AS VISÕES DA PANDEMIA: drones, reconhecimento facial, vigilância e a mitigação da privacidade

Oniye Nashara Siqueira[1]
Alexandre Celioto Contin[2]
Lucas de Souza Lehfeld[3]
Renato Britto Barufi[4]

RESUMO: A emergência social instituída pela pandemia da COVID-19 tornou o campo fértil para a ascensão acelerada dos veículos aéreos não tripulados, popularmente denominados de drones, ao passo que garantem a coleta de imagens capazes de mensurar aglomerações, identificar infratores de normas sanitárias e auxiliar na conscientização sobre os riscos de contágio e disseminação da doença. No entanto, o uso irrestrito destes equipamentos, aliado às tecnologias de reconhecimento facial, ressignificaram a vigilância estatal, culminando na mitigação da privacidade e direito de imagem pela invocação da saúde e segurança públicas. Concluímos pela necessidade de regulamentação federal do uso do equipamento pelo Poder Público, já que as normativas técnicas existentes, editadas pelas agências reguladoras, mostram-se incapazes de garantir a inviolabilidade dos direitos fundamentais e a proteção de dados pessoais. O presente artigo está amparado em pesquisa quali-quantitativa, bibliográfica e documental.

Palavras-chave: drones, pandemia, privacidade, proteção de dados, reconhecimento facial.

ABSTRACT: The social emergency instituted by the COVID-19 pandemic made the field fertile for the accelerated rise of unmanned aircraft systems, popularly called drones, while guaranteeing the collection of images capable of measuring agglomerations, identifying violators of health standards and assisting in the awareness of the risks of contagion and spread of the disease. However, the unrestricted use of this equipment, combined with facial recognition technologies, has given new meaning to state surveillance, culminating in the mitigation of privacy and image rights by invoking public health and safety. We conclude that there is a need for federal regulation of the use of the equipment by the Public Power, since the existing technical regulations, edited by the regulatory agencies, are unable to guarantee the inviolability of fundamental rights and the protection of personal data. This article is supported by quali-quantitative, bibliographic and documentary research.

Keywords: drones, pandemic, privacy, data protection, facial recognition.

[1] Mestranda em Direitos Coletivos e Cidadania pela Universidade de Ribeirão Preto - UNAERP. Bolsista PROSUP/CAPES. Especialista em Processo Civil pela Universidade de São Paulo - USP. Graduada em Direito pela Universidade de Ribeirão Preto - UNAERP.
[2] Mestrando em Direitos Coletivos e Cidadania pela Universidade de Ribeirão Preto - UNAERP. Especialista em Direito Penal e Processo Penal pela Pontifícia Universidade Católica de Minas Gerais. Advogado.
[3] Professor Pós-Doutor Orientador do Programa de Mestrado em Direitos Coletivos e Cidadania da Universidade de Ribeirão Preto - UNAERP.
[4] Mestrando em Direitos Coletivos e Cidadania pela Universidade de Ribeirão Preto (UNAERP). Especialista em Direito e Processo do Trabalho pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas).Graduado em Direito pela Universidade de Franca (UNIFRAN). Professor convidado da Faculdade de Direito de Franca e da Escola Brasileira de Estudos Jurídicos - Ribeirão Preto em cursos de extensão e pós-graduação. Advogado.

INTRODUÇÃO

As *teletelas* de George Orwell caracterizam a instituição de uma sociedade vigiada pelo *Big Brother* na narrativa trazida na obra "1984 – A Era do Grande Irmão" ORWELL, 2003, p. 301). Nela, o autor emite um alerta aos malefícios da utilização exacerbada da tecnologia enquanto meio de controle social a serviço do Estado. Semelhante alerta é emitido por Bauman ao analisar a pós-modernidade e classificar a vigilância estatal como "líquida", indetectável e inevitável, prevendo que "não haverá abrigo impossível de espionar – para ninguém" (BAUMAN, 2014, p. 19), mormente pela potencialização do uso da tecnologia, destacando, porém, o papel dos veículos aéreos não tripulados (VANTs) ou drones que, segundo alude, "poderão ver tudo, ao mesmo tempo que permanecem confortavelmente invisíveis – em termos literais e metafóricos" (BAUMAN, 2014, p. 20). Em razão da pandemia do novo coronavírus (COVID-19), há um cenário de mobilização mundial que levou países do mundo inteiro a estabelecer medidas excepcionais e urgentes para a contenção do vírus e preservação da saúde das pessoas, como o distanciamento social, uso de máscaras, intensificação das regras sanitárias *et cetera*. Para balizar a tomada de decisões, o Poder Público tem se valido de diversos implementos tecnológicos, dentre os quais destacamos os drones.

A denominação "drone" surge em 1931 e deriva da sonorização típica do equipamento, que se aproxima do som de um zangão, o que motivou a denominação de *Queen Bee* atribuída ao primeiro modelo deste tipo de aeronave Havilland DH 82B, que era operado por controle remoto (BALTAZAR, 2015, p. 28). Características como a capacidade de captação de imagens em alta resolução, compartilhamento de dados em tempo real, deslocamento veloz, alcance geográfico abrangente e possibilidade de controle da rota à distância, são atributos que evidenciam não apenas a capacidade multifacetária do equipamento. A contribuição no combate à crise de saúde instaurada decorre da capacidade dos drones de mensurar aglomerações, identificar infratores das normas sanitárias de distanciamento social e uso de máscaras ou, ainda, auxiliar na conscientização popular acerca dos riscos de contágio e disseminação da infecção.

No entanto, para além deste papel da ferramenta, indissociável examinar os limites da captação e transmissão de dados pelos drones e a possibilidade de interferência nos direitos fundamentais, em especial quanto à preservação da imagem e da privacidade. Afinal, a tensão sem precedentes causada pela pandemia pode possibilitar a instituição de

situações e condutas violadoras em prol de uma visão utilitarista da crise, sob a justificativa de garantia de um bem maior, neste caso, a segurança e/ou saúde públicas. O presente estudo, a partir desse cenário, aponta quais as vertentes de utilização estatal dos drones durante a emergência social a fim de verificar se as ferramentas tecnológicas agregadas a esse veículo, em especial o reconhecimento facial, violam a privacidade, a imagem e dados pessoais. Para tanto, iniciamos a análise do tema apontando o crescimento exponencial destes equipamentos no Brasil e no mundo para tratarmos, posteriormente, dos meios de controle e da regulamentação existentes e se estes são suficientes e efetivos à proteção das garantias fundamentais dos cidadãos. Após, analisamos as tecnologias agregadas aos drones, mormente as de reconhecimento facial, para apontar os parâmetros de tratamento e proteção de dados pessoais, ainda que em época de emergência social. Para tanto, realizamos uma pesquisa bibliográfica, seguida de uma análise crítico-valorativa da temática.

