As cortes e os desafios da era digital: a vigilância na jurisprudência comparada

The courts and the challenges of the digital age: the surveillance in comparative jurisprudence

José Adércio Leite Sampaio*
Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte – MG, Brasil

1. Introdução

Nos últimos trinta anos, a sociedade se tornou mais digital, mais global e mais conectada. A revolução da tecnologia da informação possibilitou que as pessoas passassem a se comunicar instantaneamente e cada vez mais. A medicina passou a contar com instrumentais que ajudaram nos diagnósticos, tratamento e cura das doenças. Os decisores, inclusive legisladores e formuladores de políticas pública, puderam valer-se de uma quantidade e combinação de dados jamais possíveis, tornando menos complicada a formulação de prognósticos que os auxiliam na escolha das alternativas. Os múltiplos canais de comunicação criaram um horizonte imenso de participação cidadã, prometendo uma revolução também na democracia. Essas, dentre tantas outras virtudes da "sociedade digital", também contam com sérias ameaças. Algumas menos tangíveis (ou menos tangíveis ainda), como as mudanças comportamentais e de mundividência. Outras mais concretas e já presentes, como a sofisticação dos instrumentos da criminalidade e do terrorismo.

Os Estados, a pretexto de combatê-las, também passaram a utilizar das ferramentas que as novas tecnologias lhes propiciaram. Os organismos de inteligência conseguiram coletar, armazenar, tratar e empregar um número massivo de dados pessoais. Essas atividades, pela própria natureza e finalidade, realizam-se secretamente, o que trouxe adicionalmente problemas para os direitos fundamentais e para a democracia. Em diversos Estados democráticos foram aprovadas leis para discipliná-las, embora sem a capacidade de estabelecer adequadamente os quadros de licitude ou, ao menos, sem realizar um adequado ajustamento entre a finalidade de promoção dos interesses estatais, sobretudo, de

* Pós-Doutor em Direito pela Universidad de Castilla-La Mancha (Espanha). Doutor e Mestre em Direito pela Universidade Federal de Minas Gerais. Professor da pós-graduação stricto sensu em Direito da Pontifícia Universidade Católica de Minas Gerais e da Escola Superior Dom Helder Câmara. Procurador da República. E-mail: joseadercio.contato@gmail.com.

segurança nacional e os direitos de indivíduos e grupos. É certo que estabeleceram sistemas de controle e supervisão das atividades de vigilância, mas seria razoavelmente previsível que eles apresentariam seus problemas. Entre esses sistemas não poderia faltar o Judiciário. Seria de se esperar dele um resposta altiva e contundente para prevenir e reparar os danos causados pela "tentação autoritária" dos algoritmos e do mundo digital, sob a perspectiva, ao menos, do controle da vigilância.

O presente artigo analisa como o Judiciário respondeu a essa chamada de responsabilidade. Procurou-se lançar um (primeiro) olhar sobre o problema e tentar responder se o Judiciário, como uma tradicional e requisitada garantia dos direitos, tem atendido às expectativas de prevenção e reparação. A depender da resposta, podem-se lançar desconfianças sobre a capacidade institucional do próprio Judiciário e, por extrapolação, dos demais órgãos constitucionais de promoção dos direitos, de enfrentar os desafios impostos pela nova e ambivalente "realidade virtual". Procurou-se avaliar o repertório de jurisprudência de alguns Estados, aqueles em que as questões já vieram à discussão judicial, seguindo-se, numa metodologia comparativa e indutiva, que se vale da revisão bibliográfica como ancoradouro da reflexão. Na primeira parte, é analisado o quadro geral da sociedade digital para, na segunda, ser apresentado o resultado da pesquisa jurisprudencial em sede nacional.

2. A sociedade digital

A sociedade digital é uma ideia, um processo e uma preocupação. Ideia, pela emergência de relações sociais, de constructos e reproduções culturais a partir da redefinição identitária de indivíduos e grupos na ambivalência criada pelas tecnologias digitais e sua combinação de cálculo mecânico, da eletrônica, do código binário e dos sistemas de linguagem humana, a instituir uma espécie de "sistema operacional" da virtualidade do real e da realidade do virtual[1;2]. Um processo de digitalização e datificação da vida em seus múltiplos aspectos com o emprego das constantes inovações daquelas tecnologias e os prenúncios de uma sociedade automatizada ou, em parte ou inteiramente, guiada por algoritmos[3]. Uma preocupação que se projeta em todos os âmbitos do saber e da práxis, da filosofia à política, da ética ao direito[4]. O "homo digitalis" tem diante de si um horizonte de possibilidades e um turbilhão de ameaças[5]. As ambivalências do virtual e real não deixam de notar que esse "novo" ser, se pode converter-se num e-cidadão, capaz de participar e controlar governos, é também rotineira e mais intensamente monitorado, por vontade própria ou por olhos matemáticos e programas

[1] ATHIQUE, 2013.
[2] Vejam-se as ambivalências do binômio real/virtual: DELEUZE, 1996, p. 55; LÉVY, 1996, p. 12.
[3] DUNHAM, 2015; LOEBBECKE; PICOT, 2015.
[4] E à psicologia e à neurociência com impactos comportamentais e biofuncionais do cérebro (MONTAG; DIEFENBACH, 2018).
[5] Também se identifica uma ambivalência na sinonímia que se encontra na literatura com o "homo numeralis" ou "homo horologium", associados aos ciber-homens do transhumanismo, como substituição ao "homo sapiens" (EDUARDOVYCH, 2019, pp. 147-148).

eletrônicos sofisticados[6;7]. O "homo digitalis" é, desde o seu início, "custodiebantur hominem". Esse é um problema que se põe no tempo presente e não rascunho de uma distopia miserável. Os Estados, a pretexto da defesa da segurança nacional e do combate ao crime, a todos procura vê, ouve, acompanha[8]. Os órgãos de inteligência, nome brando à espionagem e de espia estatal, valem-se de expedientes técnicos refinados para coligir, interceptar, extrair, filtrar, armazenar e analisar imenso volume de informações pessoais, em meios físicos ou eletrônicos, "on" ou "offline", estáticos ou em transmissão, para uso próprio ou compartilhado[9]. Os riscos associados a esse poder e essa prática são igualmente volumosos. Os direitos e a própria democracia correm perigo[10]. As leis procuram discipliná-la, mas, ao discipliná-la, legitimam-na, sendo incapaz de prever todas as possibilidades de aplicação, quando não servem de mero instrumento de legitimação pura e simplesmente[11]. Os mecanismos de supervisão que preveem tendem a ser pouco efetivos, pela captura à lógica securitista ou vigilante[12], restando ao Judiciário a tarefa hercúlea de contê-la nos quadros da legalidade e do respeito aos direitos[13].

Um Judiciário, por certo, dotado das garantias de independência, imparcialidade e um procedimento adequado, tende a minimizar o esforço de cooptação do discurso de emergência securitária antiterror e de combate ao crime; e, portanto, mais preparado a promover o justo equilíbrio entre as necessidades públicas e a proteção dos direitos fundamentais[14]. Claro que os juízes carecem de formação técnica apropriada para lidar com a complexidade dos aparatos tecnológicos de vigilância, mas esse déficit pode, pelo menos, em parte, ser suprido pelo recurso a peritos[15]. As soluções de controle judicial, apresentadas pelos sistemas, são diversas: controle prévio, muito além do controle de constitucionalidade das leis autorizadoras da vigilância, pela exigência de autorização para adoção das medidas; concomitante ao processo de monitoração; e posterior, no exercício de revisão da legalidade e proporcionalidade das medidas. Pode haver uma especialização na forma de colegiados típicos ou em formas atípicas ou mistas; como pode ser competência dos ramos comuns da Justiça. Importa saber, ainda que por uma curta amostragem, como o Judiciário tem respondido ao desafio[16].

3. A jurisprudência de vigilância

[6] MOEREL; PRINS, 2016; HINTZ; DENCIK; WAHL-JORGENSEN, 2017.

[7] Nessa bilateralidade, pelos menos no estágio atual, há menos a atuação cívica e mais a submissão do "sujeito digital", um misto ou compósito de múltiplas forças, identificações, afiliações e associações (ISIN; RUPPERT, 2015, p. 12), expressas em ações atomizadas (PAPACHARISSI, 2010, p. 131), à vigilância estatal (FRIEDMAN, 2018) e aos jogos algorítmicos que podem repercutir nos processos eleitorais (MANHEIM; KAPLAN, 2018).

[8] FELDMAN, 2011; FRIEDMAN, 2018.

[9] LYON, 2019, p. 65.

[10] FELDMAN, 2011; BIGO, 2012.

[11] JAUVERT, 2015; MOREL, 2015; TARROW, 2015, pp. 165-166.

[12] BALZACQ, 2005, DIXIT, 2016.

[13] SAMPAIO, 2002, pp. 79, 677ss; GINSBURG, 2005, p. 227.

[14] ROACH, 2009, pp. 155 ss, 165.

[15] CAMERON, 2000, pp. 157 ss; UNIÃO EUROPEIA, 2007, p. 45.

[16] CAPARINI, 2007, pp. 15-16; FRANÇA, 2016.

