviço, segurança dos usuários ou manutenção da ordem, o que seria não só aceitável, mas necessário diante da obrigação da fornecedora de serviço público zelar pela segurança de seus usuários dentro de suas dependências. É evidente que a captação da imagem ora discutida é utilizada para fins publicitários e consequente cunho comercial, já que, em linhas gerais, se busca detectar as principais características dos indivíduos que circulam em determinados locais e horários, bem como emoções e reações apresentadas à publicidade veiculada no equipamento. Ademais, restou incontroverso que os usuários não foram advertidos ou comunicados previa ou posteriormente acerca da utilização ou captação de sua imagem pelos totens instalado nas plataformas, ou seja, os usuários nem mesmo tem conhecimento da prática realizada pela requerida, o que viola patentemente o seu direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, ambos elencados no artigo 6º, III e IV do Código de Defesa do Consumidor. Por sua vez, o artigo 31 do mesmo diploma legal estabelece que "A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores." Não se olvide que, na qualidade de concessionária de serviço público, incumbia à requerida arcar com o risco das atividades econômicas por si exploradas, especialmente por envolver os direitos fundamentais à intimidade, à privacidade, à imagem e à honra (art. 5º, X da Constituição Federal), o que não ocorreu, vez que utilizada as imagens dos usuários coletadas durante a prestação do serviço público para fins comerciais. De todo o exposto, inegável que conduta da requerida viola patentemente o direito à imagem dos consumidores usuários do serviço público, as disposições acerca da proteção especial conferida aos dados pessoais sensíveis coletados, além da violação aos direitos básicos do consumidor, notadamente à informação e à proteção com relação às práticas comerciais abusivas, daí porque o pedido de obrigação de não fazer consistente em não se utilizar de dados biométricos ou qualquer outro tipo de identificação dos consumidores e usuários do transporte público, sem a comprovação do devido consentimento do consumidor é procedente (BRASIL, 2018).

A controvérsia, acompanhada por outras semelhantes[1], é emblemática. Porquanto, denota a complexidade das tecnologias envolvidas em soluções *smart* e as consequentes dificuldades de ajustes de tais apetrechos interconectados aos requisitos previstos na Lei (MECABÔ, 2021).

[1] Cite-se, neste sentido, o inquérito civil público proposto em face do *Facebook*, para analisar a legalidade da tecnologia de reconhecimento facial de usuários e não usuários da plataforma – Portaria n. 09/2018, Ministério Público do Distrito Federal. Também a Ação civil pública n. 1006616-14.2020.8.26.0053, em trâmite perante a 1ª Vara da Fazenda Pública de São Paulo.

5 CIDADES INTELIGENTES, MAS RESPONSÁVEIS

Além das compreensíveis preocupações quanto à excessiva vigilância, no que toca à coleta massiva de informações pessoais, outro desafio emerge às potencialidades das cidades inteligentes. Torna-se salutar o desenvolvimento de infraestruturas de segurança robustas nos bancos de dados de armazenamento – o que, por vezes, torna a solução impraticável do ponto de vista financeiro.

Apenas para ilustrar, uma pesquisa promovida pela *The State of Cloud Security*, de 2020, veiculada pela SOPHOS, sublinhou que no Brasil cerca de 80% das organizações consultadas sofreram incidentes de segurança na nuvem recentemente. A estatística é alarmante. Como defender os espaços privados e obstaculizar a ocorrência de crimes digitais quando toda uma infraestrutura de proteção das informações coletadas é comprometida? Como justificar a facilitação de tarefas do dia a dia, a partir de estratégias de cidades inteligentes, quando há riscos intensos de vazamento, acessos não-autorizados e até mesmo sequestro de bancos de dados?

Espraiar soluções *smart* em ambientes urbanos, principalmente em espaços públicos, exige um prévio alinhamento – e robustecimento – das estruturas de segurança. Nesse sentido, há toda uma lógica relevante de *privacy by design* (privacidade desde a concepção) – conceito formulado pela Comissária pela Proteção de Dados do Canadá, Ann Cavoukian (JIMENE, 2018, p. 173), que encoraja, por meio de sete princípios, uma atuação proativa e preventiva, com um dever de reflexão sobre a proteção de dados pessoais desde a criação de qualquer *software, hardware* ou aplicação (EVERSON, 2017).