VISÃO DE CIMA: a ascenção dos drones em perspectivas nacionais e internacionais

Assim como ocorreu com a *internet*, inicialmente projetada para fins militares[5] - mas posteriormente consagrada como um direito fundamental pela ONU[6] -, os drones têm sua origem pautada em tempos de guerra, tendo como principal fundamento inventivo o melhoramento de torpedos aéreos para o transporte de ogivas até o inimigo sem apresentar risco ao piloto (SILVA, 2018, p. 36). A origem bélica, no entanto, não mitiga o potencial disruptivo e inovador do equipamento como uma ferramenta extremamente flexível, podendo ser atribuída finalidade recreativa ou profissional, atuação pública ou privada[7]. Tais atributos, dentre outros, são responsáveis pela ascensão da produção e comércio destes equipamentos e sua consolidação no mercado mundial (principalmente do entretenimento e da segurança pública), que tem como líderes a China e os Estados Unidos.

[5] Castells nos revela em sua obra que "a Internet nasceu da improvável interseção da *big science*, da pesquisa militar e da cultura libertária. Importantes centros de pesquisa universitários e centros de estudos ligados à defesa foram pontos de encontro essenciais", a se denotar que o intento da ARPANET, origem remota do que conhecemos por *internet,* se deu no âmbito militar que, no entanto, restou secularizado pelas proporções mundiais que a descoberta da conectividade propiciou. (CASTELLS, 2003. p. 23).

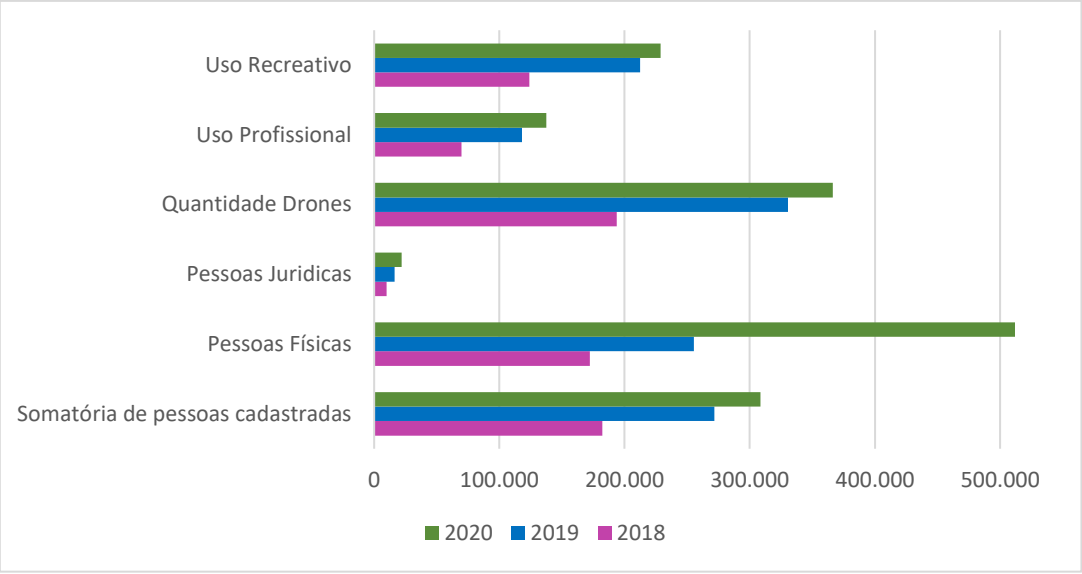
[6] A Organização das Nações Unidas (ONU) equiparou a conectividade pela *internet* como um direito fundamental ao afirmar que é a chave para a garantia do direito de liberdade de expressão, garantido no art. 19 da Declaração Universal dos Direitos Humanos. (UNITED NATIONS, 2011).

[7] No âmbito privado, as destinações comerciais mais comuns de uso dos drones são na agricultura, constituição civil, pecuária e produção de eventos.

A Administração Federal da Aviação norte-americana, setor responsável pelo controle da frota de drones no país, estima que haja 1.705.776 (um milhão setecentos e cinco mil setecentos e setenta e seis) equipamentos registrados em 2020 sendo, deste total, 28% destinados a uso comercial e 72% para recreação, conduzidos por mais de 190.000 (cento e noventa mil) pilotos certificados (ESTADOS UNIDOS, 2020). O mesmo órgão prevê que até 2040 o cenário se mantenha na média de 1.500.000 (um milhão e quinhentos mil) unidades comercializadas por ano, havendo decrescimento apenas pela saturação, mas que pode ser superado por melhoramentos na tecnologia, como a autonomia da bateria e altura de voo (ESTADOS UNIDOS, 2019). Na América Latina, exemplos, como o Chile, demonstram uma tendência crescente na indústria de vigilância estatal pelos drones. De acordo com Castellaro, nos últimos 4 (quatro) anos o país investiu cerca $USD 350.000,00 (trezentos e cinquenta mil de dólares) apenas nestes equipamentos (CASTELLARO, 2017, p. 185). O ponto favorável é apontado por Baslestreri e Falck ao afirmarem que a *Dirección General de Aeronáutica Civil de Chile (DGAC)* somente emite autorizações para pilotos de drones que possuam apólices de seguros com cobertura para ele, a aeronave e terceiros, bem como destacam que existem normativas específicas que proíbem a violação aos direitos de privacidade e intimidade das pessoas (BASLESTRERI, 2015).