A jurisprudência sobre vigilância no direito comparado é vacilante, ora conferindo proteção aos direitos; ora validando as coletas e tratamento intensivo de dados das pessoas. De um modo geral, os Tribunais especializados em controle prévio com a Corte de Vigilância e Inteligência Estrangeiras (*Foreign Intelligence Surveillance Court* – FISC) norte-americana[17], o Comissariado de Poderes de Investigação (*Investigatory Powers Commissioner's Office*) britânico e Comitê Independente (*Unabhängige Gremium*) alemão, assim como os colegiados judicialiformes, ao estilo da Comissão G-10 da Alemanha, do Tribunal de Inteligência e Defesa (*Försvarsunderrättelsedomstol* - FUD) da Suécia, da Comissão de Avaliação de Uso dos Poderes (*Toetsingscommissie Inzet Bevoegdheden* – TIB) dos Países Baixos e do Ofício para Proteção Legal (*Rechtsschutzbeauftragte* – RSB) austríaco revelam uma certa deferência aos serviços de inteligência[18]. O elevado número de ordens concedidas comparativamente às denegadas é um bom termômetro desse quadro[19]. A análise mais profunda é prejudicada pelo sigilo que também existe nos casos em que esses órgãos decidem, normalmente, dando-se acesso apenas a estatísticas e dados gerais que dificultam o exame das razões apresentadas, a menos que haja expressa determinação de publicidade nos julgados. A questão acaba sendo lançada para um eventual controle judicial posterior. Ressalta-se, aqui, primeiramente, a solução do Reino Unido com a especialização de um colegiado de juízes, o Tribunal de Poderes de Investigação (*Investigatory Powers Tribunal* - IPT).

A legislação britânica, como a da maioria dos países europeus, dá uma série de poderes aos órgãos de inteligência para vigiarem as pessoas. Um plexo de normas, denominado pelos críticos de "Carta dos Bisbilhoteiros" (*Snoopers' Charter*)[20], permite a expedição de mandado, por um juiz ou pelo Secretário do Interior, para a vigilância em massa de dispositivos eletrônicos. Essa vigilância pode ocorrer sobre as comunicações ou sobre os dados armazenados nesses dispositivos, coletando, por exemplo, o histórico de navegação da internet e dos aplicativos baixados, os nomes e senhas, bem como a localização em tempo real das pessoas. Por esse emaranhado de normas e pelas deficiências do controle judicial sobre os "serviços secretos da Rainha", a jurisprudência do Tribunal de Poderes de Investigação do Reino Unido não é muito rica em exemplos que mostrem o êxito de instituição de uma Corte especializada para controle posterior[21]. Mesmo assim, há decisões meritórias como a que reputou contrário à Convenção Europeia de Direitos Humanos o regime de obtenção e retenção massiva de dados de comunicações, previsto na Seção 94 da Lei de

[17] Numa das raras ocasiões em que a Corte se posicionou contra pedidos do Governo, foi revelado que o *Federal Bureau of Investigation* – FBI vinha se utilizando de vigilância massiva para investigar testemunhas e informantes em potencial que não eram suspeitos de crimes nem estavam envolvidos com atividades que ameaçassem a segurança nacional. Havia também indicativos de que estivesse usando a chamada "construção paralela" de provas, para inserir aquelas colhidas pelo programa de vigilância em massa da NSA em processos criminais. A vigilância permite que se busquem mandados apenas para legalizar a prática de obtenção de provas (ESTADOS UNIDOS, 2018b).

[18] FRANÇA, 2016.

[19] MURPHY, 2019.

[20] GERSCH, 2012; GILL, 2019.

[21] SCOTT, 2017; MURPHY, 2019.

Telecomunicações de 1984[22;23], modificando seu entendimento de que a intercepção em massa do Reino Unido era lícita. Assim também o fez em relação à legalidade do acesso do Reino Unido à vigilância em massa realizada por órgão de inteligência dos Estados Unidos[24]. Julgados posteriores, no entanto, mostraram-se vacilantes, dando nítidos sinais de retorno à antiga orientação[25;26]. Note-se que o IPT analisa a legalidade dos atos em face das leis de vigilância, sem avaliar, por exemplo, a sua compatibilização com a Convenção Europeia de Direitos Humanos e, menos ainda, com documentos constitucionais que reconheçam direitos fundamentais. A competência de outros órgãos jurisdicionais para exercer esse controle, sobretudo, na segunda hipótese, é polêmica, em face da supremacia do Parlamento. No final de Julho de 2019, a Alta Corte de Justiça foi acionada pelo grupo de direitos humanos "Liberty", solicitando o reconhecimento de violação da Convenção Europeia de Direitos Humanos pela prática de "hackeamento em massa" dos dados pessoais dos britânicos. A Corte, no entanto, concluiu que a vigilância massiva era lícita, sob a perspectiva da "*Human Rights Act*" de 1998. As salvaguardas criadas da "*Investigatory Powers Act 2016* (IPA)", que a autorizava, eram suficientes para evitar o risco de abuso de poder discricionário, não havendo, por conseguinte, violação à Convenção Europeia no procedimento[27;28]. Uma última nota sobre a matéria não pode deixar de ser feita. A Suprema Corte decidiu por uma pequena maioria de 4 a 3 que a "cláusula de exclusão" de recursos contra julgados do IPT, previsto na RIPA (§67 (8)), não impediria apelação fundada em erro de direito[29;30].

Na Alemanha, Tribunal Constitucional Federal acolheu o argumento do governo para não enviar as listas de "seletores" da Agência de Segurança Nacional para a comissão parlamentar de inquérito que investigava a vigilância em massa no País, reconhecendo que a segurança nacional e os interesses da política externa se impunham ao poder investigatório dos parlamentares[3132].Entretanto, declarou

[22] REINO UNIDO, 2016b.

[23] Em "*News Group Newspapers Limited and Others v The Metropolitan Police Commissioner* (IPT/14/176/8)", de 17/12/2015, reconheceu-se a ilegitimidade de vigilância sobre jornalistas, embora não lhes tenha deferido indenização (REINO UNIDO, 2015a).

[24] REINO UNIDO, 2015b.

[25] REINO UNIDO, 2017; 2018.

[26] A matéria foi submetida à Corte Europeia de Direitos Humanos: (PRIVACY INTERNATIONAL, 2016; REINO UNIDO, 2019b).

[27] REINO UNIDO, 2019a.

[28] Houve recurso para a Corte de Apelação, não julgado até o encerramento deste artigo (BBCNEWS, 2019). Apenas para informação, os recursos da "*High Court of Justice*" são feitos perante a "Corte de Apelação" e, subsequentemente, para a Suprema Corte, se se tratar de assunto de alta relevância.

[29] REINO UNIDO, 2019b.

[30] Ainda que em "obiter dictum", a maioria entendeu que era contrário ao Estado de Direito o poder de o Parlamento alterar os modos normais de controle judicial de uma decisão do executivo, ainda que prolatada por um órgão judicial como IPT, fugindo à possibilidade de revisão pela Suprema Corte. A decisão gerou intensa polêmica, pois pode comprometer a supremacia do Parlamento e abrir caminho para o controle de constitucionalidade. (SCOTT, 2020).

[31] ALEMANHA, 2016a.

[32] "*Das Interesse an der Erhaltung der außen- und sicherheitspolitischen Handlungsfähigkeit der Bundesregierung überwiegt das Recht des Untersuchungsausschusses auf Herausgabe der NSA-Selektorenlisten*" (ALEMANHA, 2016a, p. 155). Dois pontos merecem ainda ênfase nesse julgado: o reconhecimento de que os serviços de inteligência são exigências da Lei Fundamental para constituição de uma democracia, autoafirmação do Estado de Direito e para a segurança na República (ALEMANHA, 2016a, p. 139). E o reconhecimento de que a cooperação internacional, no âmbito dos serviços de inteligência, no caso entre

parcialmente contrária à Constituição a triagem de dados em bancos de dados públicos e privados, destinada a encontrar potenciais terroristas, baseada apenas numa ameaça genérica ou em tensões com governos estrangeiros. Embora se tenha reputado compatível com os direitos fundamentais a autorização legal dada à polícia para usar medidas de vigilância secreta, como a realizada em residências particulares, pesquisas remotas de sistemas de tecnologia da informação, vigilância de telecomunicações e coleta de dados de tráfego de telecomunicações para combater o terrorismo internacional, afirmou-se que tais procedimentos somente poderiam ser realizados no caso de perigo concreto para a vida ou liberdade das pessoas ou para a segurança do Estado. Também se declarou desproporcional a permissão de transferência de dados para autoridades de países estrangeiros, estabelecendo alguns princípios que deveriam orientar essa transferência[33;34] Na linha desse julgado, declarou inconstitucional uma série de restrições à Reforma do Sistema de Vigilância estrangeira, aprovada em 2016 ("*Gesetz zur Ausland-Ausland-Fernmeldeaufklärung*"), dando-se o prazo de adequação da Lei até 31 de dezembro de 2021[35]. Embora os serviços de inteligência e vigilância estratégica fossem uma necessidade do Estado, eles deveriam respeitar a Lei Fundamental. A vinculação das autoridade estatais alemãs aos direitos fundamentais não se limitaria ao território alemão, embora pudesse haver um grau diferenciado de proteção àqueles que moravam fora do País. Não a ponto de violar a liberdade de expressão e os direitos de defesa contra a vigilância das telecomunicações (arts. 5(1) e 10(1) da Lei Fundamental) dos estrangeiros no exterior. As normas disciplinadoras da transmissão de informações obtidas por meio dessa vigilância e para a cooperação com serviços de inteligência estrangeiros haviam violado o conteúdo essencial desses direitos. Afirmou-se que a transmissão de dados pessoais de vigilância estratégica somente seria permitida para a proteção de bens jurídicos relevantes e pressupunha uma situação de risco específica ou uma suspeita de crime suficientemente definida, havendo de ser documentada com a devida justificação. Os acordos de cooperação com serviços de inteligência estrangeiros só atenderiam aos requisitos de direitos fundamentais, se garantissem que as exigências do Estado de Direito fossem atendidas pelas trocas mútuas de dados e que fosse preservada a responsabilidade do Serviço de Inteligência Federal (*Bundesnachrichtendienst* – BND) pelos dados que coletasse e avaliasse. Para o Tribunal, era imprescindível que houvesse um controle objetivo e independente "do tipo judicial" da compatibilidade dos poderes de vigilância estratégica, de transmissão dos dados

a NSA norte-americana e o Serviço Federal de Inteligência alemão (BND), integravam a "Regra de Terceiros", o que impunha a confidencialidade sobre os dados, a menos que houvesse o consentimento do provedor de informações (ALEMANHA, 2016a, p. 149/150).

