Vigilância, Perfilamento e Tratamento de Dados Pessoais no Contexto do Controle Migratório

Surveillance, Profiling and Processing of Personal Data in the Context of Migratory Control

STÉFANI REIMANN PATZ[1]
Universidade Regional Integrada do Alto Uruguai e das Missões (URI).

THAMI COVATTI PIAIA[2]
Universidade Regional Integrada do Alto Uruguai e das Missões (URI).

RESUMO: O artigo tem como objetivos investigar como se dá a utilização de técnicas de perfilamento e tratamento de dados pessoais no ambiente do controle migratório. Para isso, inicialmente se analisam aspectos gerais da importância dos dados pessoais, da sociedade da vigilância, no que consistem as técnicas de perfilamento e nas repercussões das decisões automatizadas. Na sequência, observa-se como tais técnicas são utilizadas no controle migratório britânico e canadense. Depois, analisam-se as iniciativas brasileiras, com destaque ao projeto piloto Embarque Mais Seguro. Por fim, o artigo dedica-se a investigar como se dá o tratamento dos dados pessoais no âmbito do controle migratório brasileiro, observando o disposto na Lei Geral de Proteção de Dados (LGPD) e o Anteprojeto da LGPD Penal. Trata-se de uma análise doutrinária com revisão bibliográfica referenciada que, após exemplificação prática e situando o atual estágio dessas ferramentas nos controles migratórios de alguns Estados, com esteio no método dedutivo, compreende que o uso de tais ferramentas impacta os direitos humanos dos migrantes. Por fim, conclui-se a contribuição com uma perspectiva referente a novos desafios e novas abordagens de regulação ao tratamento dos dados pessoais no contexto migratório.

PALAVRAS-CHAVE: Vigilância; perfilamento; decisões automatizadas; controle migratório.

ABSTRACT: The article aims to investigate the use of profiling and processing techniques for personal data in the migration control environment. For this, we initially analyze general aspects of the

1 Orcid: https://orcid.org/0000-0002-6375-2942.
2 Orcid: https://orcid.org/0000-0001-7123-0186.

importance of personal data, of the surveillance society, which consist of profiling techniques and the repercussions of automated decisions. Next, it is observed how such techniques are used in British and Canadian migratory control. Then, the Brazilian initiatives are analyzed, as highlighted in the Embarque Mais Seguro pilot project. Finally, the article is dedicated to investigating how the processing of personal data takes place in the context of Brazilian immigration control, observing the provisions of the General Data Protection Law (LGPD) and the Penal LGPD Draft. This is a doctrinal analysis with referenced bibliographic review that, after practical examples and situating the current stage of these tools in the migratory controls of some States, based on the deductive method, understands that the use of such tools impacts human rights of migrants. Finally, the contribution is concluded with a perspective regarding new challenges and new regulatory approaches to the processing of personal data in the migratory context.

KEYWORDS: Surveillance; profiling; automated decisions; migration control.

SUMÁRIO: Considerações iniciais; Dados, vigilância e decisões automatizadas; O uso de tecnologias de perfilamento no âmbito do controle migratório; Iniciativas em solo nacional; O tratamento dos dados pessoais no contexto migratório brasileiro; Considerações finais; Referências.

CONSIDERAÇÕES INICIAIS

Pesquisas do Escritório das Nações Unidas sobre Drogas e Crime (UNODC) indicam que, a curto prazo, as restrições de movimentos a partir do alto controle e/ou fechamento de fronteiras terrestres, marítimas e aéreas irão reduzir o movimento migratório. Entretanto, a médio e longo prazo, podem resultar no aumento da migração, que, afetada pela repercussão econômica da pandemia da Covid-19, não possibilitará regularidade aos migrantes e, portanto, poderá aumentar o tráfico de pessoas (UNODC, 2020, s.p.).

Dados de 2020 mostram que existem cerca de 281 milhões de migrantes internacionais. Mais de 1,1 bilhões de pessoas em movimento no mundo. Mais de 82,4 milhões de pessoas forçadas a deixar suas casas devido a conflitos armados, violência generalizada e desastres naturais. Destes, quase 26,4 milhões são refugiados, e quase metade deles tem menos de 18 anos. Neste momento, uma em cada 95 pessoas na Terra foge de suas casas por causa de conflitos e perseguições (ACNUR, 2021; UN, 2021).

Esses dados indicam que uma parcela considerável da população passou e continuará passando por áreas de segurança, questionários, monitoramento por vídeo, escâneres corporais, entre diversas outras formas de vigilância que fazem parte do procedimento de admissão de viajantes e migrantes dentro do território de determinado Estado. Antes, a decisão de permitir ou negar a entrada em um país era tomada apenas por agen-

tes fronteiriços. Hoje, a decisão é apoiada por sistemas automatizados, que perfilam o candidato com apoio de tecnologias de reconhecimento facial e inteligência artificial, por exemplo[3].

O presente texto respalda-se na compressão que viver na contemporaneidade é habitar um mundo em que os algoritmos cada vez mais julgam decisões importantes nas vidas das pessoas. Com o avanço da *big data*[4], houve a ampliação do emprego de sistemas de inteligência artificial e o aprimoramento de sistemas de decisão automatizados[5].

Diante do exposto, o objetivo do artigo é observar como se dá o uso de tecnologias de perfilamento no ambiente do controle migratório e qual é tratamento dos dados pessoais dos migrantes no ordenamento jurídico nacional. Inicialmente, reflete-se sobre o atual contexto da sociedade dos dados, da vigilância e das decisões automatizadas. Na sequência, analisa-se o uso de tecnologias de perfilamento no ambiente do controle migratório do Reino Unido e do Canadá, e, depois, no Brasil[6]. Por fim, investiga-se qual é a disciplina que se aplica ao tratamento dos dados pessoais no contexto do controle migratório brasileiro, com ênfase no disposto na Lei Geral de Proteção de Dados Pessoais (LGPD) e na redação do Anteprojeto da LGPD Penal.

O método de abordagem será o dedutivo e o método de procedimento, o analítico, por meio da pesquisa indireta com a consulta a livros e revistas científicas. Importante notar que não se busca uma análise exaustiva do testemunho histórico, o que, pela densidade da temática, seria inviável. A proposta é tão somente situar o(a) leitor(a) acerca da temática que ocupa a agenda de proteção de dados e a agenda migratória.

---

3 Desde 2018, muitas companhias aéreas começaram a usar a tecnologia de reconhecimento facial a bordo. Só nos EUA, mais de 15 aeroportos criaram sistemas de correspondência facial para ajudar a embarcar os passageiros com mais rapidez e segurança (Thales, 2021).

4 *Big data* é o termo em inglês que descreve o grande volume de dados gerados e armazenados, que podem se estruturados e não estruturados. Dados estruturados são os dados organizados de alguma forma (banco de dados, planilhas eletrônicas, p. ex.) e dados não estruturados são os dados não submetidos a uma organização definida (*website*, mídia, arquivo de texto, p. ex.). Estima-se que apenas 10% dos dados gerados são estruturados (Kaufman, 2019, p. 32).

5 Inúmeros são os exemplos de como decisões antes tomadas por seres humanos agora dependem de modelos de risco preditivo, sistemas automatizados de *ranking* e de elegibilidade. Dentre eles se encontram as possibilidades de concessão de crédito na compra de um automóvel ou mesmo da casa própria, o cálculo do valor dos juros, a seleção de currículos para acesso ao primeiro emprego ou recolocação no mercado de trabalho e até mesmo o direcionamento de uma investigação por fraude ou a escolha de uma determinada região para a ronda policial (Marrafon; Medon, 2019).

6 A escolha dos casos concretos de utilização de ferramentas de inteligência artificial (IA) no contexto migratório pelos governos do Reino Unido e Canadá deu-se: (i) pela relevância dos projetos; (ii) pelo vasto conteúdo bibliográfico disponível nos meios digitais, e (iii) pelo fato de que, a partir dos exemplos, podem-se observar os riscos de tomada de decisões enviesadas com base nos resultados apresentados pelos sistemas.

DADOS, VIGILÂNCIA E DECISÕES AUTOMATIZADAS

A informação sempre foi um elemento crucial para o desenvolvimento humano. Hoje, mais do que nunca. Sedimentada pela evolução tecnológica, a sociedade de informação criou mecanismos capazes de processar e transmitir informações de maneira cada vez mais veloz, ocasionando novas formas de organização social. Se no passado nos organizávamos como uma sociedade "presencial", no momento somos, em grande parte, digitais. Isso implica sociabilidade amplamente medida por tecnologias que fomentam relações pessoais, culturais, mercadológicas, socioeconômicas e até mesmo de vigilância, o que se dá devido ao desenvolvimento exponencial de diferentes tecnologias, com destaque para as chamadas "tecnologias de informação e comunicação" (TIC) (Oliveira, 2021, p. 29).

Nas palavras de Stefano Rodotà, somos "assediados por computadores, espiados por olhos furtivos, filmados por telecâmeras invisíveis. Os cidadãos da sociedade da informação correm o risco de parecer homens de vidro: uma sociedade que a informática e a telemática estão tornando totalmente transparente" (2008, p. 8). Para o autor italiano, estamos assistindo a uma progressiva extensão das formas de controle social, motivadas, sobretudo, por razões de segurança. Trata-se de uma profunda mudança social. A vigilância passa de excepcional a cotidiana, das classes "perigosas" à generalidade das pessoas, do interior dos Estados ao mundo global (2008, p. 9).