No Brasil, o mercado é promissor, mas preocupante. Os primeiros investimentos ocorreram para o melhoramento da segurança pública em 2014 e 2016 devido a realização da Copa do Mundo e das Olimpíadas, o que resultou na compra de drones militares, pelo governo federal, equipados com um sensor de vigilância capaz de varrer uma área de 100 km (CASTELLARO, 2017, p. 187). De acordo com a Agência Nacional de Aviação Civil (ANAC), que é um dos órgãos responsáveis pelo controle e regulamentação do equipamento no Brasil, apenas no ano de 2020 (de janeiro a maio) foram registrados 366.615 (trezentas e sessenta e seis mil seiscentos e quinze) drones. Deste total, 62% representam o uso para recreação e o restante (38%) para uso profissional. Em comparação com o mesmo período de 2019, verificamos um aumento aproximado de 11% na quantidade total de equipamentos no país. Embora a comparação entre os dois últimos anos já demonstre importante crescimento, maior atenção deve ser despendida na análise comparativa entre os anos de 2018 e 2020, já que verificamos o aumento de 89% na quantidade de registros entre os meses de janeiro a maio.

Gráfico 1 – Registo de drones no Brasil entre 2018 e 2020.



Fonte: ANAC, 2018, 2019, 2020.

A análise dos dados da ANAC (BRASIL, 2020) corrobora o entendimento de que, muito embora tenha havido um aumento substancial no período analisado, e que por pouco não dobrou o número de drones registrados no espaço de um ano (2018 – 2019), o crescimento se mantém pela constância da demanda, ocasionada por fatores como a) a velocidade com que são aperfeiçoados, mediante o aumento de suas utilidades; b) a variedade de preços e a facilidade de comercialização[8]; c) a contribuição na segurança pública; d) a popularidade no uso recreativo e d) a ausência de normativa federal para regulamentar a atividade e comércio. Quanto à última hipótese, destacamos que não obstante a falta de regramento unificado que discipline a comercialização e o uso dos drones no país a competência de controle, registro e monitoramento é atribuída de modo concorrente a) à Agência Nacional de Telecomunicações (ANATEL), no que concerne a utilização de equipamentos de rádio transmissão acoplados; b) ao Departamento de Controle do Espaço Aéreo (DECEA), que impõe limites à altura de voo e proximidade de obstáculos e c) à própria ANAC, que regulamenta a autorização de pilotagem e classificação das aeronaves de acordo com suas características motoras, estruturais e tecnológicas.

[8] A precificação do equipamento depende das caraterísticas estruturais e dos componentes da montagem, tais como: quantidade de hélices, autonomia da bateria, resolução da imagem da câmera, peso, tamanho *et cetera*. Estas variáveis fazem com que os drones abranjam diversas faixas de valores, sendo encontrados em versões mais simples pelo valor de R$ 300,00 (trezentos reais), podendo atingir, em versões profissionais, o montante de R$ 120.000,00 (cento e vinte mil reais). (EUGENIO; ZAGO, 2019).

Ocorre que, no que tange a competência normativa[9] das sobreditas agências (que reverbera na existência de incontáveis regramentos), é importante destacar que disciplinar o âmbito de voo, impor limite ao trajeto, regulamentar o peso e a estrutura, por si só, não se mostram suficientes aos olhos do direito, mormente porque a problemática não reside apenas no fato de que um drone está sobrevoando um local, mas sim na razão pela qual o faz. Para além do levantar voo e conduzir um determinado caminho, faz-se imperioso ampliar o conceito primário de veículo aéreo não tripulado para entender que tais equipamentos há muito não são apenas aeronaves remotamente pilotadas, ao passo que envolvem outras ações em várias áreas da tecnologia como eletromagnetismo, computação, automação, cibernética e inteligência artificial (SPADOTTO, 2016). A ausência de disciplina específica para as ferramentas de captação de dados que são acopladas aos drones (como as de gravação de imagem, som e mapeamento geográfico), possivelmente, torna o campo fértil para a extração ilimitada de informações não autorizadas e invasão de privacidade tanto no âmbito privado, quanto pelo próprio poder público. Com efeito, à medida que número de aeronaves aumenta, mostra-se igualmente proporcional o potencial lesivo da situação, seja porque as tecnologias estão cada dia mais avançadas, seja em razão da ausência de regras a respeito da captação, tratamento e destinação dos dados pelos controladores. Esta falha é ainda mais evidente (e proporcionalmente preocupante) durante o lapso pandêmico que estamos enfrentando.

VISÃO DE PERTO: drones, reconhecimento facial e proteção de dados

O rosto humano tem inúmeros marcos divisórios distintos, chamados de *pontos nodais*, que são os picos e vales presentes da face, tais como a distância entre os olhos, largura do nariz, profundidade das órbitas oculares, comprimento da linha da mandíbula *et cetera*. Juntas, essas características compõe a identidade facial e visual do indivíduo, convertida na geometria do rosto. O reconhecimento facial, realizado por um algoritmo, define estes pontos, isolando-os e os medindo para então identificar que a imagem é a de um indivíduo (LEVASHOV, 2013, p. 164). O processo se inicia mediante a exibição de uma foto ou vídeo de um rosto que, em seguida, é submetido à análise do *software* que deve ser

[9] Importante esclarecer que a competência normativa das Agências Reguladoras em âmbito nacional, embora seja resultado da influência do direito administrativo norte-americano, é resultado direito da própria tripartição e consequente autonomia da administração pública que pode descentralizar suas competências, atribuindo-as às Agências. No entanto, a capacidade normativa é limitada ao disposto na legislação e na principiologia constitucional. (LEHFELD, 2006).

capaz de identificar a geometria da face, elaborando uma espécie de assinatura facial (COSTA; OLIVEIRA, 2019). Após, realiza-se a comparação desta assinatura – convertida em uma fórmula matemática – com os dados de um banco imagens pré-coletadas. Espera-se, a partir daí, que seja possível a identificação facial, baseada na busca e comparação dos padrões estabelecidos (WELINDER, 2012).

Os *softwares* que se utilizam desta tecnologia baseiam a construção algorítmica na técnica de aprendizado da máquina (*machine learning*[10]). Ou seja, a máquina é treinada para que, partindo de uma premissa lógica (exemplo: pontos nodais compõe um rosto humano), torne-se capaz de, por si só, encontrar as características individuais, identificando-as, reunindo-as e, com elas, desenvolvendo padrões de reconhecimento cada vez mais aprimorados.