[33] ALEMANHA, 2016b.

[34] "*Die Ermächtigung des Bundeskriminalamts zum Einsatz von heimlichen Überwachungsmaßnahmen (Wohnraumüberwachungen, Online-Durchsuchungen, Telekommunikationsüberwachungen, Telekommunikationsverkehrsdatenerhebungen und Überwachungen außerhalb von Wohnungen mit besonderen Mitteln der Datenerhebung) ist zur Abwehr von Gefahren des internationalen Terrorismus im Grundsatz mit den Grundrechten des Grundgesetzes vereinbar*" (ALEMANHA, 2016b, p. 1)

[35] A reforma deu poderes ao BND, serviço de inteligência estrangeira, e criou um órgão integrado por juízes da Corte Federal de Justiça (Bundesgerichtshof), por ela, indicados, e por um Procurador da República, oficiante perante aquela Corte, indicado pelo Procurador-Geral da República. Não lhe eram atribuídos claramente poderes requisitórios, nem eram garantidos recursos para desempenho da função. Havia uma disciplina lacunosa sobre os intercâmbios de dados do BND com órgãos estrangeiros, dentre outros problemas apresentados na literatura e que foram levados ao Tribunal (WETZLING, 2017).

obtidos e da cooperação com serviços estrangeiros com os requisitos de proporcionalidade; associado a um controle administrativo de legalidade do processo de monitoramento. A independência institucional deveria incluir a garantia de orçamento próprio e autonomia processual, recursos logísticos e humanos que garantissem a eficiência das tarefas realizadas. Ademais, deveriam possuir todos os poderes necessários para um controle efetivo do Serviço de Inteligência Federal[36]. Já no final de 2017, o Tribunal Administrativo Federal (*BVerwG*) havia decidido que o BND não tinha autorização legal para processar os dados da filial alemã da Repórteres Sem Fronteiras (RSF Alemanha), em seu chamado "sistema de análise de tráfego" (VerAS). Por meio desse sistema, os dados de tráfego de telecomunicações, que eram coletados massivamente, pelo BND, podiam ser analisados e interconectados. Depois dessa decisão, o órgão declarou o encerramento da análise de registros de metadados de chamadas telefônicas[37;38] O Tribunal Constitucional da Polônia também declarou parcialmente inconstitucionais e atentatórios à Convenção Europeia de Direitos Humanos diversos dispositivos de leis sobre vigilância eletrônica. As razões giraram basicamente em torno da falta de salvaguardas para realização das operações e do monitoramento dos dados, como a falta de identificação da autoridade responsável ou de supervisão independente, de garantias de destruição imediata de dados irrelevantes ou ilegalmente capturados, bem como por violação de sigilos profissionais[39].

Na França, o Conselho Constitucional julgou que, em caso de vigilância internacional, a exclusão do direito da vítima à indenização por ato ilegal do governo francês era constitucional[40]. Também não deu proteção ao pleito de diversos autores contra um decreto presidencial "confidencial" que permitiria aos serviços secretos a realização de vigilância em massa de comunicações internacionais, contentando-se pura e simplesmente com a afirmação do governo de que tal decreto inexistia[41;42]. Tampouco deu guarida ao argumento de que artigo L-854-1 da Lei de Inteligência, aprovada em 2015, visava legalizar as operações anteriormente feitas às escondidas[43]. No entanto, declarou a inconstitucionalidade de um artigo que excluía do regramento legal e do controle da autoridade independente a vigilância das transmissões por via hertziana, contrariando o argumento de que que as medidas se destinavam a garantir exclusivamente os interesses nacionais. Entendeu-se que a disposição não definia a natureza das medidas de vigilância e controle que as autoridades estavam autorizadas a tomar e

[36] ALEMANHA, 2020.
[37] KLEIN, 2018.
[38] A RSF Alemanha desenvolveu uma ferramenta on-line, chamada de "BND-Generator", para permitir que qualquer pessoa pudesse, com um simples clique de mouse, remover suas informações do banco de dados VerAS (RSF, 2018).
[39] POLÔNIA, 2014; PODKOWIK, 2015.
[40] FRANÇA, 2015.
[41] JAUVERT, 2015; pp. 44-45.
[42] "*Considérant que la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure; qu'en prévoyant que la commission peut former un recours à l'encontre d'une mesure de surveillance internationale, le législateur a assuré une conciliation qui n'est pas manifestement disproportionnée entre le droit à un recours juridictionnel effectif et le secret de la défense nationale*" (FRANÇA, 2015, §18, p. 6-7).
[43] JAUVERT, 2015; MOREL, 2015.

que, ainda assim, tais medidas não estavam sujeitas a qualquer salvaguarda substantiva ou processual[44;45].

Nos Estados Unidos, a Suprema Corte ainda não se pronunciou sobre a legitimidade da vigilância massiva, realizada pelos órgãos de inteligência, embora tenha estabelecido um precedente importante em "Carpenter v. United States". No caso, ela afirmou que as informações de localização dos celulares estavam protegidas pela garantia da Quarta Emenda contra buscas e apreensões desarrazoadas. Refutou-se o argumento, apresentado pelo governo, de que o usuário renunciaria a sua "*privacy*" ao possuir um dispositivo digital. Embora houvesse o entendimento, fundado em precedentes da Corte, de que eram exigidos mandados judiciais de interceptação de chamadas ou para acesso o conteúdo das mensagens, não existia, até a decisão, o reconhecimento de que a proteção constitucional se estendia aos metadados, nos quais se incluem os serviços de localização digital[46;47]. Alguns julgados de primeira instância têm acolhido o argumento do governo de que tais atividades gozariam de imunidade à

[44] FRANÇA, 2016.

[45] "*En dernier lieu, les dispositions contestées ne définissent pas la nature des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre. Elles ne soumettent le recours à ces mesures à aucune condition de fond ni de procédure et n'encadrent leur mise en œuvre d'aucune garantie*" (§8, p. 4). No entanto, ao aceitar o pedido de um governo, o Conselho Constitucional adiou a revogação do artigo L. 811-5 para 1/1/2018, por considerar que a revogação imediata teria o efeito de privar as autoridades públicas de qualquer possibilidade de monitorar transmissões usando o canal de rádio; bem como para permitir ao legislador remediar a inconstitucionalidade constatada (§11). De todo modo, as disposições não poderiam ser interpretadas como capazes de ser usadas como base para medidas para interceptar correspondência, coletar dados de conexão ou capturar dados Sistemas informáticos sem o controle da Comissão Nacional de Controle das Técnicas de Inteligência (*Commission nationale de contrôle des techniques de renseignement* - CNCTR) (FRANÇA, 2016, § 12, pp. 4-5).

[46] ESTADOS UNIDOS, 2018a.