Em sentido complementar, devido ao atual estado de constantes ameaças envolvendo incidentes de segurança, fala-se muito mais em resiliência cibernética[1] do que propriamente a simples adoção de medidas paliativas. Em atenção à própria principiologia da LGPD relativa à segurança e à prevenção, os sistemas devem estar prontos para os ataques e prontos para retornar ao *status quo ante* o mais rápido possível. Soluções como as *Privacy Enhancing-Technologies* (OFFICE OF THE

[1] Conforme definição mais acurada: “Resiliência cibernética é a capacidade de uma organização de transcender quaisquer estresses, falhas, perigos e ameaças aos seus recursos cibernéticos dentro da organização e seu ecossistema, de modo que a organização possa cumprir com confiança sua missão, capacitar sua cultura e manter sua maneira desejada de operar.” Trad. livre. (WORLD ECONOMIC FORUM, 2022).

PRIVACY COMMISSIONER OF CANADA, 2017), já oferecem métodos e sistemas que promovem a acuracidade no uso de dados, em paralelo à proteção da privacidade individual. São medidas que usam variados mecanismos criptográficos, técnicas de anonimização e pseudoanonimização capazes de convergir na integridade no uso responsivo de dados pessoais.

6 *SMART*, MAS TAMBÉM ANTIDISCRIMINATÓRIA

A capacidade de vigilância irrestrita germinada por dispositivos e projetos de cidades inteligentes pode ser a porta de entrada para prejuízos sistêmicos ainda mais sensíveis.

Sabe-se que soluções tecnológicas são viabilizadas, hoje, pelo uso de IAs. Baseadas nas noções de "aprendizagem, raciocínio, planejamento, percepção, compreensão de linguagem e robótica", aliada com noções de "matemática, lógica, filosofia, probabilística, linguística, neurociência e teoria da decisão" (PEIXOTO, 2019, p. 75), foi possível reduzir – por vezes anular – a essencialidade do componente humano na interpretação e extração de valor dos bancos de dados. Ou seja, com o uso delas, os dispositivos e equipamentos passam a ser capazes de aprender, prever tendências e concluir respostas, sem que isso tenha, necessariamente, a participação do intelecto humano.

A proposta parece atraente, mas um lado obscuro justifica a preocupação. Recentemente, o *Massachusetts Institute of Technology* divulgou dados de uma pesquisa, no mínimo, perturbadora: mecanismos de IA já seriam capazes de prever com precisão a raça autodeclarada dos pacientes, unicamente a partir de imagens de exames médicos (a exemplo de um raio-x). Essa é uma façanha que nem mesmo os profissionais mais experientes conseguem fazer, e não está claro como o modelo de aprendizado de máquina foi capaz de alcançar estas conclusões (GORDON, 2022). Já em 2018, outrossim, pesquisadores da Universidade de Stanford, desenvolveram uma IA que determinava com uma precisao de 81% (para homens) e 74% (para mulhres) a orientação sexual de pessoas, igualmente analisando apenas fotografias, como imagens da face. A acuracidade aumentava ainda para 91% e 83%, respectivamente, se fossem entregues ao menos cinco imagens de cada pessoa (KOSINSKI; WANG, 2018). Cumpre ressaltar que ambos os tipos de

informações (origem racial e vida sexual) são considerados dados pessoais sensíveis, à luz da LGPD.

Os episódios ilustram o fenômeno da *black box* algorítmica - uma metáfora utilizada para o ambiente emergente de *big data* atual. A hipótese é voltada à compreensão de a opacidade quanto ao funcionamento dos mecanismos e parâmetros de IA, por vezes são incompreensíveis ao próprio ser humano, seja com relação ao seu próprio desenvolver ou ao seu usuário final. Mas como pode um dispositivo realizar funções e dar respostas em que sequer o programador é capaz de esclarecer?