Na visão de Samuel Oliveira, algumas questões preocupantes decorrem do emprego maciço das inovações tecnológicas, envolvendo, por exemplo, "a consolidação da vigilância, a erosão da confiabilidade nos governos e nas instituições e as violações sistemáticas a direitos fundamentais" (2021, p. 29-30). Não há dúvidas de que a vigilância existe há muito tempo. Modos mais antigos, menos formais e menos técnicos de vigilância já existiam quando as pessoas observavam umas às outras dentro do ambiente familiar, religioso, estudantil e até em pequenas cidades.

A vigilância, entretanto, não era institucionalizada – pelo menos não nos momentos iniciais. No entendimento de Samuel Oliveira, novas formas de vigilância surgiram à medida que as instituições mudaram e se tornaram menos centrais diante de uma população crescente, urbanizada, globalizada e móvel. Com o início da era da informação e com a disseminação de instrumentos tecnológicos – computadores, aparelhos celulares, dispositivos vestíveis, entre outros –, a preços acessíveis, a vigilância adquiriu uma dimensão altamente tecnológica (2021, p. 31).

Mas por que o termo "sociedade da vigilância"? Para Samuel Oliveira, o termo deve ser utilizado porque, virtualmente, todas as atividades sociais, institucionais e negociais que possuem alguma relevância na sociedade envolvem a coleta e o monitoramento sistemático de dados, bem como a análise desses dados com o objetivo de tomar decisões, minimizar riscos, classificar grupos sociais e exercer poder (2021, p. 81). A vigilância é, portanto, "monitorar as pessoas a fim de regular ou governar seu comportamento" (Gilliom; Monahan, 2013, p. 9).

Uma das maneiras pelas quais a vigilância tem se concretizado é por meio da utilização massiva de tecnologias de reconhecimento facial (TRF) para fins de segurança e controle. Os exemplos são inúmeros. Na China, 200 milhões de câmeras compõem um sistema de vigilância capaz de identificar basicamente qualquer um dos 1.4 bilhões de habitantes do país (Mozur, 2018, s.p.). Já em Dubai, capital dos Emirados Árabes Unidos, um gigante "túnel-aquário", localizado no principal aeroporto da cidade, conta com mais de 80 câmeras que escaneiam o rosto das pessoas à medida que caminham por ele; realizada a análise das imagens obtidas, o sistema de segurança ou permite que a pessoa ingresse livremente no país ou emite um alerta, indicando a necessidade de uma análise mais aprofundada acerca de sua liberação (ONG, 2017, s.p.).

Para Stefano Rodotà, os riscos da sociedade da vigilância ligam-se tradicionalmente ao "uso político de informações para controlar os cidadãos [...], a ideia de vigilância invade cada momento da vida e se apresenta como um traço próprio das relações de mercado, cuja fluidez diz respeito à possibilidade de dispor livremente de um conjunto crescente de informações" (2008, p. 113). O uso político das informações de que fala o autor italiano pode ser facilmente relacionado à temática do texto, considerando que diversos Estados utilizam informações para aceitar ou negar a entrada de migrantes por meio do controle de fronteiras que perfilam os candidatos, com auxílio de tecnologias de reconhecimento facial e inteligência artificial.

Neste contexto, Rodotà afirma que se materializa a imagem do "homem de vidro", o verdadeiro cidadão desse novo mundo. Uma imagem que, não por acaso, "provém diretamente do tempo do nazismo e que propõe uma forma de organização social profundamente alterada, uma espécie de transformação irrefreável da 'sociedade da informação' em 'sociedade da vigilância'" (2008, p. 113). Para Daniel Solove, o processo de agregação de dados sobre alguém cria uma "pessoa digital: um retrato composto de fragmentos de informações combinadas" (2008, p. 125). Trata-se, portanto,

de um verdadeiro quebra-cabeça digital sobre uma determinada pessoa, um perfil com base nos dados disponíveis nos sistemas sobre a pessoa.

No entendimento de Rodotà, a utilização de informações pessoais para construção de perfis individuais ou de grupos deve ser observada com cuidado, considerando que:

> [...] as informações utilizadas são, de fato, sempre parciais e incompletas, mesmo quando se recorre a uma multiplicidade de bancos de dados. Além disso, permanece controversa, e a ser comprovada, a plena validade científica dos modelos usados para produzir novas informações (perfis ou outras) com base em dados coletados. Chega-se assim a "metaconhecimento" sobre as pessoas, que dificilmente podem ser verificados pelos interessados, embora até embasem decisões sobre eles. (2008, p. 115)

A técnica do perfilamento (*profiling*) está presente nos mais diversos contextos e pode ser utilizada com as mais diversas finalidades. A criação de perfis é um processo pelo qual se busca descobrir correlações entre dados que podem ser usados para identificar e representar um indivíduo ou grupo. Esses dados são transformados em conhecimento ou inferências, que, por sua vez, são utilizados para individuar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria, com a construção de prováveis atributos ou comportamentos de uma pessoa (Hildebrandt, 2008).

Nesse sentido, o Regulamento Geral sobre Proteção de Dados (RGPD)[7] da União Europeia define *profiling* em seu art. 4º, item 4, a saber:

> [...] qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações. (União Europeia, 2016)

Ao interpretar o art. 4º do RGPD e registrar que o processo de definição de perfis pode implicar um conjunto de deduções estatísticas, o extinto

7 O Regulamento Geral sobre Proteção de Dados (RGPD) – *General Data Protection Regulation* (GDPR) passou a ser aplicável a partir de 25 de maio de 2018, em substituição à legislação europeia acerca da proteção de dados (substituiu a Diretiva de Proteção de Dados de 1995 – 95/46/EC). A GDPR foi projetada para: a) harmonizar as leis de privacidade de dados em toda a Europa; b) proteger e capacitar a privacidade de dados de todos os cidadãos da UE; e c) remodelar a maneira como as organizações em toda a região abordam a privacidade dos dados.

Grupo de Trabalho do Artigo 29[8] esclarece que o *profiling* é frequentemente "utilizado para efetuar previsões sobre as pessoas, recorrendo a dados provenientes de várias fontes para inferir algo sobre uma pessoa, com base nas qualidades de outras pessoas que, estatisticamente, parecem semelhantes" (European Commission, 2017, p. 7).

Para Felix Naumann, o processo de geração de perfil de dados, ou *data profiling*, consiste em examinar os dados disponíveis em uma determinada fonte e coletar informações a respeito deles, produzindo metadados cuja análise é um passo importante para gerenciar a qualidade dos dados da fonte. Um cenário típico seria a varredura das tabelas de um banco de dados relacional para obter informações como tipos de dados, padrões de valores, completude e unicidade de colunas, ou até mesmo dependências funcionais e regras de associação (2014, p. 40-49).

Cabe pontuar, entretanto, que a geração de dados, além das bases de dados relacionais tradicionais, cresce na atualidade tendo em vista o volume de dados gerados a cada instante, algo sem precedentes na História. Nesse sentido, dados do Banco Mundial indicam que 3,000,000,000,000 *gigabytes* (GB) circulam globalmente através da internet. Isso equivale a 32 GB por mês e, por pessoa de dados, mais de 1 GB por dia, ou 325 milhões de casas assistindo a vídeos em *streaming* simultaneamente (2021, s.p.).

A título exemplificativo, Danilo Doneda indica que o perfilamento poderia ser utilizado para, por exemplo, controlar a entrada de pessoas em um determinado país pela alfândega e poderia ser utilizada pelas empresas para traçarem perfis de consumidores e, assim, direcionarem a publicidade (2006, p. 173).

Neste cenário, é preciso lembrar que a incorporação de sistemas de decisões automatizados que empregam inteligência artificial (IA) tem sido adotada com entusiasmo pelo setor privado e público em diversas áreas. O termo IA, criado por John McCarthy (1956), ganhou várias definições ao longo dos anos, mas pode-se considerar que é "o estudo de como fazer com que os computadores façam coisas que, no momento, as pessoas fazem melhor" (Rich; Knight, 1991). A área da IA deu seus primeiros passos com o

8 *Article 29 Working Party*: O Grupo de Trabalho do Artigo 29 foi criado pela Diretiva nº 95/46/CE e tratou de questões relacionadas à proteção da privacidade e dos dados pessoais até 25 de maio de 2018, data da entrada em vigor do RGPD. Disponível em: https://edpb.europa.eu/about-edpb/more-aboutedpb/article-29-working-party_en.

desenvolvimento do primeiro modelo de um neurônio artificial (McCulloch; Pitts, 1943), a criação da primeira máquina para simular uma rede neural artificial (Minsky, 1952) e os avanços na área de aprendizado, estendendo o conceito de neurônios artificiais (Rosenblatt, 1961).

Apesar de ser uma área relativamente antiga, atraiu os holofotes da mídia e da sociedade somente nas últimas décadas com a IBM e seu Deep Blue vencendo o campeão de xadrez Garry Kasparov (1997) e o Watson competindo e vencendo o jogo "Jeopardy!" (2011), com os algoritmos de recomendações da empresa Amazon (Linden, 2003), com as pesquisas do Google na área de reconhecimento de objetos em imagens (Quoc, 2012), e com o DeepMind propondo soluções para um problema que estava aberto por mais de 50 anos na área de enovelamento de proteínas (Jumper *et al.*, 2021) e na área de previsão do tempo em curto prazo (Ravuri, 2021).

Contudo, quando sistemas de IA são utilizados para fins de avaliações educacionais, campanhas políticas, seleção de candidatos a empregos, e até mesmo para a implementação de mecanismos relacionados a policiamento preditivo e a admissão de migrantes em um Estado, diversas considerações devem ser feitas. Uma delas diz respeito à falta de transparência em relação aos titulares dos dados ou destinatários desses sistemas, que, muitas vezes, não conseguem acessar ou avaliar a qualidade das inferências que são realizadas sobre eles. Tal situação coloca em risco questões fundamentais inerentes à dignidade humana, como liberdade, igualdade, não discriminação, devido processo legal, proteção dos dados pessoais e dados pessoais sensíveis e da autodeterminação informacional.