Portanto, os drones com *software* de reconhecimento facial acoplados às suas câmeras inicialmente capturam as imagens e procedem a uma análise a partir das características do rosto, transmitindo, em tempo real, o banco de dados ao controlador. Por tais propriedades, a tecnologia de reconhecimento facial, aliada à mobilidade que é característica dos drones, tem atraído o interesse governamental, principalmente no âmbito da segurança pública[11]. No Brasil, os primeiros investimentos destinavam-se a possibilitar a identificação de possíveis infratores e foragidos em multidões. Em 2019, o Governo do Estado de São Paulo anunciou a compra de 208 drones para sua utilização em eventos, protestos, reintegrações de posse e outras. À época, já se estimava que a polícia desse estado possuía ao menos 40 drones a sua disposição (PAULO, 2019). Para o carnaval do ano seguinte, o aparato foi reforçado com o aumento do número de aeronaves e com o

[10] De acordo com Giuffrida, Lederer e Vermeys o aprendizado de máquina – *machine learning* pode ser definido como: "A capacidade de um computador de modificar sua programação para dar conta de novos dados e modificar suas operações de acordo com eles. Ele usa computadores para executar modelos preditivos que aprendem com os dados existentes para prever futuros comportamentos, resultados e tendências. O aprendizado de máquina, portanto, depende de dados. Quanto mais dados puder acessar, melhor poderá 'aprender'" (tradução nossa). (GIUFFRIDA; LEDERER; VERMEYS, 2018).

[11] Na China, drones estão sendo utilizados como forma de colheita de dados sobre o cumprimento das imposições de distanciamento social. Através dessa tecnologia, com sistemas de reconhecimento facial, é possível identificar cada indivíduo, verificar se ele faz uso dos aparatos obrigatórios de proteção como máscaras, fazer aferição de temperatura corporal, orientá-lo sobre a doença e até *mandá-lo* para casa, tudo de forma automatizada. (TRINDADE, 2020).

investimento na tecnologia de reconhecimento facial[12], o que, na mesma época e para a mesma finalidade, foi também anunciado pelo Estado do Rio de Janeiro[13].

Diante da realidade instaurada, emergem questionamentos acerca da legalidade da coleta indiscriminada e não consentida destes dados e, ainda, a própria forma de destinação e armazenamento. Os sítios eletrônicos estatais disponibilizam ao público apenas notícias de cunho jornalístico acerca da inauguração da tecnologia, não havendo qualquer apontamento técnico ou mesmo a explicação acurada de como a extração e tratamento dos dados pessoais ocorre. Com efeito, para além da mera divulgação de que referida tecnologia foi implementada, é fundamental não apenas que se atribua transparência ao algoritmo, mas também que seja veiculado ao público a devida informação acerca de como estes aparatos funcionam, do que são capazes, e qual o protocolo estatal para sua utilização. Afinal, não há dúvidas de que a mera divulgação do código algorítmico é insuficiente para permitir a compreensão sobre os benefícios e malefícios da adoção de uma tecnologia desse tipo, sendo certo que a opacidade difundida neste contexto se relaciona à falta de conhecimento sobre a ciência da computação pela população, aliada a falta de transparência estatal (HARTMANN; SILVA, 2019). Hoffmann-Riem compartilha desta mesma preocupação ao assinalar que:

> É importante, não só para os usuários, mas também para os órgãos de fiscalização, bem como para o público em geral como corresponsável pela democracia, que a forma de lidar com tecnologias digitais, incluindo a utilização de IA, seja fundamentalmente compreensível, em todo caso passível de fundamentação e tão controlável quanto possível. Nesse sentido, uma transparência suficiente é um pressuposto não só para a criação de confiança, mas também de prestação de contas e, eventualmente, para a responsabilidade civil (HOFFMANN-RIEM, 2019).

Não bastasse a ineficiência informativa já identificada, as sucessivas discussões sobre a vigência da Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), aliado a ineficaz regulamentação da Autoridade Nacional de Proteção de Dados e a repentina entrada em vigor, torna indissociável crer que interessa ao poder público perpetuar determinadas situações, cabendo neste mister apontar a utilização dos drones com capacidade de

[12] "O sistema de reconhecimento facial dinâmico é algo novo no Estado de São Paulo, contudo seu uso a partir de imagens estáticas é realizado desde janeiro de 2020. Ambas as ferramentas estarão em funcionamento durante todo o período de Carnaval." (BRASIL, 2020).

[13] "Por meio de um software desenvolvido pela empresa de telefonia Oi, as câmeras são ligadas ao Centro Integrado de Comando e Controle (CICC), onde as imagens serão checadas junto aos bancos de dados da Polícia Civil (para reconhecimento facial) e do Detran (para verificação das placas dos veículos). Com a identificação positiva, equipes de patrulhamento urbano serão acionadas em tempo real." (AGÊNCIA BRASIL, 2019).

reconhecimento facial e a vigilância e colheita de dados sem consciência do titular. Outrossim, inolvidável que a instauração de uma situação pandêmica, causada pela disseminação mundial da COVID-19, exigiu o estabelecimento de uma série de medidas excepcionais e urgentes para contenção da doença que ultrapassou recentemente a marca de 1.600.000 (um milhão e seiscentos mil) brasileiros infectados e vitimou mais de 60.000 (sessenta mil) desde o registro do primeiro caso no país, em março de 2020 (BRASIL, 2020). A tomada de decisão sobre as medidas restritivas, políticas públicas e demais ações que visam controlar/diminuir o impacto econômico e social da crise, em regra, têm sido balizadas pelo tratamento de dados colhidos por tecnologias.

A mensuração do índice de isolamento social no Estado de São Paulo, por exemplo, é calculada pelo georreferenciamento[14] de *smartphones*[15]. Os drones monitoram as regiões centrais com maior possibilidade de concentração de pessoas, dispersam aglomerações com seus alto-falantes e até fazem limpeza dos espaços públicos. Tudo isso, todavia, sem qualquer controle sobre os dados pessoais obtidos durantes as diligências. Assim, para além da utilização desta tecnologia na segurança pública, cuja legalidade já era questionável, a ampliação da atuação reafirma o argumento de que a vigência da LGPD restou postergada para impedir que a) haja limitação ao uso destes aparatos, b) seja questionada a legalidade da coleta dos dados, c) seja exigida regulamentação específica para a temática e d) seja cumprido em sua integralidade o dever informativo acerca do modo, da extensão e dos riscos de utilização desta tecnologia. Importa esclarecer que não se questiona o uso da tecnologia a serviço do Poder Público. Pelo contrário, é inconteste que o tratamento das informações

[14] "A produção da geoinformação envolve o tratamento dos dados e das fontes de dados por meio do geoprocessamento. A informação é oriunda de cartas, levantamentos de campo em solo com Sistema de Posicionamento Global (em inglês, GPS – Global Positioning System)2, aerolevantamentos, drones, imagens ópticas ou radar. A produção pode ser a partir de dados históricos ou em tempo real. Atualmente, o Governo Federal não dispõe de uma base de dados geoespacial centralizada, organizada, abrangente, contínua, atualizada e de simples acesso. Os resultados desse contexto, citando exemplos de 2019, foram as dificuldades de avaliação e gerenciamento de riscos e as crises do rompimento da barragem de Brumadinho/MG, que resultou em um dos maiores desastres com rejeitos de mineração no Brasil, das queimadas e desmatamento na Amazônia e do óleo que atingiu o litoral do País" (PIMENTEL, 2020).