[47] A Corte superou a "*third-party doctrine*", que considerava uma renúncia à "*privacy*" a entrega ou transferência de dados pessoais a terceiros, possibilitando que o Estado tivesse acesso a esses dados sem necessidade de mandado (SAMPAIO, 1997). Um precedente importante usado na decisão fora "United States v. Jones", em que se considerou que a instalação de um dispositivo de rastreamento do Sistema de Posicionamento Global (GPS) em um veículo, usado para monitorar os seus movimentos, constituía uma busca sob a quarta emenda, a exigir mandado (ESTADOS UNIDOS, 2012). A Corte ficou dividida e recebeu muitas críticas. De acordo com a minoria e os críticos, o Estado poderia legitimamente requisitar qualquer informação de propriedade de terceiros, desde que essa requisição não fosse excessivamente onerosa. Como Carpenter, que detinha o celular de cujos dados de localização foram obtidos, não possuía a propriedade desses dados, pois eles pertenciam à telefônica, ele não tinha o direito de contestar a requisição. Ele teria transmitido voluntariamente essas informações à empresa de telefonia celular, por meio da compra de seus serviços (STONE, 2019). É preciso lembrar que a Suprema Corte reconhece há muito tempo que, em circunstâncias excepcionais, os tribunais devem agir no interesse de segurança nacional, de modo a impedir a divulgação de segredos do Estado (ESTADOS UNIDOS, 1875; 1953). Em contrapartida, coube a ela, mesmo diante da política antiterror, reconhecer o direito ao habeas corpus contra tentativas executivas ("Rasul v. Bush", 531 U.S. 98 [2000]) e depois legislativas ("Hamdan v. Rumsfeld", 548 U.S. 557 [2006]), e "Boumediene v. Bush", 553 U.S. 723 [2008]) de cassá-lo em relação aos presos em Guantánamo (ROACH, 2009, pp. 142-143). Assim também, embora não se tenham localizado decisões da Corte Constitucional italiana sobre a "*sorveglianza di massa",* pode-se notar que ela atribui à segurança e segredos de Estado valor constitucional. A segurança do Estado é, para ela, um "interesse essencial e irreprimível da comunidade, com um caráter claro de preeminência absoluta sobre todas as outras, na medida em que afeta [...] a própria existência do Estado" (*La sicurezza dello Stato [costituisce] un interesse essenziale, insopprimibile della collettività, con palese carattere di assoluta preminenza su ogni altro, in quanto tocca (...) la esistenza stessa dello Stato*) (decisão n 40/2012, n. 106/ 2009, n. 86/1977) (ITÁLIA, 1977; 2009; 2012). Sobre o sigilo do Estado, afirmou se tratar de um "*disciplina del segreto involge il supremo interesse della sicurezza dello Stato - comunità alla propria integrità ed alla propria indipendenza, interesse che trova espressione nell'art. 52 della Costituzione in relazione agli artt. 1 e 5 della medesima Carta*" (decisão n. 24/2014) (ITÁLIA, 2014).

fiscalização judicial, por cuidarem de segurança nacional[48]. Entretanto, já há decisões, como a da Corte de Apelação do Segundo Circuito, no sentido de que o programa de coleta de metadados telefônicos, previsto na Seção 215 da "*Patriot Act*", é inconstitucional. Entendeu-se que a necessidade e a proporcionalidade exigiriam que os dados coletados fossem relevantes para uma investigação específica e não para combater o terrorismo em geral[49]. O Tribunal de Apelação do Nono Circuito, na mesma linha, decidiu que o privilégio dos segredos de Estado não se aplicava aos casos em que se discuta a vigilância eletrônica doméstica. Diante da falta de clareza da Lei de Inteligência Estrangeira (FISA), haveria de prevalecer o "direito comum" e a proteção da "*privacy*", revertendo a decisão de primeira instância[50].

Nos Países Baixos, o Tribunal Distrital de Haia também suspendeu norma neerlandesa que obrigava as empresas de telecomunicações a reter os metadados de comunicações de seus clientes para leitura pelas autoridades, por infringir os direitos das pessoas à privacidade e proteção de dados[51;52] Essa é um entendimento encontrado no repertório de decisões de Cortes de outros Estados europeus. O Tribunal Constitucional da Bulgária com a sentença n. 13627/2008, a "Curtea Constituţională" romena com sentença de 8 de outubro de 2009; o Tribunal Constitucional da República Tcheca com sentença de 31 de março de 2011; e a Suprema Corte de Chipre com sentença de 1 de fevereiro de 2011, declararam inconstitucional ou inaplicável disposição que obrigava a retenção de dados pessoais por operadoras e provedores de telefonia e internet[53].

No Canadá, o Tribunal Superior de Justiça de Ontário estabeleceu uma série de princípios que deveriam ser cumpridos para que a coleta de informações dos serviços de telecomunicações fosse proporcional e, portanto, conforme os direitos

[48] Algumas dessas decisões sequer enfrentam a matéria, alegando ilegitimidade ativa de entidades ou indivíduos que, genericamente, questionam a invalidade das leis que autorizam a atuação dos órgãos de inteligência e segurança. No julgamento da Corte Distrital do Norte da Califórnia, afirmou-se que os indivíduos não detinham legitimidade para questionar a legalidade de atos do governo no caso de vigilância da NSA (ESTADOS UNIDOS, 2019). O recurso está pendente de julgamento perante a Corte de Apelação do Nono Circuito. (COHNMAY, 2017). Assim também, em 16/12/2019, a Corte Distrital de Maryland, em "Wikimedia Foundation v. NSA", decidiu que a autora não havia apresentado provas suficientes de que a NSA estava monitorando os usuários da Wikipedia, mas que, mesmo que tivesse feito a prova, o privilégio de segredos de Estado impediria a continuidade do processo. Houve recurso à Corte de Apelação do Quarto Circuito (BUATTI; PALMER, 2019).

[49] ESTADOS UNIDOS, 2015.

[50] ESTADOS UNIDOS, 2019.

[51] PAÍSES BAIXO, 2015.

[52] Entretanto, o Superior Tribunal de Justiça da Irlanda não conheceu de ação movida contra a coleta massiva de dados, com base em legislação doméstica, baseando-se no julgado do Tribunal de Justiça (IRLANDA, 2017). A Suprema Corte não exigiu que a ordem de busca fosse expedida necessariamente por um juiz, mas por uma autoridade imparcial: "*it is necessary for the person authorising the search to be able to assess the conflicting interests of the State and the individual in an impartial manner. Thus, the person should be independent of the issue and act judicially*" (IRLANDA, 2012). A questão está em aberto (McINTYRE, 2016, p. 146). Assim também a Corte Constitucional húngara reputou legítimas as previsões legais de retenção de dados e de autorizações de vigilância que eram deixadas ao Executivo sem controle de órgão independente nem do Judiciário. Entendeu-se "a prevenção e eliminação de riscos à segurança nacional exigem decisões políticas". Nessa matéria somente o Executivo poderia realizar um "equilíbrio justo entre os interesses da segurança nacional e os direitos fundamentais". A Lei, ao obrigar o controle posterior pelo Comissário de Direitos Humanos, atenderia às salvaguardas constitucionais e convencionais necessárias (BESSEGHINI, 2016).

[53] GUELLA, 2017, p. 352.

fundamentais[54]. No México, a Suprema Corte de Justiça exigiu mandado judicial para o acesso e análise de dados armazenados em telefone celular[55], bem como dos metadados de comunicações armazenados pelas empresas de telecomunicações, a incluir os números discados por um usuário, a identidade dos chamadores e a duração da chamada[56]. Um mandado judicial também seria exigido para interceptação de e-mail, abrangendo o acesso à chave ("login") e à senha[57]. Entendeu, porém, que seria dispensável para o monitoramento de geolocalização por celular[58]. Enfim, considerou constitucional a obrigação imposta às operadoras e provedoras de reter dados de comunicação de todos os mexicanos[59].

Na Colômbia, o Tribunal Constitucional, ao examinar a Lei 1621, que disciplina as atividades de inteligência, mas que não trata especificamente da vigilância em massa, reforçou a necessidade de as interceptações das comunicações dependerem de alvo específico, no âmbito de uma investigação criminal, requerendo ordem judicial prévia. Essa ordem pode, no entanto, vir apenas subsequentemente, para verificar a regularidade de medidas determinadas pelo Procurador-Geral da República. Dentre essas medidas, estão a realização de buscas domiciliares, apreensões de dispositivos de armazenamento de dados, exceto se para procurar seletivamente, em um banco de dados, as informações confidenciais de um acusado[60]; bem como a recuperação de informações de registros da internet ou de outras tecnologias similares e a interceptação de comunicações de um acusado em uma investigação criminal, devendo o controle judicial dar-se dentro de 36 horas nesses últimos dois casos[61]. Também há dispensa de ordem judicial para o monitoramento do espectro eletromagnético[62], o que deixa ampla margem à dúvida sobre as salvaguardas dos direitos. O Tribunal ainda entendeu que a instalação de câmeras de vigilância em veículos de transporte público era justificada pelo objetivo legítimo de proteger o interesse geral e garantir a ordem pública. Ressaltou, porém, que a coleta e o armazenamento das informações captadas se submeteriam às disposições da lei sobre proteção de dados pessoais. Independentemente de onde os sistemas de vigilância estivessem instalados, se no espaço público, em locais abertos ao público, em áreas comum, ou em locais que, por serem privados, transcendessem o público, o manuseio e tratamento das informações capturadas pelos sistemas de vigilância deveriam observar os princípios de legalidade, finalidade, liberdade, transparência, acesso e circulação restrita, segurança e confidencialidade e expiração[63]. O mesmo debate se estabeleceu no Chile com a instalação de um sistema de videovigilância, realizada por meio de câmeras aéreas de alta tecnologia montadas em balões de ar quente (rol 18.481/2016) e por drones (rol 38.527/2017). A Suprema Corte entendeu que não haveria violação ao direito à intimidade, se fossem cumpridos certos requisitos como: (a) limitarem-se à coleta em espaços públicos. Em espaços

[54] CANADÁ, 2016.
[55] MÉXICO, 2013.
[56] MÉXICO, 2016.
[57] MÉXICO, 2011.
[58] MÉXICO, 2014.
[59] MÉXICO, 2016.
[60] COLÔMBIA, 2007.
[61] COLÔMBIA, 2007; 2009; 2014.
[62] COLÔMBIA, 2012.
[63] COLÔMBIA, 2020.

privados, somente quando se tratasse de monitoramento de um evento que pudesse constituir a prática de um crime; (b) um delegado municipal deveria certificar, pelo menos uma vez por mês, que nenhuma imagem fora capturada de espaços de natureza privada; (c) as gravações deveriam ser destruídas após trinta dias, a menos que a gravação tivesse capturado uma ofensa ou falha criminal; e (d) todo cidadão deveria ter acesso às gravações[64]. Em geral, a jurisprudência das cortes dos países latino-americanos exige mandado judicial para que sejam interceptadas as comunicações telefônicas e telemáticas, o que importa, pelo menos, em princípio, negativa à vigilância massiva de dados pessoais[65;66].