Para Laurianne-Marie Schippers e Marília Papaléo Gagliardi, muitas vezes existe a concepção de que algoritmos seriam imparciais e, portanto, seriam ideais para tomar decisões no lugar de seres humanos, que poderiam apresentar decisões enviesadas e prejudicadas por suas próprias percepções. Se é uma máquina que está fazendo sugestões de conteúdo, ou organizando o sistema de identificação, esta deveria, em tese, não possuir nenhum conteúdo discriminatório em sua origem (Schippers; Gagliardi, 2021, s.p.).

No entendimento de Ana Frazão, a transferência ou delegação total do processo decisório de agentes públicos e privados para sistemas algorítmicos é procedimento que envolve diversos riscos, considerando as limitações já apontadas na programação e nos *designs* de tais sistemas. Para a autora, mesmo quando não ocorre a terceirização total e o sistema algorítmico tem o papel de ser apenas um auxiliar no processo decisório, permanecen-

do o ser humano com a "última palavra", os desafios não são banais. Afinal de contas, pouco se sabe sobre como se comportam seres humanos diante de decisões algorítmicas, havendo o fundado receio de que tendam a concordar com os seus resultados, até porque, considerando a opacidade dos algoritmos, não conseguem compreendê-los nem os questionar (2021, s.p.).

De acordo com Ana Frazão, o chamado fenômeno do viés da automação (*automation bias*) sugere que

> [...] ferramentas de automação influenciam decisões humanas de formas significativas e geralmente ruins. Dois tipos de erros são particularmente comuns: (i) erros de omissão, nos quais as pessoas não reconhecem quando os sistemas automatizados erram e (ii) erros comissivos, nos quais as pessoas seguem os sistemas automatizados sem considerar suas informações contraditórias. (2021, s.p.)
>
> Consequentemente, a autora entende que uma forte confiança em sistemas automatizados pode "alterar as relações das pessoas com as suas tarefas, criando uma espécie de 'para-choque' entre as decisões e os seus impactos, com a consequente perda do senso de responsabilidade e da *accountability*" (2021, s.p.).

Neste contexto, Zygmunt Bauman reflete sobre a adiaforização, em que sistemas e processos se divorciam de qualquer consideração de caráter moral. Para o autor, um ângulo da adiaforização em termos de vigilância é a forma como dados do corpo (dados biométricos, DNA) ou por ele desencadeados (por exemplo, situações em que faz um *login*, usa-se um cartão de acesso ou mostra-se a identidade) são sugados para bases de dados a fim de serem processados, analisados, concatenados com outros dados e depois cuspidos de volta como "replicação de dados" (2013, p. 15).

As informações que fazem as vezes da pessoa são constituídas de "dados pessoais" apenas no sentido de que se originaram em seu corpo e podem afetar suas oportunidades e escolhas existenciais. A "replicação e fragmentação de dados" tende a inspirar mais confiança que a própria pessoa – que prefere contar sua própria história. Os *designers* de *software* dizem que estão simplesmente "lidando com dados", de modo que seu papel é "moralmente neutro" e suas avaliações são apenas "racionais" (2013, p. 15).

De uma forma geral, o uso de tecnologias de decisões automatizadas pode incrementar a celeridade e a acurácia na análise de uma quantidade

expressiva de processos e situações, contemplando princípios relevantes de celeridade, eficiência e economia. Entretanto, acurácia e celeridade não podem ser as métricas-fim ou fundamento raiz da utilização de sistemas de inteligência artificial, mas deve existir uma associação com a sustentabilidade, a inclusão e proteção da diversidade, a solidariedade e a equidade (Peixoto, 2020, p. 318).

Diante do exposto, percebe-se que os dados pessoais, a vigilância e as decisões automatizadas são temas que possuem grandes conexões entre si, e que podem ser vistos em diversos segmentos da sociedade atual. Nesse contexto, imperioso lembrar os ensinamentos de Shoshana Zuboff sobre o capitalismo de vigilância e como ele é visto como um movimento que visa impor uma nova ordem coletiva baseada em uma certeza total. A autora informa que somos "as fontes do superávit crucial do capitalismo de vigilância: os objetos de uma operação de extração de matéria-prima tecnologicamente avançada e da qual é cada vez mais impossível escapar" (2020, p. 22). Sob essa perspectiva, o próximo tópico busca compreender como as técnicas de perfilamento são utilizadas no ambiente do controle migratório e como elas podem impactar os migrantes.

O USO DE TECNOLOGIAS DE PERFILAMENTO NO ÂMBITO DO CONTROLE MIGRATÓRIO

Nesta perspectiva, a vigilância é uma dimensão-chave do mundo moderno. Conforme Zygmunt Bauman, viajantes em passagem por aeroportos sabem que precisam atravessar não apenas o controle de passaportes em sua versão do século XXI, mas também por novos dispositivos, como escâneres corporais e aparelhos de checagem biométrica, que têm proliferação desde os atentados de 11 de setembro nos Estados Unidos (2013, p. 9).

Neste contexto, a segurança transformou-se em um empreendimento orientado para o futuro e funciona por meio da vigilância, tentando monitorar o que *vai* acontecer pelo emprego de técnicas digitais e raciocínio estatístico. A segurança funciona a distância tanto no espaço quanto no tempo, circulando de maneira fluida, juntamente com os Estados-Nação, mas para além deles, em um domínio globalizado. Na visão de David Lyon, "processos de estereotipia e medidas de exclusão estão à espera dos grupos desafortunados o bastante para serem rotulados de 'indesejados'" (2013, p. 13).

As dimensões tecnológicas, ou melhor, tecnossociais, da vigilância atual relacionam-se com a classificação da população em categorias, tendo em vista um tratamento diferencial. Surgem questões relacionadas a como

as tecnologias provocam consequências menos catastróficas, porém não menos insidiosas, em particular para grupos já discriminados.

Alguns governos ao redor do mundo já se valem de ferramentas de inteligência artificial para auxiliar na tomada de decisões para realizar controles migratórios. Neste sentido, o texto observa as atividades dos governos do Reino Unido e do Canadá a fim de identificar como essas tecnologias de perfilamento estão sendo utilizadas e quais os potenciais impactos aos direitos humanos dos migrantes. Por fim, observaremos as iniciativas no Brasil, com destaque ao projeto Embarque Mais Seguro.

No Reino Unido, a triagem e definição da fila de pedidos de visto era realizada de forma automatizada, por meio de um sistema que classificava os pedidos, a partir das informações fornecidas pelos aplicantes, em três possíveis bandeiras: vermelha, amarela e verde. De acordo com o Home Office, órgão do Reino Unido responsável pela imigração, dentre outras atribuições relacionadas à segurança, a análise realizada pelo sistema servia como um auxílio às decisões de concessão de visto a serem tomadas pelos agentes. Para Henry McDonald, do *The Guardian*, a decisão final era tomada por pessoas naturais, com base na separação e sistematização feita pelo algoritmo (BBC, 2020, s.p.).

Em 2020, diversas notícias surgiram alegando que o algoritmo utilizado estaria fazendo classificações negativas e de cunho racista. Conforme a BBC, a acusação formada pelo Joint Council for the Welfare of Immigrants[9] e o grupo Foxglove[10] era a de que a categorização realizada pelo sistema levaria em conta, dentre outras informações, a nacionalidade do migrante. Nesse sentido, o próprio sistema de migração do Reino Unido (Home Office) utilizaria uma lista de nacionalidades suspeitas que seriam automaticamente classificadas com a bandeira vermelha (BBC, 2020, s.p.).

A apuração partiria de uma premissa de dificultar o processo de obtenção de vistos de imigrantes com base na nacionalidade, e acarretaria

9 O Conselho Conjunto para o Bem-Estar dos Imigrantes (JCWI) é uma instituição de caridade independente do Reino Unido que fornece informações sobre imigração e aconselhamento jurídico gratuito sobre questões relacionadas à imigração, incluindo direito a benefícios (Barnet, 2021).

10 Foxglove é uma organização independente e sem fins lucrativos do Reino Unido. Em seus primeiros dois anos, construiu um histórico de responsabilização de grandes empresas de tecnologias e governos. A organização forçou a divulgação de contratos secretos entre gigantes da tecnologia e o governo, conhecidos como "NHS Covid-19 data deals", parou o algoritmo racista de vistos do Home Office e ajudou a tornar a avaliação justa para todos os alunos no Reino Unido, desafiando o algoritmo de Ofqual. Foxglove é formada por uma equipe de advogados especialistas em tecnologia e especialistas em comunicação (Foxglove, 2021).

problemas como, por exemplo, as análises de concessão de vistos serem muito mais demoradas, passarem por uma averiguação mais severa e terem uma chance maior de serem negadas (BBC, 2020, s.p.). De acordo com o Foxglove, essa discussão tem ocorrido desde 2017 no sistema de justiça britânico. Todavia, apenas em agosto de 2020, com o processo ainda em curso, o departamento do Home Office optou por parar o uso do algoritmo, a fim de auditá-lo para identificar a presença de potenciais vieses que gerassem discriminação e qualquer tomada de decisão negativa de forma injustificada (Heaven, 2020, s.p.).