[15] Segundo informações do Instituto de Pesquisas Tecnológicas, o sistema Sistema de Informações e Monitoramento Inteligente do Governo do Estado de São Paulo (SIMI-SP) que mede o índice de isolamento social tem seus dados "disponibilizados pelas prestadoras de serviços de telecomunicação (Vivo, Claro, Tim, Oi) por meio de uma plataforma *Big Data* que é gerida pela Associação Brasileira de Recursos em Telecomunicações (ABR Telecom). Segundo as prestadoras de serviços de telecomunicação, o índice de isolamento é baseado na localização obtida pelas antenas de celulares (Estações Rádio Base – ERBs), as quais "marcam" uma referência para o lugar onde o celular "dormiu" entre as 22h00 e 2h00. Durante o dia, um celular que tenha se afastado desta referência (que é variável, mas, para dar uma ideia, chega a aproximadamente 200 metros na cidade de São Paulo), é considerado fora do isolamento. Todo este processamento é feito pela operadora". (BRASIL, 2020).

colhidas pode ser útil na execução de políticas governamentais de combate à COVID-19 já que podem monitorar o isolamento social, auxiliar na conscientização da população acerca dos riscos causados pelas aglomerações, mensurar a aderência ao uso de máscaras ou mesmo indicar as pessoas com quem o infectado teve contato (JUNIOR; MODESTO, 2020). O que nos preocupa, no entanto, é a ausência de ciência da população acerca da coleta e tratamento dos dados durante esse lapso temporal pandêmico justificado genericamente pela instauração da crise sanitária causada pela COVID-19.

Assim, da mesma maneira com que inúmeros diplomas normativos (Constituição Federal, Código de Defesa do Consumidor, Lei de Acesso à Informação e a própria Lei Geral de Proteção de Dados quando trata do livre consentimento informado) garantem ao cidadão o direito informativo e ao Estado o dever correspondente, não há qualquer excesso de cautela, quiçá exigência exacerbada na investigação proposta, até mesmo porque os algoritmos estão sujeitos a erros, passíveis da condução de sucessivas violações, como bem aludem Molinaro e Sarlet:

> Os sistemas de autoaprendizagem podem usar dados de um grupo consideravelmente grande de pessoas para identificar fatores relevantes, como comportamentos relacionados à saúde, e localizar indivíduos e conteúdos neste sistema de coordenadas. Tais abordagens permitem recomendações e interações rápidas e individualizadas com "assistentes de máquina". Todavia, eles são necessariamente acompanhados pela divulgação de informações pessoais e, se necessário, induzem ao engano e à manipulação de decisões pessoais na medida em que podem adicionar vieses cognitivos nos
> processos deliberativos (MOLINARO; SARLET, 2020).

Uma saída viável para o impasse é vista pela garantia de que os dados, embora colhidos, passaram por um processo de anonimização ou pseudoanonimização, que consiste na "aplicação de medidas técnicas para impossibilitar a associação direta ou indireta dos dados ao indivíduo" (ALMEIDA et al., 2020) ou na remoção dos identificadores e a substituição por um código chave único (criptografia). A garantia de anonimização ou pseudoanonimização dos dados, no entanto, não exime o Poder Público de efetivar a obrigação informativa, mas, pelo menos, mitiga a ilegalidade da coleta massificada de informações dos cidadãos. Isto porque, em geral, os dados submetidos a estes processos não são tidos como dados pessoais ao passo que não permitem a identificação de seu titular (ALMEIDA et al., 2020). É esta, inclusive, a conclusão do Parecer nº 1192/2020/SEI-MCTIC emitido pela Comissão da Covid-19 do Ministério da Ciência, Tecnologia, Inovações e

Comunicações[16], e pela Advocacia Geral da União no Parecer nº. 00280/2020/CONJUR-MCTIC/CGU/AGU[17].

VISÃO DE LONGE: vigilância líquida, mitigação da privacidade e o futuro dos drones no brasil.

Em 1934, George Orwell, pseudônimo utilizado pelo escritor Eric Arthur Blair, escreveu a obra "1984 – A Era do Grande Irmão", narrativa sobre uma sociedade futurista controlada por um Estado totalitário que tinha como líder a figura mitológica do *Grande Irmão*. Na ficção, a polícia se utilizava de um equipamento tecnológico onipresente denominado *teletela*, que captava, recebia e enviava imagens e sons a uma central que vigiava permanentemente os cidadãos (ORWELL, 2003, p. 80). Embora a distopia *orwelliana* retrate um romance sem maiores pretensões de vidência sobre o futuro, externa ares de preocupação e avisos às próximas gerações, relativamente a utilização descontrolada da tecnologia enquanto meio de vigilância e controle social a serviço do Estado. Trazendo a mesma temática, Michel Foucault destacou o modelo *pan-óptico*. Nele, o autor analisa a invenção de Bentham, que parte da ideia de controle e amedrontamento coletivo a partir da existência de um *olho que tudo vê,* situado em uma espécie de mirante, no centro de uma de um complexo prisional. A demonstração de eficácia do modelo emerge de uma ideia de vigilância constante, baseada na pressão psicológica que alcança uma perspectiva de exercício de poder e institui um estado de tensão que, por sua vez, mobiliza o comportamento dos vigiados (FOCAULT, 2009, p. 113).