Assim também na África do Sul. Em setembro de 2019, Supremo Tribunal da África do Sul (*High Court of South Africa*) decidiu e que as leis do país não autorizavam a vigilância em massa. Não fora em caráter absoluto ou do mérito da vigilância intensiva em si, mas pela inexistência de disposições legais que, segundo o governo, dariam amparo à medida. A "*National Strategic Intelligence Act*", ao dar-lhe poder para "reunir, correlacionar, avaliar e analisar informações nacionais e estrangeiras", não permitia que se interceptassem ou coletassem "secretamente as comunicações pela internet". De acordo com o Tribunal, se o governo realmente entendesse que a vigilância em massa fosse tão importante para a segurança nacional, o mínimo que deveria fazer era aprovar "uma lei que di[ssesse] inteligivelmente que o Estado pode fazê-lo", garantindo-se as salvaguardas constitucionais necessária[67;68]. A Suprema Corte da Índia, por igual, afirmou que a vigilância deve ser sempre para alvos determinados ou em atenção a procedimentos que resguardem o direito à "*privacy*" dos indivíduos[69].

Em virtude da pandemia do COVID-19, diversos governos adotaram os instrumentos de vigilância, sob argumento de prevenir a contaminação das pessoas pelo novo coronavírus[70]. Em Israel, por exemplo, o serviço secreto de segurança, "*Shin Bet*", recebeu ordem do Chefe de Governo para começar a rastrear, por meio dos dados de localização dos celulares, os movimentos de israelenses, em um esforço para acompanhar a propagação da doença. O rastreamento visa identificar e pôr em quarenta as pessoas que estiveram em contato a, pelo menos, dois metros e por, no mínimo, dez minutos com alguém que fosse portador do vírus. A tecnologia de rastreamento cibernético era, até então, permitida apenas para a localização de suspeitos de terrorismo. A Suprema Corte de Justiça do País, em

[64] HERRERA, 2018.
[65] RODRIGUEZ, 2017.
[66] A Suprema Corte da Argentina já decidiu que se pode usar do "habeas data" para obtenção de informações sobre dados pessoais que se encontrem nas agências e forças de segurança, sem prejuízo do fato de que o fornecimento dessas informações pudesse, eventualmente, afetar a segurança, a defesa nacional, relações externas ou investigação criminal, assunto que, em cada caso, deve ser invocado pelo chefe da respectiva instituição (ARGENTINA, 1999).
[67] ÁFRICA DO SUL, 2019.
[68] A Corte, ao analisar a "labiríntica" norma sobre a competência do órgão de inteligência, não identificara qualquer autorização para que as comunicações da Internet fossem secretamente coletadas, correlacionadas ou analisadas por serviço de inteligência doméstico e estrangeiro: "*Nowhere else in the NSIA is there a reference to using interception as a tool of information gathering, still less any reference to bulk surveillance as a tool of information gathering*" (p. 60). Para que houvesse vigilância em massa, "*the least that can be required is a law that says intelligibly that the State can do so*" (ÁFRICA DO SUL, 2019, p. 62)
[69] SUBRAMANIAN, 2020.
[70] MELLO; WANG, 2020; MONTJOYE; HOUSSIAU, 2020.

"*Meir v. Prime Minister*", reconheceu a legitimidade da aplicação da medida durante o período da pandemia, entendendo que a proteção da "segurança nacional", prevista pela Lei do "*Shin Bet*", abrangia situações de emergência sanitária. Proibiu, no entanto, que a polícia usasse as informações coligidas para outras finalidades persecutórias. Baseando-se na "doutrina de não delegação", segundo a qual os principais parâmetros para o exercício da discrição administrativa devem ser previstos em lei formal, determinou ao Parlamento a aprovação de lei para disciplinar a medida, tendo em vista que o Primeiro-Ministro a regulara com base em seu poder de emergência, bem como para instituir uma comissão parlamentar para acompanhar a sua execução[71].

No Brasil, não há uma legislação específica sobre vigilância intensiva. Existe um plexo de normas esparsas de proteção de informações pessoais em bancos dados (como o Código de Defesa do Consumidor, Lei de Telecomunicações, Código Civil, Lei de Cadastro Positivo, Lei de Acesso à Informação e Marco Civil da Internet), a serem mais bem sistematizadas pela Lei Geral de Proteção (Lei 13.709/2018), e a disciplina da interceptação das comunicações telefônicas e telemáticas (Lei 9.296/1996)[72]. A jurisprudência tem dado respostas igualmente fragmentadas, notadamente na esfera penal, mas que podem sinalizar precedentes importantes para uma eventual discussão sobre possibilidade e limites de um procedimento de inteligência. Entende-se, por exemplo, que a proteção constitucional ao sigilo das comunicações de dados, conferida pelo art. 5º, XVII, da Constituição, requer a expedição de mandado judicial ou de autorização consciente do investigado para apreensão de computadores[73]. Mesmo nessa derradeira hipótese, o exame pericial nos equipamentos apreendidos é condicionado à autorização específica da autoridade judicial responsável pela supervisão das investigações[74]. Já se afirmou também que há proteção constitucional da comunicação "de dados" e não dos "dados em si mesmos", ainda quando armazenados em computador[75], de modo que "a obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não depende dos procedimentos previstos na Lei de Interceptação Telefônica (Lei 9.296/1996)"[76], o que é duvidoso e parece discutível mais ainda pelo fato de, com o Marco Civil da Internet, passarem a ser protegidas, de modo expresso, as conversas armazenadas em dispositivos eletrônicos (art. 7º, III)[77]. No Superior Tribunal de Justiça, já havia firme entendimento de que a prova oriunda do acesso aos dados armazenados no aparelho celular, relativos a mensagens de texto, SMS, conversas por meio de aplicativos (inclusive "WhatsApp") e correios eletrônicos, obtidos pela polícia no momento da prisão em flagrante e sem prévia autorização judicial, era ilícita, por violar à intimidade e à vida privada do indivíduo, no termos do art. 5°, X, da Constituição[78;79]. Talvez a resposta mais promissora tenha sido dada pelo STF com

[71] ISRAEL, 2020. CHAHCKO, 2020; MAGID, 2020.
[72] PINHEIRO, 2020.
[73] BRASIL, 1994.
[74] BRASIL, 2006.
[75] BRASIL, 2006.
[76] BRASIL, 2017.
[77] BRASIL, 2014.
[78] BRASIL, 2017.
[79] O Tribunal Superior do Trabalho tem admitido a videovigilância nos locais de trabalho, salvo em recintos íntimos como vestiários, refeitórios e banheiros, como forma de prevenir contra furtos e roubos (AIRR n.

a suspensão da medida provisória que obrigava as empresas de telefonia fixa e móvel a disponibilizar ao Instituto Brasileiro de Geografia e Estatística (IBGE) a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas. Os dados compartilhados seriam utilizados para a produção de estatística oficial por meio de entrevistas domiciliares não presenciais. O problema não seria a obrigação em si, mas a falta de definição "apropriada" de "como" e "para que" seriam utilizados os dados coletados. De acordo com a relatora, "a norma não oferec[ia] condições para a avaliação da sua adequação e necessidade. Desatende[ria], assim, a garantia do devido processo legal" [80]. A situação de emergência, criada pela pandemia da COVID-19, não poderia gerar um regime de coleta dos dados, sem o reforço das garantias procedimentais para evitar o abuso ou desvio de finalidade no tratamento. A proteção aos direitos da esfera privada havia sido vulnerada[81].

4. Considerações finais

Embora a sociedade digital, produto da revolução tecnológica e das comunicações, a integrar linguagem humana e linguagem de máquina, crie um mundo de comodidades e de melhoria na qualidade de vida, traz uma série de riscos associados, da ética à política, da moral ao direito. Um desses riscos é dado pela prática da vigilância intensiva que propicia. Os Estados, a pretexto de defenderem a segurança nacional e combaterem a criminalidade, passaram a dotar os organismos especializados em vigilância de estruturas técnicas e de suportes legais para realização de coleta, filtragem, armazenamento, tratamento, emprego próprio ou compartilhado de um grande volume de dados pessoais.

Os mecanismos de supervisão, instituídos pelas leis, apresentam problemas de efetividade, seja pela própria dinâmica das atividades de inteligência, seja pela captura à retórica de securitização. Nesse ambiente nebuloso, o Judiciário é chamado a intervir em defesa dos direitos fundamentais e, em última instância, da própria democracia. Os sistemas dão respostas diferentes às necessidades de controle judicial da vigilância. Às vezes, negando-o. Na maioria das vezes, admitindo-o, na forma de órgãos jurisdicionais ou judicialiformes especializados ou da Justiça comum; em controle prévio, concomitante ou sucessivo. A jurisprudência é demasiadamente variada.