Já no contexto do Canadá, o The Citizen Lab, em conjunto com o International Human Rights Program da Faculdade de Direito da Universidade de Toronto, publicou uma pesquisa de Petra Molnar e Lex Gill chamada *Bots at the gate: a Human Rights analysis of automated decision-making in Canada's immigration and refugee system*. O relatório elaborado em 2018 indica que o governo canadense também se utiliza de ferramentas de tomadas de decisão automatizada no âmbito migratório e de refúgio (Molnar; Gill, 2018, p. 14).

O documento aponta para a possibilidade e riscos de usos de ferramentas de tomadas de decisão automatizadas em diversos momentos do fluxo migratório. Entretanto, há a menção de que o governo emprega tais ferramentas na análise dos solicitantes de visto, mas não é possível verificar como essa análise é feita e quais são os critérios utilizados (2018, p. 24-5). Sob essa perspectiva, é possível afirmar que há falta de transparência nos procedimentos, impossibilitando, inclusive, que a sua neutralidade seja verificada.

O relatório também destaca que o algoritmo pode ser utilizado para fazer classificações sobre a veracidade do alegado por um candidato a visto. Por exemplo, se ele realmente é casado (2018, p. 25-33). Essa decisão influencia diretamente na credibilidade do aplicante, e pode ser imprescindível para a concessão ou não do visto.

O documento não se posicionou de forma repulsiva à própria tecnologia, mas ao uso irresponsável dela, podendo exacerbar disparidades. Identificou-se que o governo canadense, desde 2014, ampliou o uso de tecnologia e está desenvolvendo um sistema de análise preditiva para automatizar atividades até então conduzidas por funcionários de imigração (2018, s.p.). A pesquisa afirma que o Canadá tem obrigações domésticas e internacionais claras com o respeito e a proteção dos direitos humanos e

que cabe aos políticos, funcionários públicos, tecnólogos e engenheiros, assim como advogados, sociedade civil e universidade, adotarem uma ampla visão crítica dos impactos reais do uso de tecnologia sobre a vida humana (2018, s.p.). Para os autores, o desafio não é como usar novas tecnologias para consolidar velhos problemas, mas, em vez disso, para melhorar entender como podemos usar esta oportunidade para imaginar e projetar sistemas mais transparentes, equitativos e justos (2018, p. 7).

Na visão de Fabiano Hartmann Peixoto, o tema apresenta fundamento jurídico, já que as várias facetas do uso de sistemas de decisão automatizados podem atingir direitos humanos, incluindo direitos à igualdade e à não discriminação; liberdade de movimento, expressão, religião e associação; privacidade, vida, liberdade e segurança das pessoas. Para o autor, a temática também desperta questões de direito constitucional e administrativo, acesso à justiça, responsabilidade público e privada, capacidade de gestão pública e governamental, bem como outros impactos globais (2020, p. 309).

Diante do exposto, percebe-se que as tecnologias de perfilamento envolvendo TRF e IA já estão sendo utilizadas no ambiente do controle migratório em diversos lugares do mundo[11]. Nesse contexto, cabe frisar que os exemplos citados são casos chave para observar o desenvolvimento da temática; entretanto, não são os únicos: Estados Unidos, Nova Zelândia, Austrália, entre outros países, também utilizam tecnologias similares. Na sequência, observa-se como a temática se desenvolve no Brasil.

INICIATIVAS EM SOLO NACIONAL

Inicialmente, destaca-se o projeto piloto Embarque Mais Seguro. Trata-se de um sistema de reconhecimento por biometria, que valida a identidade do viajante por *selfies* tiradas na hora comparadas com bases de dados públicas preexistentes do Denatran e do Barramento SGD (TSE)[12]. Conforme informações divulgadas pela Serpro, empresa de inteligência em tecnologia

11 Saiba mais em: SCHIPPERS, Laurianne-Marie; GAGLIARDI, Marília Papaléo. *Inteligência artificial e controle migratório*: algoritmos podem discriminar migrantes? Publicado em: 16 jan. 2021. Disponível em: https://medium.com/o-centro-de-ensino-e-pesquisa-em-inova%C3%A7%C3%A3o-est%C3%A1/intelig%-C3%AAncia-artificial-e-controle-migrat%C3%B3rio-algoritmos-podem-discriminar-migrantes-85d04-d152440. Acesso em: 10 set. 2021.

12 O barramento de serviços é uma solução centralizada que permite que um órgão envie processos ou documentos administrativos digitais para outro de maneira segura e com confiabilidade de entrega. Tal solução permite o trâmite eletrônico entre plataformas distintas (SEI, 2021).

da informação (TI) do governo federal, em parceria com o Ministério da Infraestrutura (MInfra), o objetivo do projeto é tornar o processo de embarque nos aeroportos mais eficiente e as viagens aéreas mais seguras. Para garantir os resultados, estão sendo realizados projetos piloto em vários aeroportos do País. No momento, o projeto já foi implementado nos aeroportos de Florianópolis (SC), Salvador (BA), Belo Horizonte (Confins), Santos Dumont (RJ) e Congonhas (SP) (Serpro, 2021, s.p.).

A finalidade do serviço é a segurança da informação, a prevenção de fraudes, o aumento da proteção à integridade física no transporte aéreo, a facilitação do transporte aéreo, o aumento da eficiência e da velocidade dos processos aeroportuários. Além disso, os dados coletados durante o piloto serão utilizados para estudos estatísticos visando à melhoria do serviço (2021, s.p.).

O projeto encontra-se alinhado com as principais iniciativas e projetos internacionais do setor, como Programa de Identificação de Viajantes (*Traveller Identification Programme – TRIP*) da Organização da Aviação Civil Internacional (OACI) e *One ID* da Associação Internacional do Transporte Aéreo (IATA) (2021, s.p.).

De acordo com a Serpro, o uso de todas as informações coletadas está alinhado à Lei Geral de Proteção de Dados Pessoais (LGPD). No *site* do projeto, é possível identificar a área "Aviso de Privacidade", em que encontram o nome e o endereço do controlador, o nome e o endereço do encarregado de dados, informações gerais sobre o tratamento dos dados, dados de oferta do serviço, geração de dados de *login* e direito dos titulares de dados (2021, s.p.). Nesse contexto, a empresa afirma que, em relação ao tratamento de dados, atua em consonância com

> [...] sua missão institucional, respeitando o direito fundamental à privacidade e visando o melhor uso da tecnologia da informação para a satisfação da sociedade e de seus clientes, e a sustentabilidade e autonomia empresarial, garantindo a segurança, estabilidade e a continuidade de seus serviços. (2021, s.p.)

A Serpro afirma que busca garantir que os dados pessoais sejam tratados sempre em conformidade com as bases legais da LGPD e garante que os dados são tratados estritamente para as finalidades informadas, sem desvio na direção de outros propósitos. Com relação às bases legais para o tratamento de dados, a empresa reconhece como bases legais o cumprimento de obrigação legal, a execução de políticas públicas, o legítimo interesse ou a

garantia da prevenção à fraude e à segurança do titular, dentre as hipóteses previstas nos arts. 7º e 11 da LGPD (2021, s.p.).

Quando o assunto é a segurança da informação e privacidade, a empresa informa que adota controles e procedimentos de segurança de forma a assegurar a confidencialidade, integridade, disponibilidade e privacidade dos dados sob sua responsabilidade. (2021, s.p.).

Em relação ao compartilhamento de dados coletados, a Serpro informa que compartilha com operadores e terceiros. As empresas fornecedoras de equipamentos biométricos são consideradas operadores de dados pessoais, pois tratam dados em nome do controlador. Os dados pessoais compartilhados com estes operadores são apenas aqueles necessários para o funcionamento dos equipamentos biométricos no contexto do tratamento (foto frontal, com data/hora e sigla do aeroporto onde foi coletada; dados do cartão de embarque: número do voo, nome, data, trecho), na medida em que apenas capturam tais dados, transmitem e recebem uma resposta de ação a ser executada. Nem todos os dados mencionados são tratados por todos os operadores indicados. A finalidade do compartilhamento com tais operadores guarda relação com o próprio objetivo do serviço Embarque Mais Seguro, já que, para a viabilização deste, é necessária a participação de fornecedores especializados neste tipo de equipamento (2021, s.p.).

Em relação aos terceiros, a empresa informa que os dados tratados durante o processo são compartilhados com a Secretaria de Aviação Civil (SAC/MInfra), que possui a finalidade pública de administrar a aviação civil no território nacional e executar, dentro de suas competências legais, estudos e análises estatísticas baseadas nos dados coletados no projeto em questão. A base legal é a prevista no art. 7º, III, da LGPD, definida nas situações de tratamento e uso compartilhado de dados necessários à execução de políticas públicas (2021, s.p.).

A Serpro informa que todos os agentes de tratamentos e terceiros participantes do projeto firmam termo de tratamento de dados pessoais em que são estipulados os deveres e as responsabilidades dos participantes. Apesar de a página da Serpro indicar que o projeto está alinhado à Lei Geral de Proteção de Dados, na prática não é exatamente o que ocorre (2021, s.p.).

Consoante informações do Instituto de Referência em Internet e Sociedade (IRIS), pesam sobre o projeto Embarque Mais Seguro vários questionamentos relativos ao tratamento dos dados pessoais. Tais questionamentos incluem a legitimidade do compartilhamento de dados entre o Denatran

e o Serpro, até a ausência de esclarecimentos sobre a tecnologia utilizada no Programa e, por fim, informações relativas e elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) (IRIS, 2020, s.p.).

Neste contexto, serão abordadas brevemente algumas lacunas nas informações da Serpro e do MInfra sobre a tecnologia de reconhecimento facial em aeroportos e o projeto Embarque Mais Seguro. De acordo com o IRIS, a elaboração do RIPD deve ocorrer antes do tratamento de dados pessoais dos titulares. O Instituto questiona se

> [...] foi feito um relatório de impacto pelo Ministério da Infraestrutura e Serpro antes de ser feito qualquer teste com pessoas naturais no Aeroporto Internacional de Florianópolis? Se sim, por que o relatório de impacto não foi publicizado ou por que ele não foi sequer mencionado? Se não, por que o relatório de impacto não foi elaborado? (2020, s.p.)