Partindo destas premissas acerca da vigilância e inserido no contexto da liquidez dos fenômenos sociais, Bauman entende que ela sofreu igual modificação, diluindo-se e incorporando-se ao nosso dia a dia. Calcado sobre a premissa da segurança pública ou

[16] "No contexto brasileiro, cabe ressaltar inicialmente que, sob a ótica da LGPD, fortemente inspirada pelo marco jurídico europeu, dados anônimos não são considerados dados pessoais e não são abarcados pela lei. Assim, em análise preliminar, considerando-se o disposto na LGPD (que, reitere-se, somente entrará em vigor em agosto), não parecem existir óbices jurídicos ao compartilhamento de dados agregados e anônimos referentes à movimentação de indivíduos para fins específicos de combate ao COVID19, tomando-se os devidos cuidados quanto à minimização dos dados com vistas a evitar a reidentificação dos indivíduos envolvidos". (BRASIL, 2020, p. 3).

[17] "Considerando o princípio da supremacia do interesse público sobre o particular, considerando que o caso em tela visa atender a interesse público imediato de combater a pandemia COVID19, verifica-se que o espírito da LGPD, alça questões de saúde pública, como a realização de estudos em saúde pública, como limite à proteção do dado pessoal, sendo tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, mantendo sempre que possível a anonimização ou pseudonimização dos dados". (ADVOCACIA GERAL DA UNIÃO, 2020).

privada, a tecnologia vem sendo utilizada como mecanismo de fiscalização, marketing e controle (BAUMAN, 2014, p. 50).

Ao contrário do slogan do partido do conto de George Orwell que brada "O Grande Irmão está de olho em você" e por isso ninguém está só (ORWELL, 2003, p. 81), é característica da vigilância líquida pós-moderna a invisibilidade e autonomia, pois os cidadãos, "servos voluntários" das tecnologias de vigilância, embora não as vejam, são por elas sempre *vistos* (BAUMAN, 2014, p. 52), reforçando a premissa de que, quanto mais rígida e perceptível são as estruturas de controle, maior a resistências daqueles a elas submetidas. Ao contrário, quanto mais dissimulada e sutil for a vigilância (líquida), maior a chance de que os indivíduos a ela consintam, ainda que inconscientemente. Nesta esteira de ideias, destacam-se os drones. A evolução das tecnologias da informação, por si só, já facilitou a implementação de um estágio acurado de vigilância sem que fosse necessária qualquer coerção estatal para tanto, já que os dados pessoais (quando não são colhidos sem o prévio aviso) têm sido voluntariamente fornecidos pela população.

Vale registrar que mesmo os dados aparentemente inofensivos e insignificantes podem ser valiosos e igualmente perigosos quando cruzados com outras fontes, inclusive porque – insistimos – a finalidade da coleta e a destinação dos dados não são informadas pelo Poder Público o que, inclusive, revela intentos pouco democráticos já que "viver em um grupo social democraticamente organizado tomou outro sentido, e isto inclui, em primeira linha, ter a nítida noção do que efetivamente significa hoje *divulgar* informações" (RUARO; RODRIGUEZ; FINGER, 2011), sendo esta, portanto, uma tarefa crucial incumbida aos Estados. Ademais, a realidade tecnológica instaurada modificou a conotação de privacidade que, de acordo com Doneda, passou a se caracterizar pela proteção de dados passando de um interesse puramente individual para se interligar à personalidade, às liberdades fundamentais e a dignidade da pessoa humana (DONEDA, 2006, p. 91).

Com efeito, a instituição da situação de emergência pública causada pela pandemia da COVID-19 elevou sobremaneira o patamar de coleta despercebida e exacerbada de dados pessoais sob a justificativa utilitarista de que há supremacia da saúde pública em relação à proteção à imagem e à privacidade, por exemplo. Não há direito fundamental ilimitado ou mesmo princípios absolutos, de modo que, na colisão entre a privacidade, proteção da imagem e a saúde pública, indispensável a realização do sopesamento das normas constitucionais que os tutelam, consoante proposto por Alexy (ALEXY, 2011, p. 111) e que,

embora represente a instituição de restrições à esfera subjetiva e objetiva, tem sido amplamente aceita no neoconstitucionalismo (SARLET, 2015, p. 405-406).

Ocorre que, em que pese a possibilidade de mitigação de um direito constitucionalmente protegido, não há de se falar em completa exclusão de outro. A diretriz é que o intérprete garanta a coexistência dos direitos. Ou seja, saúde, segurança e privacidade devem concorrer para um bem comum em que um deles, no entanto, se sobressaia aos demais sem violá-los (JUNIOR; MODESTO, 2020) sendo esta, talvez, a *resposta mais correta* (DWORKIN, 2007). Neste sentido, indispensável atribuir limites aquele que pode parecer o *novo normal* e que tem servido de escusa para o aumento da exposição da privacidade e intimidade do cidadão em um espaço com pouca ou nenhuma regra, sem perspectiva de como esses mesmos dados poderão vir a ser utilizados em detrimento do indivíduo futuramente.

É pouco ou nada crível que, superada a situação extrema, os dados pessoais colhidos neste lapso sejam voluntaria e informadamente descartados pelo Poder Público em um ambiente seguro. Assim como é ingênuo acreditar que o investimento nas tecnologias vigilantes (como os drones dotados de reconhecimento facial) sejam direcionados à outra finalidade que não seja precipuamente colher dados da população e instituir uma espécie de Grande Irmão pós-*pan-óptico*. O futuro, portanto, do uso de drones no país, após a sua presente utilização estatal em circunstâncias de ausência de clara regulamentação e justificativa de uma situação emergencial em prol da segurança e saúde públicas, ainda é incerto frente aos ditames constitucionais, em especial na proteção da intimidade, privacidade e imagem do cidadão. Por isso, recomenda-se cautela e amplo controle institucional e social do aparato tecnológico estatal no combate à pandemia, pois esta não tem o condão de prospectar um perfil de Estado-polícia, que não reflete a verdadeira finalidade estatal, qual seja, o bem comum da sociedade.

CONCLUSÃO

A ascensão exponencial da utilização de drones no Brasil e no mundo reforça o nicho mercadológico da captação de imagens, sons e dados por aeronaves não tripuladas como uma tecnologia disruptiva e multifacetária, capaz de implementar novas formas de realização do dever de garantia da segurança nacional. No entanto, infere-se de uma análise geral da atuação das agências reguladoras que as normativas existentes limitam-se à regulamentação da utilização do equipamento (como o planejamento de voo, regras de

distância de obstáculos, peso do equipamento, *et cetera*) não havendo, neste mister, limitadores acerca das tecnologias acopladas à aeronave, mormente às de reconhecimento facial.