Órgãos jurisdicionais especializados, na competência de controle prévio, como a FISC norte-americana, ou de controle sucessivo, como o IPT britânico, têm-se mostrado muito deferente às demandas dos órgãos de inteligência. A Justiça ordinária e constitucional tem apresentado resultados vacilantes. Admite-se, por exemplo, a legitimidade da vigilância em massa, na jurisprudência britânica e francesa; embora tenha encontrado obstáculo no Tribunal Constitucional Federal da Alemanha, na Corte Constitucional polonesa, no Supremo Tribunal da África do

1830/2003-011-05-40. 3a Tr, AIRR 1926/2003-044-03-40.6, de 2/4/2005); assim também o empregador pode obter provas para a justa causa por meio do rastreamento do e-mail corporativo, utilizado pelo empregado (TST-RR-613/2000-013-10-00.7) (RUARO; HAIIZENREDER JR., 2015)

[80] BRASIL, 2020; D'AGOSTINO; VIVAS; FALCÃO, 2020.

[81] *Os Ministros parecem reconhecer, embora sem enunciação muito clara, um direito à proteção de dados pessoais autônomo, prescindindo da tutela da esfera íntima e familiar das pessoas.*

Sul e da Índia. A exigência de mandado judicial prévio e individualizado, o que equivale à negativa das interceptações intensivas, é encontrada na orientação das Cortes Supremas da América Latina, como na Argentina, no Brasil e no México. O Tribunal Constitucional colombiano não o requer para interceptação do espectro eletromagnético. O estabelecimento de supervisão adequada dos serviços de vigilância eletrônica aparece no repertório jurisprudencial de vários lugares como na Alemanha, na França e na Polônia, assim como na orientação de tribunais inferiores no Canadá. O armazenamento de dados e mesmo de metadados é admitido pelas cortes de alguns lugares; e refutado por outras, como na Bulgária, no Chipre e na República Tcheca.

A vigilância por câmeras em locais públicos é tolerada pelos tribunais de praticamente todos os países, desde que cercada de algumas cautelas, a exemplo do Chile e da Colômbia. Os serviços de geolocalização prescindem de autorização judicial na Suprema Corte do México, mas não, para a Suprema Corte dos Estados Unidos. A jurisprudência, todavia, é mutante como a própria tecnologia envolvida. Ao que parece, o Judiciário ainda não encontrou seu exato lugar no mundo datificado. Se é que encontrará algum dia.

Referências

ÁFRICA DO SUL. Alta Corte. *Case 25978/2017, Amabhungande Centre for Investigave Journalist v. Minister of Justice*. Joanesburgo, 16 de setembro de 2019. Disponível em: https://privacyinternational.org/sites/default/files/2019-09/Judgment%20AMABHUNGANE%20v%20MIN%20JUSTICE%20%26%20OTH.pdf. Acesso em: 22 mar. 2020.

ALEMANHA. *BVerfGE 143*, 1. [S.I.], de 20 de setembro de 2016a. Disponível em: https://www.servat.unibe.ch/dfr/bv143001.html. Acesso em: 11 fev. 2020.

ALEMANHA. Tribunal Constitucional Federal. *1 BvR 966/09*. Karlsruhe, 20 de abril de 2016b. Disponível em:https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html. Acesso em: 11 fev. 2020.

ALEMANHA. Tribunal Constitucional Federal. *1 BvR 2835/17*. Karlsruhe, 19 de maio de 2020. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html. Acesso em 20 mai. 2020.

ARGENTINA. Suprema Corte de Justicia de la Nación. *Ganora, Mario Fernando y otra s/ hábeas corpus.* Buenos Aires, 16 de setembro de 1999. Disponível em: https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verUnicoDocumentoLink.html?idAnalisis=473193&cache=1622590265560. Acesso em: 11 mar. 2020.

ATHIQUE, Adrian. *Digital Media and Society*: An Introduction. Cambridge: Polity Press, 2013.

BALZACQ, Thierry. The three faces of securitization: Political agency, audience and context. *European journal of international relations*, [S.I.], v. 11, n. 2, p. 171-201, 2005.

BBCNEWS. Rights group loses mass surveillance appeal in High Court. *BBC,* [S.I.], 19 jul. 2019. Disponível em: https://www.bbc.com/news/uk-49153593. Acesso em: 15 mar. 2021.

BESSEGHINI, Maschietto M. *Szabò and Vissy v. Hungary: a step back?* Lexology, [S.I.], 5 dez. 2016. Disponível em: https://www.lexology.com/library/detail.aspx?g=435b47eb-31a0-4240-b17a-27894e7fffd7. Acesso em: 20 mai. 2020.

BIGO, Didier. Security, surveillance and democracy. *Routledge handbook of surveillance studies*, [S.I.], v. 27, pp. 277-84, 2012.

BRASIL. *Lei nº 9.296, de 24 de julho de 1996.* Brasília, DF: Presidência da República, 24 jul. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm#:~:text=Art.,principal%2C%20sob%20segredo%20de%20justi%C3%A7a.>. Acesso em: 20 mar. 2020.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Brasília, DF: Presidência da República, 23 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 mar. 2020.

BRASIL. Superior Tribunal de Justiça. 5ª Turma. *RHC 77.232/SC*. Relator: Ministro Félix Fischer, Brasília, 03 de outubro de 2017. Disponível em: https://processo.stj.jus.br/processo/revista/inteiroteor/?num_registro=201602706592&dt_publicacao=16/10/2017. Acesso em: 16 mar. 2020.

BRASIL. Supremo Tribunal Federal. Pleno. *ADI-MC 6387/DF*. Relatora: Ministra Rosa Weber, Brasília, 07 de maio de 2020. Disponível em: https://www.migalhas.com.br/arquivos/2020/4/C47A659344BE14_compartilhamento.pd. Acesso em: 8 mai. 2020.

BRASIL. Supremo Tribunal Federal. Pleno. *AP 307/DF.* Relator: Ministro Ilmar Galvão, Brasília, 13 de dezembro de 1994. Disponível em: http://www.stf.jus.br/portal/inteiroTeor/obterInteiroTeor.asp?numero=307&classe=AP. Acesso em: 20 mar. 2020.

BRASIL. Supremo Tribunal Federal. Pleno. *RE 418416/SC*. Relator: Ministro Sepúlveda Pertence, Brasília, 10 de maio de 2006. Disponível em: http://www.stf.jus.br/portal/inteiroTeor/obterInteiroTeor.asp?id=395790. Acesso em: 20 mar. 2020.

BUATTI, Jim; PALMER, Aeryn. *District Court rules for government in Wikimedia Foundation's mass surveillance case against the NSA*. Wikimedia Foundation, [S.I.], 17 dez. 2019. Disponível em: https://wikimediafoundation.org/news/2019/12/17/district-court-rules-for-government-in-wikimedia-foundations-mass-surveillance-case-against-the-nsa/. Acesso em: 20 mar. 2020.

CAMERON, Iain. *National Security and the European Convention on Human Rights.* The Hague: Kluwer Law; Martinus Nijhoff, 2000.

CANADÁ. Ontario Superior Court of Justice. *R v. Rogers Communications.* Ontario, 14 de janeiro de 2016. Disponível em: https://www.mcinnescooper.com/wp-content/uploads/2016/06/ECLR-Jan-Feb-2016-pg-15-16.pdf. Acesso em 11 abr. 2020.

CAPARINI, Marina. Controlling and overseeing intelligence services in democratic states. *In*: BORN, Hans; CAPARINI, Marina (eds). *Democratic control of intelligence services*: Containing rogue elephants. London: Routledge, 2007, p. 3-24.

CHAHCKO, Elena. *The Israeli Supreme Court Checks COVID-19 Electronic Surveillance.* Lawfare, [S.I.], 05 maio 2020. Disponível em: https://www.lawfareblog.com/israeli-supreme-court-checks-covid-19-electronic-surveillance. Acesso em: 20 abr. 2020.

COHNMAY, Cindy. *Judge Orders Government to Provide Evidence About Internet Surveillance*. EFF, [S.I.], 23 abr. 2017. Disponível em: https://www.eff.org/deeplinks/2017/05/judge-orders-government-provide-evidence-about-internet-backbone-upstream. Acesso em: 17 mar. 2020

COLÔMBIA. Corte Constitucional. *Expediente D-11902 Boletín No. 31***.** Bogotá, 04 de março de 2020. Disponível em: https://www.corteconstitucional.gov.co/noticia.php?Corte-declara-ajustados-a-la-Constituci%C3%B3n-apartes-del-C%C3%B3digo-de-Polic%C3%ADa-que-se-refieren-al-uso-de-c%C3%A1maras-de-vigilancia-e-hizo-precisiones-sobre-el-manejo-y-tratamiento-de-informaci%C3%B3n-captada-y-almacenada-en-sistemas-de-video-o-medios-tecnol%C3%B3gicos-8869. Acesso em 20 mar. 2020.

COLÔMBIA. Corte Constitucional. Pleno. *Sentencia C-131.* Bogotá, 24 de fevereiro de 2009. Disponível em: http://www.corteconstitucional.gov.co/ RELATORIA / 2009 / C-131-09.htm.