Ambos, Serpro e MInfra, estão sujeitos às obrigações da LGPD como agentes de tratamento de dados pessoais. Sobre o tema, o IRIS lembra o caso do IBGE de compartilhamento de dados, que foi julgado pelo Supremo Tribunal Federal (STF) em 2020 – na ADIn 6387/2020. O caso consolidou o entendimento de que, em situações que irão envolver o tratamento de um grande volume de dados pessoais da população brasileira, é fundamental que um Relatório de Impacto seja elaborado antes de qualquer operação de tratamento (2020, s.p.). No caso do Embarque Mais Seguro, já houve o compartilhamento da base de dados do Denatran com a Serpro e não é possível, inclusive, saber se foi realizado um relatório de impacto para avaliar os riscos associados a esse compartilhamento (2020, s.p.).

Na visão do Laboratório de Políticas Públicas e Internet (LAPIN), o emprego irrestrito de tecnologias de vigilância impacta negativamente os direitos fundamentais dos indivíduos. Isso porque, além dos impactos diretos sobre a privacidade, o tratamento de dados advindo do uso de tais tecnologias tende a refletir vieses algoritmos que reforçam discriminações e a impactar o direito à proteção de dados da população. As avaliações de risco, portanto, são instrumentos a serem utilizados pelos agentes de tratamento para discernir sobre a licitude da atividade e compreender os riscos que se impõem (Lapin, 2021, p. 31).

Outro ponto de questionamento é por que a base de dados do Denatran foi compartilhada com a Serpro e está sendo usada para verificação de identidade dos passageiros nos aeroportos por meio de tecnologias de reconhecimento facial. Consoante o Instituto, a base de dados do

Denatran possui atualmente dados pessoais de cerca de 78 milhões de pessoas. Essa mesma base de dados foi alvo de controvérsias anteriores, como, por exemplo, o vazamento de dados em 2019 no Detran RN e no Detran RJ, além da solicitação pela Agência Brasileira de Inteligência (ABIN) à Serpro de todas as CNHs no Brasil (2020, s.p.).

Por fim, o IRIS entende que o País precisa, urgentemente, mudar a mentalidade de desenho e implementação de políticas públicas que se valem de tecnologias como as de reconhecimento facial, a fim de que a garantia dos direitos possa ser preservada e avanços na prestação de serviços públicos possam ser feitos, desde que sempre resguardados os direitos de todas as pessoas envolvidas (2020, s.p.). Conforme o Relatório do Instituto, a postura que vem sendo adotada é sempre "compartilhar bases de dados, implementar tecnologias de reconhecimento facial e depois pensar em talvez fazer um relatório de impacto, e isso precisa urgentemente mudar" (2020, s.p.).

No Brasil, outro uso comum de TRF em aeroportos é o da Receita Federal (RFB). Desde 2016, a Receita utiliza o sistema de reconhecimento facial da empresa NEC em 14 aeroportos internacionais, como os de Brasília, Guarulhos, Recife, Rio de Janeiro e Salvador (NEC, 2016, s.p.). A contratação ocorreu via licitação, pela modalidade de pregão eletrônico, e o valor do contrato foi de R$ 7.576.090,72 (Brasil, 2015, s.p.).

O objeto do contrato foi o fornecimento de solução de TRF para localizar viajantes com risco aduaneiro identificado. Dessa forma, "os servidores dos órgãos de controle podem identificar inequivocamente os indivíduos de potencial interesse (previamente selecionados pelo sistema de gerenciamento de risco) e encaminhá-los para fiscalização minuciosa" (Lapin, 2021, p. 61).

Para tanto, a Receita informou que

> a solução tecnológica se processa exclusivamente de forma interna no ambiente computacional da RFB, que é acessado apenas por servidores públicos cadastrados com certificado digital. A RFB não compartilha os dados da solução de reconhecimento facial nem com a iniciativa privada nem com outro órgão público.

Ainda, a Receita afirmou que não existem mecanismos no sistema para extrair os dados coletados mediante solicitação do titular (Lapin, 2021, p. 61).

Há, ainda, o projeto piloto de Cidades Inteligentes, que inclui sistema inteligente de controle, monitoramento e segurança, chamado Fronteira Tech, inaugurado em dezembro de 2019, em parceria com a Receita Federal e o Instituto de Desenvolvimento Tecnológico. O projeto funciona de forma integrada com o banco de dados da Receita Federal e reforça o controle aduaneiro na Ponte da Amizade, em Foz do Iguaçu (PR), na fronteira entre Brasil e Paraguai, e utiliza:

– 35 luminárias inteligentes, com duas câmeras em cada, totalizando 70 equipamentos com capacidade de fazer reconhecimento facial e identificar placas de automóveis;

– 4 câmeras fixas com as mesmas tecnologias instaladas em pontos estratégicos;

– 15 luminárias de LED com telegestão e GPS;

– 11 sensores de tiro;

– *software* de inteligência artificial que identifica padrões e gera dados que ajudam no combate ao contrabando e ao tráfico de drogas e armas;

– identifica e alerta para a placa de um veículo roubado e a identificação facial para procurados da justiça (ABDI, 2021a, s.p.).

Em setembro de 2021, o projeto foi implementado nas áreas de fronteira de Pacaraima, em Roraima (RR), na divisa do Brasil com a Venezuela. O investimento da Agência Brasileira de Desenvolvimento Industrial (ABDI) na região de Pacaraima é da ordem de R$ 3,1 milhões. Os recursos são destinados à instalação e manutenção dos equipamentos, que incluem luminárias inteligentes com dimerização (10); luminárias inteligentes com câmeras de vigilância integradas (20); *software* de reconhecimento facial; câmeras de sensoriamento do tipo *speed dome* (4); *datacenter* para armazenamento e processamento de imagens e dados; telas de *videowall*; câmeras de reconhecimento de placas de veículos (4); *software* de reconhecimento de placas; drone com câmera termográfica, além da licença dos *softwares* por três anos (ABDI, 2021b, s.p.).

Nos casos acima mencionados, portanto, é possível notar a utilização e a implementação de algoritmos em diferentes momentos do processo migratório. Uma das finalidades observadas seria aquela de acelerar e/ou facilitar os processos migratórios; contudo, há risco com respeito à possi-

bilidade de erro do sistema[13]. Identificar uma pessoa como sendo outra ou simplesmente não a identificar pode levar a situações de discriminação ou restrição injustificada de direitos. O reconhecimento facial corre o risco de ser transformado em arma pela aplicação da lei contra comunidades marginalizadas em todo o mundo. De Nova Delhi a Nova York – passando pelo Brasil –, essa tecnologia invasiva poderia "virar nossas identidades contra nós, além de minar os direitos humanos" (Mahmoudi, 2021). Ou seja, perfilar alguém erroneamente em um contexto do controle migratório, por exemplo, pode levar a abordagens e apreensões indevidas, além das violações de direitos humanos[14], e casos de racismo[15], transfobia e islamofobia.

Diante do exposto, compreende-se que o uso de tecnologias de perfilamento no ambiente do controle migratório pode auxiliar na celeridade do processo; entretanto, o uso de sistemas automatizados precisa seguir diretrizes que respeitem os direitos humanos dos migrantes, com ênfase na não discriminação, no tratamento igualitário, na transparência das decisões e na dignidade da pessoa humana.

O TRATAMENTO DOS DADOS PESSOAIS NO CONTEXTO MIGRATÓRIO BRASILEIRO

Os incrementos tecnológicos dos últimos anos criaram modelos sofisticados de tratamentos de dados pessoais. Vivemos em uma sociedade orientada por dados, conhecida como *data-driven society*, em que o uso de serviços de empresas, no campo da comunicação, do comércio, do turismo ou entretenimento, sujeita-se ao tratamento de dados. Garantir a proteção de dados do indivíduo é fundamental nesse contexto (Viola; Heringer; Carvalho, 2021, p. 4).

Na visão de Samuel Oliveira, nos últimos anos também se intensificaram as discussões sobre a questão da segurança. Nesse cenário, ganhou

13 ROGERS, Lindsay. *Facial recognition technology at airports isn't even working*. Publicado em: 15 fev. 2021. Disponível em: https://www.insidehook.com/daily_brief/travel/airport-facial-recognition-not-working. Acesso em: 6 dez. 2021.

14 No documentário *Coded Bias*, disponível na plataforma de *streaming* Netflix, a pesquisadora Joy Buolamwini apresenta um relato técnico e ao mesmo tempo uma denúncia social acerca dos vieses presentes em algoritmos de reconhecimento facial.

15 *Conforme Bruno Souza, a maioria das câmeras que fazem reconhecimento facial na cidade do Rio de Janeiro foram instaladas no bairro de Copacabana – o cartão-postal da cidade. No segundo dia do uso, uma mulher foi presa ao ser identificada erroneamente pelo sistema, que apontou mais de 70% de semelhança entre ela e Maria Leda, uma pessoa foragida da Justiça. Entretanto, a verdadeira criminosa estava presa desde 2015. As polícias militar e civil do Rio de Janeiro utilizaram um banco de dados desatualizado. Esse caso é emblemático porque expõe a falha da máquina de leitura biométrica facial e a irresponsabilidade por parte da secretaria de segurança pública (Souza, 2021).*

força a ideia de que um afrouxamento na proteção de dados pessoais seria uma maneira eficaz de se combater a violência e até mesmo o terrorismo (Oliveira, 2021, p. 133). Para Stefano Rodotà, se seguirmos esse raciocínio, "a questão corre o risco de ser posta de maneira imprópria, como se segurança e proteção de dados fossem valores incompatíveis e como se a tutela de um excluísse automaticamente qualquer relevância do outro" (Rodotà, 2004, p. 95).