A matemática Cathy O'Neil, em complemento, identifica esse fenômeno como algoritmos de destruição em massa (O'NEIL, 2020, p. 8). Para ela, o uso de modelos automatizados e preditivos como um todo urgem por uma maior transparência para que sejam revelados "*os dados de entrada que estejam usando, bem como os resultados dos direcionamentos. E precisam ser abertos a auditorias. Trata-se de motores poderosos, afinal. Devemos ficar de olho neles*" (O'NEIL, 2020, p 337). Vale lembrar que, nos termos do art. 20 da LGPD, os titulares de dados têm o direito a obter a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados[1].

Um relatório da Anistia Internacional, intitulado *Xenofhobic Machines* revelou como 26 mil famílias, sobretudo de imigrantes turcos e marroquinos, ficaram sem acesso ao subsídio do Estado que lhes permitia manter os filhos com menos de 12 anos em creches ou estabelecimentos de ensino. Na origem, a causa foi a implementação de um algoritmo que avaliava previamente os pedidos endereçados ao Estado como potencialmente fraudulentos (SOARES, 2021).

O design deste algoritmo reforçou o viés institucional existente no vínculo entre raça, etnia e crime. Com isso, foi generalizado um padrão de comportamento

[1] Mulholland e Frajhof registram duas considerações a respeito do exercício desse direito: "A primeira refere-se ao fato de que a lei autoriza o pedido de revisão, mas isto não significa que, após a análise pelo controlador, o resultado final necessariamente será alterado. A segunda, reconhece à primeira vista, a discricionariedade da autoridade nacional para realizar a auditoria apenas quando o controlador se negar a fornecer as informações elencadas no parágrafo primeiro. A existência desta condição pode dar margem para que o controlador se negue a exercer a explicação com base em uma simples alegação de que seu código estaria protegido pelo segredo comercial ou industrial, pois sabe que a atuação da autoridade em auditar seu algoritmo será optativa. Por sua vez, caso a explicação concedida ao titular não seja suficientemente clara - impedindo que a pessoa seja capaz de compreender se houve ou não um tratamento discriminatório, ou o motivo pelo qual o algoritmo decidiu de uma maneira e não de outra-, parece que o titular de dados terá menos garantias do que se o controlador de dados tivesse meramente alegado a proteção do sigilo do seu algoritmo" (MULHOLLAND; FRAJHOF, 2019, p. 272).

para toda uma raça ou grupo étnico. Essas falhas discriminatórias foram reproduzidas por um mecanismo de autoaprendizagem e o resultado foi um extenso ciclo de classificação de cidadãos não holandeses como potencialmente fraudadores (ORMEROD, 2022).

No Brasil, o Departamento de Polícia do Ceará conta com sistemas de reconhecimento facial para identificar suspeitos. No início de 2022, o software foi amplamente criticado quando identificaram que foi utilizada uma foto de Michael B. Jordan, estrela afro-americana do filme “A Pantera Negra”, na lista de procurados da polícia por um tiroteio em massa que deixou cinco mortos na véspera do Natal (AMNESTY INTERNACIONAL, 2021). O episódio, apesar de esdrúxulo, revela os riscos em potencial do uso de soluções tecnológicas em contextos de segurança pública, trazendo urgência para uma disciplina legal da matéria.

No setor da saúde, de forma exemplificativa, onde também situações complexas de discriminação algorítmica já tomam protagonismo no debate público (SIMIONITE, 2020), observa-se uma maior intervenção regulatória em alguns países. A Food and Drug Administration (FDA) dos EUA, a Health Canada e a Agência Reguladora de Medicamentos e Produtos de Saúde do Reino Unido (MHRA) recentemente formularam princípios para aprendizado de máquina. De acordo com o entendimento, devem ser calibradas noções referentes à segurança, limitação na coleta de dados, utilização de componentes humanos em fases do processo, transparência e participação do titular dos dados na interpretação de resultados (FDA, 2021). São diretrizes importantes para ajustar o uso da IA, não apenas na área da saúde, mas como nos diversos segmentos inseridos no contexto de cidades inteligentes.