COLÔMBIA. Corte Constitucional. Pleno. *Sentencia C-336*. Bogotá, 09 de maio de 2007. Disponivel em: https://www.corteconstitucional.gov.co/relatoria/2007/C-336-07.htm. Acesso em: 11 mar. 2020.

COLÔMBIA. Corte Constitucional. *Sentencia C-540/12.* Bogotá, 2012. Disponível em: https://www.corteconstitucional.gov.co/relatoria/2012/c-540-12.htm. Acesso em 1 mai. 2020.

COLÔMBIA. Corte Constitucional. Pleno. *Sentencia C-594.* Bogotá, 20 de agosto de 2014. Disponível em: https://www.corteconstitucional.gov.co/RELATORIA/2014/C-594-14.htm. Acesso em 11 mar. 2020.

D'AGOSTINO, Rosanne; VIVAS, Fernanda; FALCÃO, Márcio. STF decide manter suspenso repasse ao IBGE de dados de usuários de empresas de telefonia. *G1,* Brasília, 07 maio 2020. Disponível em: https://g1.globo.com/politica/noticia/2020/05/07/stf-decide-manter-suspenso-repasse-de-dados-de-usuarios-de-empresas-de-telefonia-ao-ibge.ghtml. Acesso em: 07 mai. 2020.

MONTJOYE, Yves-Alexandre; HOUSSIAU, Florimond. *Can we fight COVID-19 without resorting to mass surveillance?* CPG Blog*,* Londres, 21 mar. 2020. Disponível em: https://cpg.doc.ic.ac.uk/blog/pdf/fighting-covid-19.pdf. Acesso em: 15 abr. 2020.

DELEUZE, Gilles. O atual e o virtual. *In*: ALLIEZ, Éric (ed). *Deleuze*: filosofia virtual. Trad. Heloisa B. S. Rocha. São Paulo: Ed. 34, 1996.

DIXIT, Priya. Securitization and terroristization: analyzing states' usage of the rhetoric of terrorism. *In*: KOCH, Bettina (ed). *State Terror, State Violence*: Global Perspectives*.* Wiesbaden: Springer VS, 2016, p. 31-50.

DUNHAM, Ian M. Big Data: A Revolution That Will Transform How We Live, Work, and Think. *The AAG Review of Books,* [S.I.], v. 3, n. 1, pp. 19-21, 2015.

EDUARDOVYCH, Radutniy O. Adaptation of criminal and civil law in view of scientific-technical progress (artificial intelligence, dao and digital human). *Problems of Legality,* [S.I.], n. 144, p. 138-152, 2019. Disponível em: http://plaw.nlu.edu.ua/article/view/155819. Acesso em: 11 mar. 2020.

ESTADOS UNIDOS. Corte de Apelação do Segundo Circuito. *American Civil Liberties Union v. Clapper*. [S.I.], 29 de outubro de 2015. Disponível em: https://law.justia.com/cases/federal/appellate-courts/ca2/14-42/14-42-2015-10-29.html. Acesso em: 11 abr. 2021.

ESTADOS UNIDOS. Foreign Intelligence Surveillance Court*. Memorandum Opinion and Order.* Washington, 18 de outubro de 2018b. Disponível em: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf Acesso em: 22 mar. 2020.

ESTADOS UNIDOS. Suprema Corte. *Carpenter v. United States,* 585 U. S (2018). Washington, 22 de junho de 2018a. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. Acesso em 22 mar. 2020.

ESTADOS UNIDOS. Suprema Corte. *Totten v. United States,* 95 U.S. 105 (1875). Washington, 1875. Disponível em: https://supreme.justia.com/cases/federal/us/92/105/. Acesso em: 15 mar. 2020.

ESTADOS UNIDOS. Suprema Corte. *United States v. Jones*, 565 U.S. 400 (2012). Washington, 23 de janeiro de 2012. Disponível em: https://www.supremecourt.gov/opinions/11pdf/10-1259.pdf. Acesso em 22 mar. 2020.

ESTADOS UNIDOS. Suprema Corte. *United States v. Reynolds,* 345 U.S. 1 (1953). Washington, 1953. Disponível em: https://supreme.justia.com/cases/federal/us/345/1/. Acesso em: 15 mar. 2020.

ESTADOS UNIDOS. Tribunal de Apelação do Nono Circuito. *Fazaga v. FBI.* [S.I.], 28 de fevereiro de 2019. Disponível em: http://cdn.ca9.uscourts.gov/datastore/opinions/2019/02/28/12-56867.pdf. Acesso em 20 mar. 2020.

FELDMAN, Shelley. Surveillance and Securitization. *In*: FELDMAN, Shelley; GEISLER, Charles C.; MENON, Gayatri A. (ed). *Accumulating insecurity*: violence and dispossession in the making of everyday life. Athens: University of Georgia Press, 2011, p. 185-212.

FRANÇA. Conselho Constitucional. *Décision n° 2015-722*. Paris, 26 de novembro de 2015. Disponível em: https://www.conseil-constitutionnel.fr/decision/2015/2015722DC.htm. Acesso em: 22 abr. 2020.

FRANÇA. Conselho Constitucional. *Décision n° 2016-590 QPC.* Paris, 21 de outubro de 2016**.** Disponível em: https://www.conseil-constitutionnel.fr/decision/2016/2016590QPC.htm. Acesso em: 22 abr. 2020.

FRIEDMAN, Lawrence. Remnants of Information Privacy in the Modern Surveillance State. *New England Law Review,* Boston, v. 52, n. 1, p. 19-03, 2018.

GERSCH, Adam. Covert surveillance-a snoopers' charter. *Archbold Review*, [S.I.], p. 5-8, 2012.

GILL, Barnaby. *The Wheel of Reincarnation Turns Again: Time for Another Go at the Clipper Chip?* Researchgate, [S.I.], dec. 2019. Disponível em: https://www.researchgate.net/profile/Barnie_Gill/publication/340209335_The_Wheel_of_Reincarnation_Turns_Again_Time_for_Another_Go_at_the_Clipper_Chip/links/5e7cf427299bf1a91b7eda58/The-Wheel-of-Reincarnation-Turns-Again-Time-for-Another-Go-at-the-Clipper-Chip.pdf. Acesso em: 15 fev. 2021.

GINSBURG, Tom. Beyond Judicial Review: Ancillary Powers of Constitutional Courts. *In*: GINSBURG, Tom; KAGAN, Robert (eds). *Institutions and public Law*: Comparative approaches. New York: Peter Lang Publishing Inc, 2005, p. 225-244.

GUELLA, Flavio. Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali. *DPCE Online*, [S.I], v. 30, n. 2, pp. 349-357, 2017.

HERRERA, Samuel M. Videovigilancia y privacidad: Consideraciones en torno a los casos Globos y Drones. *Revista Chilena de Derecho y Tecnología,* Santiago, v. 7, n. 2, p. 137-162, 2018.

HINTZ, Arne; DENCIK, Lina; WAHL-JORGENSEN, Karin. Digital citizenship and surveillance| digital citizenship and surveillance society—introduction. *International Journal of Communication,* Los Angeles, v. 11, p. 731–739, 2017.

IRLANDA. Superior Tribunal de Justiça (High Court). *Digital Rights Ireland -v- Minister for Communications,* IEHC 307. Dublin, 2017. Disponível em: http://courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/0190a4f5271f984980258191004109f7?OpenDocument. Acesso em: 11 abr.2020.

IRLANDA. Suprema Corte. *Damache v DPP,* IESC 11. Dublin, 2012. Disponível em: https://www.legislationline.org/download/id/4060/file/Supreme_Court_Ali_Charaf_Damache_FEb%202012.pdf. Acesso em: 11 abr. 2020.

ISIN, Engin; RUPPERT, Evelyn. *Becoming digital citizens.* Lanham: Rowman & Littlefield, 2015.

ISRAEL. Suprema Corte de Justiça*. Meir v. Prime Minister.* Jerusalém, 19 de março de 2020. Disponível em: https://versa.cardozo.yu.edu/sites/default/files/upload/opinions/Ben%20Meir%20v.%20Prime%20Minister.pdf. Acesso em: 20 abr. 2020.

ITALIA. Corte Constitucional. *Decisão 24/2014*. Roma, 2014. Disponível em: http://www.giurcost.org/decisioni/2014/0024s-14.html. Acesso em: 20 abr. 2020.

ITALIA. Corte Constitucional. *Decisão 40/2012*. Roma, 2012 Disponível em: http://www.giurcost.org/decisioni/2012/0040s-12.html. Acesso em: 20 abr. 2020.

ITALIA. Corte Constitucional. *Decisão 86/1977.* Roma, 1977. Disponível em: http://www.giurcost.org/decisioni/1977/0086s-77.html. Acesso em: 10 abr. 2020.

ITALIA. Corte Constitucional. *Decisão 106/2009*. Roma, 2009. Disponível em: http://www.giurcost.org/decisioni/2009/0106s-09.html. Acesso em: 20 abr. 2020.

JAUVERT, Vicent. Coomente la France écoute (aussi) le monde. *L'Obs,* [S.I.], 01 jun. 2015. Disponível em: https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html. Acesso em 14 abr. 2020.