A tutela do direito à proteção de dados e à privacidade dos migrantes explicita uma questão latente na regulação jurídica do tema, que é a da composição e tensão entre os direitos do titular dos dados e o interesse público ou estatal (Gediel; Corrêa, 2021 p. 619). Diante do exponencial progresso do uso de sistemas automatizados de decisão no ambiente do controle migratório, surgem preocupações quanto aos seus riscos e aos meios regulatórios adequados. Nesse cenário, faz-se necessário destacar que existem os seguintes tratamentos de dados no contexto migratório: (i) o tratamento de dados pessoais realizado por companhias aéreas para a execução dos seus serviços; (ii) o tratamento com o objetivo da segurança pública[16]; e também (iii) o tratamento voltado para a segurança nacional[17].

Inicialmente, cabe lembrar que o arcabouço legislativo nacional já conta com normativas que versam sobre a proteção da privacidade, seja na esfera constitucional, seja na infraconstitucional. Nesta senda, destacam-se a Constituição Federal de 1988 (que apontou a inviolabilidade da vida privada, o sigilo das comunicações, além do *habeas data* como instrumento

16 A segurança pública tem um capítulo próprio na Constituição Federal de 1988, que está contido no Título V, "Da Defesa do Estado e das Instituições Democráticas". O capítulo III do Livro V, "Da Segurança Pública", consigna somente o art. 144, onde se extrai a definição constitucional do conceito de segurança pública, explícita no *caput*: "A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio" (Brasil, 1988). Ao atribuir ao Estado o dever pela segurança pública, reconhece-o como serviço público a ser garantido pela máquina estatal, direito inalienável de todos os cidadãos. Já a definição da segurança também como responsabilidade de todos pode ser interpretada à luz da necessidade de que haja participação social nas políticas públicas relacionadas a esse campo. Adicionalmente, é possível compreender que a segurança pública não pode ser vista apenas como atribuição do Estado, uma vez que a sociedade tem um papel importante não somente na participação e no controle das políticas, como também na socialização dos indivíduos, na perpetuação dos mecanismos informais de controle social e de autocontrole, a partir da perspectiva de que não é somente o controle pelo Estado que garante a segurança de todos (Fontoura; Rivero; Rodrigues, 2015, p. 143).

17 Segurança nacional não se confunde com segurança pública. Entende-se aqui segurança nacional como um estado em que se percebe, materialmente: a) a estabilidade e a inviolabilidade dos limites fronteiriços do Estado; b) a capacidade de se traduzir a soberania nacional, bem como a capacidade nacional de projetar poder no exterior, em um conjunto de medidas que proporcione ganhos sociais e econômicos para a população nacional; c) a solidez e a impessoalidade do sistema constitucional, assim como sua impermeabilidade em relação a pressões externas; e d) a garantia da previsibilidade legal das relações político-eleitorais e econômicas (Costa, 2018, p. 124-125).

apto a assegurar a proteção de informações e dados pessoais), o Código Civil de 2002 (que protege diretamente a vida privada), o Código de Defesa do Consumidor de 1990 (que o faz, dedicando a Seção VI à proteção de bancos de dados e de cadastros dos consumidores), além do Marco Civil da Internet de 2014, que trouxe dispositivos destinados à proteção da privacidade, que, por sua vez, constitui um dos pilares da lei.

A própria Lei de Migração (Lei nº 13.445/2017) faz referência expressa ao direito de proteção de dados pessoais do migrante e lhe assegura, em seu art. 4º, XIII, direito à informação e à confidencialidade, com remissão ao disposto na Lei de Acesso à Informação (LAI – Lei nº 12.527/2011). A LAI estabeleceu as regras para o tratamento dos dados pessoais pelo Poder Público, que fica submetido ao dever de transparência e de respeito à "[...] à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" (art. 31 da Lei nº 12.527/2011). A tutela de tais direitos deve ser pensada na sua vinculação aos princípios da Lei de Migração, previsto em seu art. 3º, sobretudo na vedação à xenofobia, à discriminação e à criminalização da migração (Brasil, 2017; Brasil, 2011).

Além disso, está em tramitação, no Congresso Nacional, o Projeto de Emenda Constitucional (PEC) nº 17/2019, aprovado pela Câmara e em tramitação no Senado e que visa incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, além de fixar a competência privativa da União para legislar sobre a proteção e tratamento de dados pessoais (Senado, 2021, s.p.).

Se o País já conta com tantas legislações sobre o tema, por que criar mais uma? Na visão de Eduardo Magrani, a regulação existente é insuficiente para "proteger os dados pessoais e a privacidade em suas mais diversas facetas. Daí a importância da LGPD, que veio preencher as lacunas da legislação e é aplicável a uma gama mais ampla de usos da internet" (2019, p. 87).

Nesta senda, pontua-se que a Lei nº 13.709, de 14 de agosto de 2018, conhecida como Lei Geral de Proteção de Dados (LGPD), foi influenciada por legislações semelhantes adotadas nos Estados Unidos da América (EUA) – a *California Consumer Privacy Act* (CCPA) – e na União Europeia, denominada *General Data Protection Regulation* (GDPR) e segue a tendência mundial do aumento do foco em privacidade e proteção de dados.

Na visão do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio), a LGPD trouxe um novo paradigma que passou a fundamentar a

abordagem do direito à privacidade, centrado no ideal de autodeterminação informativa, autonomia e controle do cidadão de seus dados. Esse novo ambiente regulatório busca harmonizar a proteção dos direitos dos indivíduos e a provisão de segurança jurídica nas relações permeadas pelo tratamento de dados pessoais, em um mundo hiperconectado e marcado pelo vigilantismo (ITS, 2021, s.p.).

O primeiro cenário (o tratamento de dados pessoais realizados por companhias aéreas) é contemplado pela LGPD, considerando que a lei dispõe sobre o

> tratamento de dados pessoais, inclusive nos meios digitais, [...] *por pessoa jurídica de direito público ou privado*, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Brasil, 2018, s.p. – grifos nossos)

O segundo e o terceiro cenários, por sua vez, não encontram proteção na LGPD. Neste cenário, é preciso pontuar que, no momento da construção da lei, os legisladores preferiram deixar de fora o tratamento de dados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, conforme disposto no art. 4º, III, da LGPD.

O § 1º do artigo em comento afirma que o tratamento de dados pessoais "previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta lei" (Brasil, 2018, s.p.).

As peculiaridades dessa lei específica são justificadas pelo desafio de se garantir um equilíbrio entre a investigação penal, atividade que demanda tratamento de dados de diversos atores, e os direitos fundamentais de privacidade e proteção de dados (Costa; Reis, 2021, s.p.). Nesse contexto, é preciso compreender que não há dados pessoais insignificantes e que há

> um direito autônomo à proteção de dados pessoais e o seu duplo efeito sobre os deveres do Estado (um dever negativo de não interferir indevidamente no direito fundamental e um dever positivo de adotar medidas positivas para a proteção desse direito). (Mendes, 2020, s.p.)

Em novembro de 2020, um anteprojeto de lei sobre a temática foi apresentado à Presidência da Câmara dos Deputados, conhecido como Anteprojeto da LGPD Penal. O anteprojeto possui doze capítulos e 68

artigos, divididos em oito eixos temáticos: (i) âmbito de aplicação da lei; (ii) condições de aplicação; (iii) base principiológica; (iv) direitos e obrigações; (v) segurança da informação; (vi) tecnologias de monitoramento; (vii) transferência internacional de dados; e (viii) a autoridade de supervisão.

O texto teve duas inspirações principais: a LGPD e a Diretiva nº 2016/680 da União Europeia, cujo objeto é similar àquele do anteprojeto. Especificamente para o capítulo VII, sobre tecnologias de monitoramento, a inspiração veio de leis estadunidenses da cidade de Nova York e do estado de Washington (Costa; Reis, 2021, s.p.).

O anteprojeto regula somente as alíneas *a* e *d* (segurança nacional e atividades de investigação e repressão de infrações penais, respectivamente), deixando para regulação posterior as alíneas *b* e *c*, referentes aos tratamentos de dados para defesa nacional e segurança do Estado. Essa lacuna demanda a criação de regulação o mais brevemente possível, a fim de proteger, de forma adequada, os direitos dos titulares de dados individual e coletivamente.

Na visão de Laura Schertel Mendes, relatora da comissão de juristas instituída para elaboração do anteprojeto, é preciso refletir sobre a possibilidade de expandir e incluir as alíneas *b* e *c*, podendo, assim, ser transformadas em um capítulo à parte do atual anteprojeto. A relatora entende que é difícil avançar em alguns termos no contexto nacional, entre eles o da defesa nacional e da segurança do Estado (2021, s.p.).

O texto do anteprojeto é um bom ponto de partida para o debate fundamental sobre a relevância de se regular uma participação mais ativa e transparente no controle e acesso às informações dos titulares aos seus dados, em especial no caso de dados sensíveis e biométricos, como o uso de tecnologias de reconhecimento facial. O texto estabelece requisitos e limitações aos usos admissíveis dos dados pessoais por parte das autoridades, cria obrigações de transparência a serem respeitadas pelos controladores de dados e prevê a elaboração de relatórios de impacto na ocasião do tratamento de dados pessoais sensíveis (ITS, 2020, p. 8). O documento prevê ainda a necessidade de os sistemas responsáveis por decisões automatizadas serem auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia (ITS, 2020, p. 9).