A lacuna normativa representa uma preocupação, ao passo que pode reverberar na instauração de um estado de vigilância estatal ilimitado, combinado pelas nuances de Orwell, ao descrever as *teletelas* e de Bauman, quando aponta a invisibilidade do controle em tempos de liquidez. Somado à este contexto, há o enfrentamento dos países à situação pandêmica causada pela disseminação da COVID-19, o que, por si só, já traz tensões. Se de um lado o Poder Público deve buscar no uso de drones um meio eficaz para o combate à proliferação do vírus, não se pode permitir que, por uma visão utilitarista da crise, direitos fundamentais sejam mitigados sem qualquer sopesamento, sob a justificativa de que a problemática instaurada garante violações às garantias fundamentais de privacidade em prol, apenas, da saúde e segurança públicas. Neste mister, a Lei Geral de Proteção de Dados representa um marco normativo nacional sobre a temática capaz de, ao menos, nortear a atuação do Poder Público, já que a imperatividade do texto e a aplicabilidade das multas que nele estão contidas estão condicionadas à sua vigência, postergada sucessivamente e agora prevista para o ano de 2021. Por enquanto, aspiramos por uma atuação ética da administração pública, dos operadores das tecnologias e dos cientistas da computação no que concerne a colheita, tratamento e descarte dos dados, a fim de garantir a construção de algoritmos que não violem direitos fundamentais e que realizem, ao menos, a pseudoanonimização em respeito à proteção de imagem e ao direito de privacidade do detentor dos dados.

Portanto, concluímos pela indispensabilidade de regulamentação das tecnologias, a fim de limitar e sua utilização pelo Poder Público e, portanto, impedir um estado de vigilância ininterrupta autorizado pela emergência social causada pela pandemia mas que, sem dúvida, deixará rastros após o período de crise. Outro fator indispensável é a vigência da LGPD e sua efetivação na ordem jurídica nacional. A administração pública deve respeitar seus ditames, atribuindo transparência às tecnologias de colheita de dados, o que deve ser acompanhado pela aplicação pelos Tribunais do regramento, a fim de não apenas balizar o uso das tecnologias neste lapso de emergência social, mas ainda possibilitar a ostensiva conscientização popular acerca dos riscos para a privacidade e proteção de informações pessoais, alcançando, assim, um alinhamento entre os direitos fundamentais à saúde,

segurança e privacidade, sem que nenhum se torne coadjuvante durante a pandemia e, após, no que podemos chamar de *novo normal*.

REFERÊNCIAS

ADVOCACIA GERAL DA UNIÃO. Parecer n. 00280/2020/CONJUR-MCTIC/CGU/AGU. Ações do Poder Público que envolvem coleta de dados de usuários/COVID 19. Disponível em: https://sapiens.agu.gov.br/documento/402680296. Acesso em: 05 jul. 2020

AGÊNCIA BRASIL. Câmeras de reconhecimento facial começam a funcionar em Copacabana. Portal Globo. 27 fev. 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/cameras-de-reconhecimento-facial-comecam-funcionar-em-copacabana.html. Acesso em: 08 jul. 2020.

ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução: Virgílio Afonso da Silva. 5 ed. São Paulo: Malheiros, 2011.

ALMEIDA, Bethania de Araujo et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. Ciência e Saúde Coletiva. v.25, supl.1, p.2487-2492, 2020. Disponível em: https://www.arca.fiocruz.br/handle/icict/41770. Acesso em: 02 jul. 2020.

BALTAZAR, Helena Maria Nunes Marques. Veículos Aéreos Não Tripulados e Legalidade. 2015. 114 f. Dissertação (Mestrado em Ciência Política e Relações Internacionais – Área de Especialização em Globalização e Ambiente) – Universidade Nova de Lisboa. Disponível em: https://run.unl.pt/bitstream/10362/18928/1/VeiculosAereosNaoTripuladosLegalidade.pdf. Acesso em: 08 jul. 2020.

BASLESTRERI, Miguel Gomis; FALCK, Fernando. De ficción a realidad: drones y seguridad ciudadana en América Latina. Revista Científica de la Escuela de Postgrados de la Fuerza Aérea Colombiana. vol. 10. Enero - Diciembre de 2015. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=5682849. Acesso em: 05 jul. 2020

BAUMAN, Zygmunt. Vigilância Líquida: diálogos com David Lyon. Rio de Janeiro: Zahar, 2014.

BRASIL. Agência Nacional de Aviação Civil. Quantidade de Cadastros. 2020. Disponível em: https://www.anac.gov.br/assuntos/paginas-tematicas/drones/quantidade-de-cadastros. Acesso em: 08 jul. 2020.

_____. Governo do Estado de São Paulo. Instituto de pesquisas Tecnológica. IPT responde perguntas frequentes (FAQs) sobre índices de isolamento social divulgados pelo Governo de SP. Disponível em: https://www.ipt.br/noticia/1623-_perguntas_sobre_isolamento_social.htm. Acesso em: 08 jul. 2020

_____. Governo do Estado de São Paulo. Polícia Civil tem central de monitoramento para o carnaval 2020. Disponível em: https://www.saopaulo.sp.gov.br/spnoticias/policia-civil-tem-central-de-monitoramento-para-carnaval-2020/. Acesso em: 08 jul. 2020.

_____. Lei 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em 08 fev. 2020.

_____. Ministério da Ciência, Tecnologia, Inovações e Comunicações. Nota informativa nº 1192/2020/SEI-MCTIC. Comitê de Crise Covid-19. Rede Conectada MCTIC. Ações do Poder Público que envolvem coleta de dados de usuários. Secretaria de Telecomunicações Departamento de Serviços de Telecomunicações. 2020.

_____. Ministério da Saúde. Painel coronavírus. Disponível em: https://covid.saude.gov.br/. Acesso em: 08 jul. 2020.

CASTELLARO, Sebastián Becker. Drones en latinoamerica: industria, discursos y violaciones a los derechos humanos. In: 5º Simposio Internacional LAVITS - Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias. Santiago, Chile, 2017. p. 182-203. Disponível em: <https://www.academia.edu/40501101/DRONES_EN_LATINOAMERICA_INDUSTRIA_DISCURSOS_Y_VIOLACIONES_A_LOS_DERECHOS_HUMANOS>. Acesso em: 09 fev. 2020.