No Brasil, no entanto, o debate é ainda incipiente. Uma Comissão de juristas foi instituída pelo Congresso Nacional, a fim de formalizar subsídios à apresentação de um texto substitutivo aos Projetos de Leis (PLs) relativos à regulação (PLs 5.051/2019, 872/2021 e 21/2020). Não obstante o notável amadurecimento da matéria após a entrega do relatório final dos trabalhos, são consideráveis os desafios sobretudo em termos de implementação e eficácia efetivas quanto à adoção das medidas pelos diversos atores e desenvolvedores em um país de proporções continentais, complexo e heterogêneo.

Sem o devido debate e consentâneo desenho disciplinar e regulatório, o festejo antecipado e incentivo eventualmente irresponsável na implementação de

cidades inteligentes podem representar severo desprezo das liberdades e garantias individuais.

CONCLUSÕES

Para além de uma preocupação relevante e natural com relação (i) à coleta de dados pessoais, vigilância massiva e capacidade de operacionalizar dispositivos, soluções e equipamentos *smart* às disposições da LGPD; (ii) aos problemas para garantir mecanismos eficazes de segurança nos bancos de armazenamento dos dados pessoais coletados; tem-se (iii) os riscos decorrentes das fórmulas de aprendizado de máquina e o potencial discriminatório que estratégias "inteligentes" podem causar em contextos urbanos.

Por essas breves razões, é certo que a utilização massiva de dados pessoais para arquitetar sistemas inteligentes exige, além de uma regulação eficaz e facilmente ajustável às mutações tecnológicas e transformações sociais, a compreensão de que somente com *accountability*, ponderação, e responsabilização é que o progresso técnico-científico assegurará uma real melhora na vida urbana[1]. Uma verdadeira cidade inteligente é aquela que concilia o dinamismo tecnológico com valores fundamentais[2]. Em outras palavras, ser *smart* é a cidade que tenha como vértice não apenas a evolução tecnológica, mas também a inserção e fomento da dignidade da pessoa humana sobre espaços físicos e virtuais, enquanto verdadeiros destinatários de quaisquer soluções idealizadas[3].

---

[1] Acerca da tutela aplicável aos dados pessoais, Maia aponta: "Relativamente à privacidade dos dados pessoais, a despeito da intenção manifestação por parte da doutrina estrangeiro, no sentido de considerá-los objeto de propriedade para tornar a sua tutela mais efetiva, o que os asseguraria eficácia erga omnes e ambulatoriedade, concluímos pela desnecessidade de tal opção no Brasil, onde os direitos da personalidade são irrenunciáveis e dotados de eficácia perante terceiros em virtude de sua positivação, pelo legislador constituinte, como direitos fundamentais" (MAIA, 2019, p. 694).

[2] Bodin de Moraes destaca que "[a] necessidade urgente de regular dilemas criados por tais pesquisas contemporâneas, com todos os desdobramentos político-sociais que elas suscitam, encontrou um legislador sem o preparo necessário para oferecer respostas claras, simples e rápidas – e não poderia ser diferente. A elaboração de uma ordem jurídica que regule fato sociais novos implica a definição, *a priori*, de grandes linhas, ou princípios, que possam servir de parâmetro, de referência, para a sua normatização" (BODIN DE MORAES, 2017, p. 100).

[3] Com relação ao ciberespaço, Rodotà leciona que "Internet e o ciberespaço devem permanecer disponíveis para permitir a livre formação da personalidade, para o exercício da liberdade de expressão e de associação, realização de iniciativas cívicas, experimentação de novas formas de democracia" (RODOTÀ, 2008, p. 169).

REFERÊNCIAS

596 ACRES. ***Mission and story***. Disponível em: <https://596acres.org/mission-and-story/>. Acesso em: 06.08.2022.

AMNESTY INTERNACIONAL. **Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms**. 25 Out. 2021. Disponível em: <https://www.amnesty.org/en/latest/news/2021/10/xenophobic-machines-dutch-child-benefit-scand. Acesso em: 22.10.2022.

ANTONIALLI, Dennys Marcelo; KIRA, Beatriz. Planejamento urbano do futuro, dados do presente: a proteção da privacidade no contexto das cidades inteligentes. ***Revista Brasileira de Estudos Urbanos e Regionais***, n. 22, 2020.