Atualmente, o anteprojeto encontra-se na Câmara dos Deputados à espera de um parlamentar que o apresente formalmente, tornando-o, assim, um projeto de lei (PL). Após, o futuro PL seguirá os trâmites comuns do pro-

cesso legislativo, sendo submetido à avaliação das mais diversas comissões, votado, enviado ao Senado e submetido à sanção presidencial (Costa; Reis, 2021, s.p.).

Em razão de todo o exposto, percebe-se que o tratamento de dados pessoais no âmbito do controle migratório encontra-se em uma zona cinzenta. Dos três cenários apresentados no início do tópico, apenas o primeiro apresenta uma regulamentação específica, ou seja, o tratamento de dados pessoais realizado por companhias aéreas para a execução dos seus serviços deve seguir as orientações da Lei Geral de Proteção de Dados. Os outros dois cenários ainda não são regulamentados.

O segundo cenário, do tratamento de dados pessoais com o objetivo da segurança pública, deverá seguir as orientações do Anteprojeto da LGPD Penal, que ainda está em tramitação, e que, sem dúvidas, poderá sofrer modificações até a sua entrada em vigor. Por fim, o terceiro cenário, do tratamento voltado para a segurança nacional, ainda não possui uma legislação específica ou sequer um projeto de lei em andamento, configurando, portanto, uma lacuna no ordenamento jurídico brasileiro.

Por fim, compreende-se que a regulação estatal é condição urgente para sustentar o próprio papel evolutivo das tecnologias empregadas em sistemas de decisões automatizadas e garantir a defesa do humano ao revés dos danos que tais sistemas porventura possam causar.

CONSIDERAÇÕES FINAIS

O aumento exponencial dos fluxos migratórios e a utilização crescente do uso massivo das tecnologias digitais, para incrementar o controle nas fronteiras, trazem à tona o debate sobre a proteção dos dados pessoais dos migrantes. Nas iniciativas do Reino Unido e Canadá, pode-se notar a utilização e implementação de algoritmos em diferentes momentos do processo migratório. Uma das finalidades observadas seria aquela de acelerar e/ou facilitar os processos migratórios; entretanto, também é possível identificar a possibilidade de usos diversos desses sistemas automatizados, como a discriminação baseada em dados de origem, raça e gênero.

Trata-se de temáticas de extrema complexidade, que envolvem desde os movimentos migratórios, a coleta e tratamento de dados pessoais, as decisões automatizadas e a sociedade da vigilância, além dos avanços de novas tecnologias de perfilamento. Diante do exposto, compreende-se que as decisões automatizadas realizadas no âmbito de controle migratório não

apenas têm o potencial de discriminar migrantes, como provavelmente já o vem fazendo desde sua implementação. Possíveis soluções para que estes sistemas passem a atribuir um tratamento igualitário a migrantes, respeitando convenções internacionais que estabelecem a não discriminação e igualdade entre pessoas, consistiriam na maior transparência sobre as variáveis usadas para as decisões tomadas, bem como na inclusão e constante atualização de variáveis que não estivessem somente vinculadas a bases de dados de decisões pretéritas (Schippers; Gagliardi, 2021).

Neste contexto, compreende-se que o Direito precisa estar atento aos avanços tecnológicos, e, no que diz respeito à proteção de dados pessoais, é preciso considerar, além do princípio da dignidade da pessoa humana, a "finalidade, pertinência, proporcionalidade, simplificação, harmonização e necessidade" (Rodotà, 2008, p. 10).

Por fim, conclui-se a contribuição com uma perspectiva referente a novos desafios e novas abordagens: em um primeiro momento, compreende-se que é preciso buscar a criação de algoritmos isentos de vieses, que garantam a isonomia nas decisões automatizadas, inclusive de cunho migratório. Na sequência, entende-se que é necessário regular o tratamento dos dados pessoais no contexto migratório, em especial no que diz respeito ao tratamento de dados pessoais para segurança pública e para segurança nacional, considerando as lacunas da Lei Geral de Proteção de Dados e o andamento do Anteprojeto da LGPD Penal.

REFERÊNCIAS

ABDI. *Fronteira Tech*. 2021a. Disponível em: https://www.abdi.com.br/projetos/fronteira-tech. Acesso em: 20 set. 2021.

_____. *Fronteira Tech é lançado em Roraima*. 2021b. Disponível em: https://www.abdi.com.br/postagem/fronteiratech-e-lancado-em-roraima. Acesso em: 20 set. 2021.

ACNUR. *Dados sobre refúgio*. Publicado em: 18 jun. 2021. Disponível em: https://www.acnur.org/portugues/dados-sobre-refugio/. Acesso em: 17 set. 2021.

BAUMAN, Zygmunt; LYON, David. *Vigilância líquida*. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BANCO MUNDIAL. *World Development Report 2021*. Disponível em: https://wdr2021.worldbank.org/stories/crossing-borders/. Acesso em: 21 set. 2021.

BARNET. *Joint Council for the Welfare of Immigrants*. Disponível em: https://www.barnet.gov.uk/directories/directme/joint-council-welfare-immigrants. Acesso em: 30 nov. 2021.

BBC NEWS. *Home Office drops "racist" algorithm from visa decisions*. Publicado em: 4 ago. 2020. Disponível em: https://www.bbc.com/news/technology-53650758. Acesso em: 21 mar. 2021.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 dez. 2021.

_____. *Contrato RFB-Copol nº 22-2015*. Disponível em: http://receita.economia.gov.br/sobre/licitacoes-e-contratos/contratos-deti/2015/contrato-rfb-copol-no-22-2015-nec.pdf/view. Acesso em: 10 set. 2021.

_____. *Lei nº 12.527, de 18 de novembro de 2011*. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em:
20 set. 2021.

_____. *Lei nº 13.445, de 24 de maio de 2017*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm. Acesso em: 20 set. 2021.

_____. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 set. 2021.

BRUNO, Fernanda. Entrevista: Fernanda Bruno. Vigilância hoje. *Revista Dispositiva*, v. 2, n. 1, maio 2013/out. 2013. Disponível em: http://periodicos.pucminas.br/index.php/dispositiva/article/download/6091/5680. Acesso em: 10 set. 2021.

COSTA, Eduarda; REIS, Carolina. *Histórico da LGPD Penal*: o que foi feito até aqui e quais são os próximos passos? Publicado em: 16 abr. 2021. Disponível em: https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/. Acesso em: 23 set. 2021.

COSTA, Frederico Carlos de Sá. Sobre o conceito de "segurança nacional". In: *Tensões Mundiais*, [s.l.], v. 5, n. 9, p. 123-140, 2018. DOI: 10.33956/tensoesmundiais.v5i9jul/dez.670. Disponível em: https://revistas.uece.br/index.php/tensoesmundiais/article/view/670. Acesso em: 7 dez. 2021.

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

EUROPEAN COMMISSION. Article 29 Working Party. Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679, 17/EN, WP251rev.01, Oct. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/items/612053. Acesso em: 16 set. 2021.

FONTOURA, Natália de Oliveira; RIVERO, Patricia Silveira; RODRIGUES, Rute Imanishi. Segurança pública na Constituição Federal de 1988: continuidades e perspectivas. In: *IPEA*. Políticas sociais: acompanhamento e análise – Vinte anos da Constituição Federal, v. 3, 2009. Disponível em: https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=5606. Acesso em: 7 dez. 2021.

FOXGLOVE. *Who we are*. Disponível em: https://www.foxglove.org.uk/who-we-are/. Acesso em: 30 nov. 2021.

FRAZÃO, Ana. *Discriminação algorítmica*: a relação entre homens e máquinas. Publicado em: 28 jul. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-a-relacao-entre-homens-e-maquinas-28072021. Acesso em: 16 set. 2021.

GEDIEL, José Antônio Peres; CORRÊA, Adriana Espíndola. Proteção de dados pessoais nos processos migratórios. In: BIONI, Bruno et al. *Tratado de proteção de dados pessoais*. Forense. Edição do Kindle. 2021.

GILLIOM, John; MONAHAN, Torin. *Supervision*: an introduction to the surveillance society. Chicago: The University of Chicago Press, 2013.

HEAVEN, Will Douglas. The UK is dropping an immigration algorithm that critics say is racist. *MIT Technology Review*. Publicado em: 5 ago. 2020. Disponível em: https://www.technologyreview.com/2020/08/05/1006034/the-uk-is-dropping-an-immigration-algorithm-that-critics-say-is-racist/. Acesso em: 21 mar. 2021.

HILDEBRANDT, Mireille. Defining profiling. A new type of knowledge. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge. *Profiling the European Citizen*: cross-disciplinary perspectives, Londres: Springer, p. 17-44, 2008. Disponível em: https://www.researchgate.net/publication/226744267_Defining_Profiling_A_New_Typ e_of_Knowledge. Acesso em: 10 set. 2021.

IRIS. *Programa Embarque Seguro*: reconhecimento facial em aeroportos no Brasil. Publicado em: 2 dez. 2020. Disponível em: https://irisbh.com.br/programa-embarque-seguro-questionamentos-sobre-reconhecimento-facial-em-aeroportos-no-brasil/. Acesso em: 28 set. 2021.

ITS. *Comentários ao Anteprojeto de Lei de Proteção de Dados para a Segurança Pública*: tecnologia de reconhecimento facial. Disponível em: https://itsrio.org/pt/publicacoes/comentarios-ao-anteprojeto-de-lei-de-protecao-de-dados-para-a-seguranca-publica/. Acesso em: 20 set. 2021.