CASTELLS, Manuel. A galáxia da internet: reflexões sobre a internet, negócios e sociedade. Rio de Janeiro, Zahar, 2003.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. O uso de tecnologias de reconhecimento facial em sistemas de vigilância e suas implicações no direito à privacidade. Revista de Direito, Governança e Novas Tecnologias. Belém, v. 5, n. 2, p. 01 – 21, Jul/Dez. 2019. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/5777. Acesso em: 05 jul. 2020.

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

DWORKIN, Ronald. O Império do Direito. Tradução Jefferson Luiz Camargo; revisão técnica Gildo Sá Leitão Rios. 2ª edição, São Paulo: Martins Fontes, 2007.

ESTADOS UNIDOS. Federal Aviation Administration. FAA Aerospace Forescast: fiscal years 2020 - 2040. 2019. Disponível em: https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2020-40_FAA_Aerospace_Forecast.pdf. Acesso em: 08 jul. 2020.

_____. Federal Aviation Administration. UAS By the numbers. 2020. Disponível em: https://www.faa.gov/uas/resources/by_the_numbers/. Acesso em: 08 jul. 2020.

EUGENIO, Fernando Coelho; **ZAGO**, Hugo Bolsoni. O livro dos drones: um guia completo para entender todas as partes e funcionamento. Alegre: CAUFES, 2019

GIUFFRIDA, Iria; **LEDERER**, Fredric; **VERMEYS**, Nicolas. A legal perspective on the trials and tribulations of ai: how artificial intelligence, the internet of things, smart contracts,

and other technologies will affect the law. Case Western Reserve Law Review. v. 68, n. 3, p. 747–782, 2018

HARTMANN, Ivar A.; **SILVA**, Lorena Abbas da. Inteligencia artificial e moderação conteúdo: o sistema content id e a proteção de direitos autorais na plataforma Youtube. Revista Ius Gentium. Curitiba, v. 10, n. 3, p. 145-165, set./dez. 2019. Disponível em: https://www.uninter.com/iusgentium/index.php/iusgentium/article/view/503. Acesso em: 06 jul. 2020.

HOFFMANN-RIEM, Wolfgang. Inteligência Artificial como oportunidade para a regulação jurídica. Direito Público. [S.l.], v. 16, n. 90, dez. 2019. ISSN 2236-1766. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3756. Acesso em: 02 jul. 2020

JUNIOR, Marcos Ehrhardt; **MODESTO**, Jéssica Andrade. Danos colaterais em tempos de pandemia: preocupações quanto ao uso dos dados pessoais no combate a COVID-19. Redes: Revista Eletrônica Direito e Sociedade. Canoas, v. 8, n. 2, 2020. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/view/6770. Acesso em: 04 jul. 2020.

LEHFELD, Lucas de Souza. Controles das Agências Reguladoras: a participação cidadã como limite à sua autonomia. 2006. 416 f. Tese (Doutorado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2006. Disponível em: https://tede2.pucsp.br/bitstream/handle/7142/1/Tese%20Lucas%20de%20Souza%20Lehfeld%20.pdf. Acesso em: 09 jul. 2020.

LEVASHOV, Kirill. The Rise of a New Type of Surveillance for Which the Law Wasn't Ready (2013). Columbia Science and Technology Law Review. v. 15, p. 167-168, Fall 2013. p. 164.

MOLINARO, Carlos Alberto; **SARLET**, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de big data. Revista Brasileira de Direitos Fundamentais & Justiça. v. 13, n. 41, p. 183-212, 2020. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/811/964. Acesso em: 03 jul. 2020.

PAULO, Paula Paiva. Governo de SP irá comprar 208 drones para usar em protestos, reintegrações de posse e salvamentos aquáticos. Portal G1. São Paulo, 12/04/2019. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2019/04/12/governo-de-sp-ira-comprar-208-drones-para-atuar-em-protestos-reintegracoes-de-posse-e-salvamentos-aquaticos.ghtml. Acesso em: 06 jul. 2020.

PIMENTEL, Paula. A governança da geoinformação no âmbito do governo federal do Brasil. Revista brasileira de planejamento e orçamento. Brasília. V. 10, n. 1, p. 80-96, 2020. Disponível em: https://www.assecor.org.br/files/3815/8895/5856/Revista_RBPO-Vol10_n1-05_p.pdf. Acesso em: 02 jul. 2020.

ORWELL, George. 1984. 29ª edição. São Paulo: Companhia Editora Nacional, 2003.

RUARO, Regina Linden; **RODRIGUEZ**, Daniel Piñeiro; **FINGER**, Brunize. O direito a proteção de dados pessoais e a privacidade. Revista da Faculdade de Direito UFPR. Curitiba, v. 53, 2011. Disponível em: https://revistas.ufpr.br/direito/article/view/30768. Acesso em: 03 jul. 2020.

SARLET, Ingo Wolfgang. A eficácia dos direitos fundamentais. 12ª ed. Porto Alegre: Livraria do Advogado. 2015.

SILVA, Moisés Câmara da. A "revolução militar" dos drones (2001 a 2018): da "caçada humana" no Afeganistão às várias frentes de batalha no Oriente Médio e ao aumento da escala da guerra entre as "grandes potências". 2018. 229f. Dissertação (Programa de Pós-graduação em Relações Internacionais - PPGRI) - Universidade Estadual da Paraíba, João Pessoa, 2018.

SPADOTTO, Anselmo José. Análise jurídica e ambiental do uso de drones em área urbana no Brasil. Revista de Direito da Cidade. v. 08, n. 2. p. 611-630. 2016. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rdc/article/view/21809. Acesso em: 09 jul. 2020.

TRINDADE, Rodrigo. Fiscais de máscara, febre e movimentação: como é nosso futuro com drones. Portal UOL. São Paulo, 12/06/2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/06/12/cade-a-mascara-drones-policiais-estao-prontos-para-o-novo-normal-distopico.htm. Acesso em: 06 jul. 2020

UNITED NATIONS. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Disponível em: https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Acesso em: 05 jul. 2020.

WELINDER, Yana. A face tells more than a thousand posts: developing face recognition privacy in social networks. Harvard Journal of Law & Technology. vol. 26, n. 1, 2012. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108. Acesso em: 06 jul. 2020.