ARENDT, Hannah. **A *condição humana***. 10ª ed. Rio de Janeiro: Forense Universitária, 2004.

BODIN DE MORAES, Maria Celina. ***Danos à pessoa humana****: uma leitura civil-constitucional dos danos morais*. 2ª ed. Rio de Janeiro: Processo, 2017.

BRASIL. Tribunal de Justiça do Estado de São Paulo. **Ação civil pública n. 1090663-42.2018.8.26.0100**. 37ª Vara Cível do Foro Central de São Paulo. Juíza Lívia Martins Trindade.

BRAUNEIS, Robert; GOODMAN, Ellen P. Algorithmic transparency for the smart city. ***Yale Jorunal of Law & Technology***, vol 20, n. 103, 2018.

CHAKRABORTY, Ranjani. *The lost neighborhood under New York's Central Park*. **VOX**. 20 Jan. 2020. Disponível em: <https://www.vox.com/2020/1/20/21070883/central-park-seneca-village>. Acesso em: 06.08.2022.

DORE, Eder. ***Exemplos de Cidades Inteligentes****: 3 iniciativas incríveis*. Disponível em: <https://maplink.global/blog/exemplos-de-cidades-inteligentes/>. Acesso em: 07.08.2022.

EUROPEAN COMMISSION. ***Smart cities****: Cities using technological solutions to improve the management and efficiency of the urban environment*. Disponível em: <https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en>. Acesso em: 08.08.2022.

EVERSON, Eric. Privacy by Design: Taking Ctrl of Big Data. ***Cleveland State Law Review***, Cleveland, v. 65, nº 1, p. 28–42, 2017. Disponível em: <https://engagedscholarship.csuohio.edu/clevstlrev/vol65/iss1/6>. Acesso em: 04.04.2023.

EXAME. ***Três atributos que tornam a tecnologia 5G disruptiva para os negócios***. Disponível em: <https://exame.com/inovacao/tres-atributos-que-tornam-a-tecnologia-5g-disruptiva-para-os-negocios/>. Acesso em: 06.08.2022.

FDA. ***Good Machine Learning Practice for Medical Device Development****: Guiding Principles*. Disponível em:<https://www.fda.gov/medical-devices/software-medical-device-samd/good-machine-learning-practice-medical-device-development-guiding-principles>. Acesso em: 22.10.2022.

FERGUSON, Andrew Guthrie. *Predicting Predictive Policing in NYC*. **HUFFPOST**. 8 Jul. 2016. Disponível em: <https://www.huffpost.com/entry/predicting-predictive-pol_b_7757200>. Acesso em: 22.10.2022.

GORDON, Rachel. Artificial intelligence predicts patients' race from their medical images. **MIT NEWS**. 20 Maio 2022. Disponível em: <https://news.mit.edu/2022/artificial-intelligence-predicts-patients-race-from-medical-images-0520> Acesso em: 22.10.2022.

HAN, Byung-Chul. ***O que é poder?*** Trad. Gabriel Salvi Philipson. Petrópolis: Vozes, 2019.

IDC. ***Future of Industry Ecosystems****: Shared Data and Insights Shared Data and Insights are Making Organizations More Resilient, Flexible and Profitable*. 6 Jan. 2021. Disponível em: <https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/>. Acesso em: 22.10.2022.

KITCHIN, Rob. ***The Promise and Perils of Smart Cities***. Disponível em: <https://www.scl.org/articles/3385-the-promise-and-perils-of-smart-cities#:~:text=In%20short%2C%20the%20smart%20city,pragmatic%2C%20neutral%20and%20apolitical%20ways>. Acesso em: 06.08.2022.

KOSINSKI, Michal; WANG, Yilun. Deep Neural Networks Are More Accurate Than Humans at Detecting Sexual Orientation From Facial Images. ***Journal of Personality and Social Psychology*** *February*, 2018 Vol. 114, Issue 2, p. 246–257.

MAIA, Roberta Mauro Medina. *Vivendo nas nuvens: dados pessoais são objeto de propriedade?* TEPEDINO, Gustavo; DE MENEZES, Joyceane Bezerra (Coord.) **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019.