JUMPER, John; EVANS, Richard; PRITZEL, Alexander et al. Highly accurate protein structure prediction with AlphaFold. *Editorial Nature*, 596, 2021.

KAUFMAN, Dora. *A inteligência artificial irá suplantar a inteligência humana?* Barueri: Estão das Letras e Cores, 2019.

LAPIN. *Vigilância automatizada*: uso de reconhecimento facial pela Administração Pública. Publicado em: jul. 2021. Disponível em: https://lapin.org.br/2021/07/07/

vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/. Acesso em: 20 set. 2021.

LINDEN, Greg; SMITH, Brent; YORK, Jeremy. Amazon.com recommendations: item-to-item collaborative filtering. *IEEE Internet Computing*, v. 7, 2003.

MAGRANI, Eduardo. *Entre dados e robôs*: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MAHMOUDI, Matt. *Ban dangerous facial recognition technology that amplifies racist policing*. Publicado em: 26 jan. 2021. Disponível em: https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing/.

MARRAFON, Marco; MEDON, Filipe. *Importância da revisão humana das decisões automatizadas na Lei Geral de Proteção de Dados*. Publicado em: 9 set. 2019. Disponível em: https://www.conjur.com.br/2019-set-09/constituicao-poder-importancia-revisao-humana-decisoes-automatizadas-lgpd. Acesso em: 7 dez. 2021.

MCCARTHY, John et al. *A proposal for the Dartmouth summer conference on artificial intelligence* – Conference Announcement for the seminal meeting on AI, 1955. Disponível em: http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html. Acesso em: 24 out. 2021.

MCCULLOCH, Warren Sturgis; PITTS, Walter. *A logical calculus of the ideas immanent in nervous activity*. Grã-Bretanha: Bulletin of Mathematical Biophysics 5, 1943.

MENDES, Laura Schertel. *Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal*: construção, temas e perspectivas. Publicado em: 26 abr. 2021. Disponível em: https://www.anymeeting.com/916-078-548/EA54DC89884C3F. Acesso em: 27 abr. 2021.

_____. *Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais*. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 20 set. 2021.

MINSKY, Marvin. *A Neural-Analogue Calculator Based upon a Probability Model of Reinforcement*. Massachusetts: Harvard University Psychological Laboratories, 1952.

MOLNAR, Petra; GILL, Lex. *Bots at the gate*: a human rights analysis of automated decision-making in Canada's immigration and refugee system. International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto, 2018). Disponível em: https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf. Acesso em: 21 mar. 2021.

MOZUR, Paul. Inside China's dystopian dreams: A.I., shame and lots of cameras. *The New York Times*. Publicado em: 7 ago. 2018. Disponível em: https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html. Acesso em: 22 set. 2021.

NAUMANN, Felix. *Data profiling revisited*. 2014. ACM SIGMOD Record, 42. Disponível em: https://dl.acm.org/doi/10.1145/2590989.2590995. Acesso em: 27 abr. 2021.

NEC. *Receita Federal utilizará tecnologia de identificação facial da NEC em 14 aeroportos internacionais do País*. 2016. Disponível em: https://br.nec.com/pt_BR/press/PR/20160409060302_11186.html. Acesso em: 10 set. 2021.

OLIVEIRA, Samuel R. de. *Sorria, você está sendo filmado!*: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

ONG, Thuy. *Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints*. Publicado em: 10 out. 2017. Disponível em: https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium. Acesso em: 22 set. 2021.

PEIXOTO, Fabiano Hartmann. Direito e inteligência artificial na (não) redução de desigualdades globais: decisões automatizadas na imigração e sistemas de refugiados. *Revista Direitos Culturais*, Santo Ângelo, v. 15, n. 37, set./dez. 2020. Disponível em: http://san.uri.br/revistas/index.php/direitosculturais/article/view/222/86. Acesso em: 26 mar. 2021.

QUOC, Viet Le et al. *Building high-level features using large scale unsupervised learning*. In: Proceedings of the 29th International Conference on International Conference on Machine Learning (ICML), 2012. Edimburgo, Escócia.

RAVURI, Suman; LENC, Karel; WILLSON, Matthew et al. Skilful precipitation nowcasting using deep generative models of radar. *Editorial Nature*, 597, p. 672, 2021.

RICH, Elaine; KNIGHT, Kevin. *Artificial intelligence*. 2. ed. Nova Iorque: McGraw-Hill, 1991.

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

_____. Transformações do corpo. *Revista Trimestral de Direito Civil*, v. 19, n. 5, p. 91-107, 2004.

ROSENBLATT, Frank. *Principles of neurodynamics*: perceptions and the theory of brain mechanism. Buffalo: Cornell Aeronautical Lab Inc., 1961.

SCHIPPERS, Laurianne-Marie; GAGLIARDI, Marília Papaléo. *Inteligência artificial e controle migratório*: algoritmos podem discriminar migrantes? Publicado em: 16 jan. 2021. Disponível em: https://medium.com/o-centro-de-ensino-e-pesquisa-em-

inova%C3%A7%C3%A3o-est%C3%A1/intelig%C3%AAncia-artificial-e-controle-migrat%C3%B3rio-algoritmos-podem-discriminar-migrantes-85d04d152440. Acesso em: 10 set. 2021.

SEI. *Barramento de Serviços do PEN*. Disponível em: https://portalsei.df.gov.br/barramento/. Acesso em: 7 dez. 2021.

SENADO. *PEC que inclui a proteção de dados pessoais na Constituição volta para o Senado*. Publicado em: 3 set. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/09/03/pec-que-inclui-a-protecao-de-dados-pessoais-na-constituicao-volta-para-o-senado. Acesso em: 20 set. 2021.

SERPRO. *Embarque + seguro*. Disponível em: https://campanhas.serpro.gov.br/embarque-mais-seguro/. Acesso em: 20 set. 2021.

SOLOVE, Daniel J. *Understanding privacy*. Cambridge: Harvard University Press, 2008.

SOUZA, Bruno. *Panóptico: reconhecimento facial renova velhas táticas racistas de encarceramento.* Publicado em: 22 abr. 2021. Disponível em: http://observatorioseguranca.com.br/panoptico-reconhecimento-facial-renova-velhas-taticas-racistas-de-encarceramento/. Acesso em: 6 dez. 2021.

UNIÃO EUROPEIA. Parlamento e Conselho. Regulamento (EU) nº 2016/679, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva nº 95/46/CE (Regulamento Geral de sobre Proteção de Dados). *Jornal Oficial da União Europeia,* [s.l.], L 119/1, 4 maio 2016. Disponível em: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434. Acesso em: 10 set. 2021.

UN, Desa. *International Migration 2020 Highlights*. Publicado em: jan. 2021. Disponível em: https://www.un.org/development/desa/pd/sites/www.un.org.development.desa.pd/files/international_migration_2020_highlights_ten_key_messages.pdf. Acesso em: 17 set. 2021.

UNODC. *How Covid-19 restrictions and the economic consequences are likely to impact migrant smuggling and cross-border trafficking in persons to Europe and North America*. Disponível em: https://www.unodc.org/documents/islamicrepublicofiran//2020/05/Covid-related-impact-on-SoM-TiP.PDF. Acesso em: 22 set. 2021.

VIOLA, Mario; HERINGER, Leonardo; CARVALHO, Celina. *O anteprojeto da LGPD Penal e as regras sobre transferência internacional de dados pessoais*. Publicado em: ago. 2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/07/Relatorio-Transferencia-de-dados-pessoais.pdf. Acesso em: 20 set. 2021.

ZUBOFF, Shoshona. *A era do capitalismo de vigilância*: a luta por um futuro humano na nova fronteira do poder. Trad. George Schlesinger. 1. ed. Rio de Janeiro: Intrínseca, 2020.

Sobre as autoras:

Stéfani Reimann Patz | *E-mail:* stefani.patz@hotmail.com

Mestranda em Direitos Especiais pelo Programa de Pós-Graduação *Stricto Sensu* em Direito. Mestrado e Doutorado da Universidade Regional Integrada do Alto Uruguai e das Missões (URI), *Campus* Santo Ângelo/RS. Bolsista Capes/Prosuc. Bacharela em Direito pela URI, *Campus* Santo Ângelo/RS. Pesquisadora voluntária dos projetos de pesquisa "Crisálida: Direito e Arte", "Internet, liberdade de informação, manipulação de comportamentos e a desestabilização do processo democrático" e do Centro de Estudos e Pesquisas em Direito e Tecnologia (Cedetec). Membro do Instituto Nacional de Proteção de Dados (INPD).

Thami Covatti Piaia | *E-mail:* thamicovatti@hotmail.com

Doutora em Direito pela Universidade Federal do Rio Grande do Sul – UFRGS (2013). Contemplada com bolsa da Capes durante o período de Doutoramento e contemplada com bolsa do Programa de Doutorado Sanduíche no Exterior (PDSE) pelo período de onze meses na Universidade de Illinois, *Campus* de Urbana-Champaign – Estados Unidos. Mestre em Direito pela Universidade Regional Integrada do Alto Uruguai e das Missões – URI, *Campus* de Santo Ângelo/RS. Graduada em Direito pela Universidade Regional Integrada do Alto Uruguai e das Missões – URI, *Campus* de Frederico Westphalen/RS. Professora na Graduação e no Programa de Pós-Graduação *Stricto Sensu* em Direito. Mestrado e Doutorado da Universidade Regional Integrada do Alto Uruguai e das Missões – URI, *Campus* de Santo Ângelo/RS. Possui inscrição na Ordem dos Advogados do Brasil.

Data de submissão: 30 de setembro de 2021.
Data de aceite: 7 de dezembro de 2021.