MECABÔ, Alex. ***Para além da privacidade****: proteção de dados pessoais e desafios à regulação*. Dissertação - Mestrado em Direito das Relações Sociais - Faculdade de Direito, Universidade Federal do Paraná (UFPR), Curitiba, 2021. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/73339/R%20-%20D%20-%20ALEX%20MECABO.pdf?sequence=1&isAllowed=y>. Acesso em: 04.03.2023.

MULHOLLAND, Caitlin; FRAJHOF, Isabela Z. Inteligência artificial e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Coords.). ***Inteligência artificial e direito****: ética, regulação e responsabilidade*. São Paulo: Thomson Reuters Brasil, 2019.

MUNTEAN, Pete. ***Porn plays on screen in D.C.'s Union Station***. USA Today. 17 maio 2017. USA Today. 17 Maio 2017. Disponível em:

<https://www.usatoday.com/story/news/nation-now/2017/05/17/porn-plays-screens-d-c-s-union-station/327411001/>. Acesso em: 06.10.2022.

NEC. ***Which cities are smart cities? 5 examples of smart cities around the world***. 14. fev. 2022. Disponível em: < https://www.nec.co.nz/market-leadership/publications-media/which-cities-are-smart-cities-5-examples-of-smart-cities-around-the-world/>. Acesso em: 22.10.2022.

ORMEROD. Alex González. *How AI reinforces racism in Brazil. Rest Of World*. 22 Abr. 2022. **Rest of World**. Disponível em: <https://restofworld.org/2022/how-ai-reinforces-racism-in-brazil/>. Acesso em: 22.10.2022.

PARENTI, Claris; NOORI, Negar; JANSSEN; Marijin. A Smart Governance diffusion model for blockchain as an anti-corruption tool in Smart Cities. ***Journal of Smart Cities and Society***, vol. 1, 2022, p. 71-92.

PIOVESAN, Flávia; GONZAGA, Victoriana Leonora Corte. *Empresas e direitos humanos: desafios e perspectivas à luz do direito internacional dos direitos humanos*. In: PIOVESAN, Flávia; SOARES, Inês Virginia P.; TORELLY, Marcelo. **Empresas e direitos humanos**. Salvador: JusPodivm, 2018.

PREFEITURA DE SÃO PAULO. ***GeoSampa***. Disponível em: <http://geosampa.prefeitura.sp.gov.br/PaginasPublicas/_SBC.aspx>. Acesso em: 06.08.2022.

RITO, Fernanda Paes Leme Peyneay; GUEIROS, Pedro Teixeira. O Social Credit System na Era dos Dados. *PragMATIZES* - ***Revista Latino-Americana de Estudos em Cultura***, Niterói/RJ, Ano 10, n. 19, p. 170-213, set. 2020.

RODOTÀ, Stefano. ***A vida na sociedade da vigilância****: a privacidade hoje*. Org., sel. e apr. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SIMIONITE, Tom. *How an Algorithm Blocked Kidney Transplants to Black Patients*. **WIRED**. 26 Out. 2020. Disponível em: <https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/. Acesso em: 22.10.2022.

SNYDER, John Beltz. *Researchers hack a self-driving car by putting stickers on street signs*. **AUTOBLOG**. 4 Ago. 2017. Disponível em: <https://www.autoblog.com/2017/08/04/self-driving-car-sign-hack-stickers/> Acesso em: 06.10.2022.

SOARES, Mariana Ribeiro. Holanda. *Relatório expõe como um "algoritmo xenófobo" influenciou a atribuição de apoios sociais às famílias*. **RTP**. 25 Out. 2021. Disponível em: <https://www.rtp.pt/noticias/mundo/holanda-relatorio-expoe-como-um-algoritmo-xenofobo-influenciou-a-atribuicao-de-apoios-sociais-as-familias_n1358439>. Acesso em: 22.10.2022.

WILLIAMS, Clarence. *Hackers hit D.C. police closed-circuit camera network, city officials disclose*. **The Washington Post**. 27 Jan. 2017. Disponível em:

<https://www.washingtonpost.com/local/public-safety/hackers-hit-dcpolice-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html?utm_term=.39a287b8b971>. Acesso em: 22.10.2022.