KLEIN, Sebastian. Federal Administrative Court Prohibits Storage and Use of Telecommunications Metadata by the Federal Intelligence Service. *European Data Protection Law Review*, Berlim, v. 4, p. 110-113, 2018.

LÉVY, Pierre. *O que é o virtual?* Trad. Paulo Neves. São Paulo: Ed. 34, 1996.

LOEBBECKE, Claudia; PICOT, Arnold. Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *The Journal of Strategic Information Systems*, [S.I.], v. 24, n. 3, p. 149-157, 2015.

LYON, David. Surveillance capitalism, surveillance culture and data politics *In*: BIGO, Didier; ISIN, Engin; RUPPERT, Evelyn (eds). *Data Politics:* Worlds, Subjects, Rights. London; New York: Routledge, 2019, p. 64-77.

MAGID, Jacob. High Court lets Shin Bet continue phone tracking now Knesset oversight in place. *The Times of Israel*, [S.I.], 25 mar. 2020. Disponível em: https://www.timesofisrael.com/high-court-green-lights-phone-surveillance-after-knesset-oversight-panels-formed/. Acesso em 20 abr. 2020.

MANHEIM, Karl M.; KAPLAN, Lyric. Artificial Intelligence: Risks to Privacy and Democracy. *The Yale Journal of Law & Technology*, New Haven, v. 21, p. 106-188, 2018.

McINTYRE, T.J. Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective. *In*: SCHEININ, Martin; KRUNKE, Helle; AKSENOVA, Marina (eds.). *Judges as Guardians of Constitutionalism and Human Rights*. Cheltenham: Edward Elgar, 2016, p. 136-172.

MELLO, Michelle M.; WANG, C. Jason. Ethics and governance for digital disease surveillance. *Science*, [S.I.], v. 368, n. 6494, p. 951-954, 2020.

MÉXICO. Suprema Corte de Justiça da Nação. 1ª Sala. *Amparo en Revisión 1621/2010*. Cidade do México, 01 de agosto de 2011. Disponível em: https://suprema-corte.vlex.com.mx/vid/voto-particular-amparo-directo-revision-326743599. Acesso em 15 mar. 2020.

MÉXICO. Suprema Corte de Justiça da Nação. 1ª Sala. *Contradicción de Tesis 194/2012*. Cidade do México, 28 de fevereiro de 2013. Disponível em: https://suprema-corte.vlex.com.mx/vid/-472091286. Acesso em 15 mar. 2020.

MÉXICO. Suprema Corte de Justiça da Nação. 2ª Sala. *Amparo en Revisión 964/2015*. Cidade do México, 04 de maio de 2016. Disponível em: https://www.supremacorte.gob.mx/sites/default/files/versiones-taquigraficas/documento/2016-11-22/versión%20publica%20del%204%20de%20mayo%20de%202016_0.pdf. Acesso em 15 mar. 2020.

MÉXICO. Suprema Corte de Justiça da Nação. Sessão Plenária. *Acción de Inconstitucionalidad 32/2012*. Cidade do México, 16 de janeiro de 2014. Disponível em: https://www.cndh.org.mx/sites/default/files/doc/Acciones/Acc_Inc_2012_32_Demanda.pd. Acesso em 15 mar. 2020.

MOEREL, Lokke; PRINS, Corien. Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things. *SSRN 2784123*, [S.I.], 25 maio 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123. Acesso em: 11 mar. 2020.

MONTAG, Christian; DIEFENBACH, Sarah. Towards homo digitalis: important research issues for psychology and the neurosciences at the dawn of the internet of things and the digital society. *Sustainability*, [S.I.], v. 10, n. 2, pp. 415-436, 2018. Disponível em: https://www.mdpi.com/2071-1050/10/2/415/pdf. Acesso em: 11 mar. 2020.

MOREL, Camille. Stratégie maritime – Le réseau mondial de câbles sous-marins: une toile dans la Toile. *Revue Défense Nationale*, Paris, v. 2015/9, n. 784, p. 117-120, 2015.

MURPHY, Cian C. State Surveillance and Social Democracy: Lessons after the Investigatory Powers Act 2016. *SSRN 3494880*, [S.I.], 16 dec. 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3494880. Acesso em 20 abr. 2020.

PAÍSES BAIXOS. Tribunal Distrital de Haia. *Privacy First Foundation c.s. versus The Netherlands*. Haia, 11 de março de 2015. Disponível em: http://theiii.org/documents/DutchDataRetentionRulinginEnglish.pdf. Acesso em 11 abr. 2020.

PAPACHARISSI, Zizi A. *A private sphere:* Democracy in a digital age. Cambridge: Polity Press, 2010.

PINHEIRO, Patricia P. *Proteção de Dados Pessoais*: Comentários à Lei n. 13.709/2018-LGPD. São Paulo: Saraiva Educação SA, 2020.

PODKOWIK, Jan. Privacy in the digital era – Polish electronic surveillance law declared partially unconstitutional: Judgment of the Constitutional Tribunal of Poland of 30 July 2014, K 23/11. *European Constitutional Law Review*, Cambridge, v.11, n. 3, p. 577-595, 2015.

POLÔNIA. Tribunal Constitucional. *K 23/11*. Varsóvia, 30 de julho de 2014. Disponível em: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20140001055/O/D20141055.pdf. Acesso em: 22 mar 2020.

PRIVACY INTERNATIONAL. *Privacy International v. Secretary of State for the Foreign and Commonwealth Office et al.* (UK Mass Surveillance / UK-US Intelligence Sharing). Privacy International, [S.I.], 2016. Disponível em: https://privacyinternational.org/legal-case-files/1619/privacy-international-v-secretary-state-foreign-and-commonwealth-office-et-al. Acesso em 20 fev. 2020.

REINO UNIDO. Alta Corte de Justiça. Queen's Bench Division. Divisional Court. *Liberty v. Secretary of State for the Home Department et al.* Westminster, 29 de julho de 2019a. Disponível em: https://www.judiciary.uk/wp-content/uploads/2019/07/Liberty-judgment-Final.pdf. Acesso em 20 mar. 2020.

REINO UNIDO. *Investigatory Powers Act 2016.* 2016a. Disponível em: http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted. Acesso em: 22 mar. 2020.

REINO UNIDO. Investigatory Powers Tribunal. *Liberty & Others v. the Security Service, SIS*, GCHQ, IPT/13/77/H. Londres, 22 de junho de 2015b. Disponível em: https://www.ipt-uk.com/judgments.asp?id=27. Acesso em 20 mar. 2020.

REINO UNIDO. Investigatory Powers Tribunal. *News Group Newspapers Limited and Others v The Metropolitan Police Commissioner*. IPT/14/176/8. Londres, 17 de dezembro de 2015a. Disponível em: https://www.ipt-uk.com/judgments.asp?id=30. Acesso em 20 abr. 2020.

REINO UNIDO. Investigatory Powers Tribunal. *News Privacy International v Secretary of State for Foreign and Commonwealth Affairs* (No. 2) (Note) UKIPTrib 15_110-CH. Londres, 18 de dezembro de 2017. Disponível em: https://www.ipt-uk.com/docs/Privacy%20International%20v%20SSFCA%20and%20Ors%201%20December%202017.pdf. Acesso em: 20 mar. 2020.

REINO UNIDO. Investigatory Powers Tribunal. *News Privacy International v Secretary of State for Foreign and Commonwealth Affairs* 2 All ER 166. Londres, 2018. Disponível em: https://www.matrixlaw.co.uk/wp-content/uploads/2018/07/Privacy-International-v-Secretary-of-State-for-Foreign-and-Commonwealth-Affairs-2018-UKIP-Trib-IPT-15-110-CH.pdf. Acesso em: 20 mar. 2020.

REINO UNIDO. Investigatory Powers Tribunal. *Privacy International v. Secretary of State for the Foreign and Commonwealth Office et al* UKIPTrib 15_110-CH. Londres, 17 de outubro de 2016b. Disponível em: https://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf. Acesso em 20 mar. 2020.

REINO UNIDO. Suprema Corte. *R (Privacy International) v Investigatory Powers Tribunal and others,* UKSC 22. Londres, 15 de maio de 2019b. Disponível em: https://www.supremecourt.uk/cases/uksc-2018-0004.html. Acesso em 11 mar. 2020.

SEM FRONTEIRAS (RSF). BND ends illegal data processing after ruling on RSF Germany lawsuit. *RSF*, 23 maio 2018. Disponível em: https://rsf.org/en/news/bnd-ends-illegal-data-processing-after-ruling-rsf-germany-lawsuit. Acesso em 5 mar. 2020.

ROACH, Kent. Judicial Review of the State's Anti-Terrorism Activities: The Post 9/11 Experience and Normative Justifications for Judicial Review. *Indian Journal of Constitutional Law*, Hyderabad, v. 3 p. 138-167, 2009.

RODRIGUEZ, Katitza. *Comparative Analysis of Surveillance Laws and Practices in Latin America*. EFF, [S.I.], out. 2017. Disponível em:

https://necessaryandproportionate.org/comparative-analysis-surveillance-laws-and-practices-latin-america. Acesso em: 11 fev. 2020.

RUARO, Regina Linden; HAIZENREDER JÚNIOR, Eugênio Haizenreder. Proteção da privacidade no contrato de trabalho: Da normatização legal a situações de conflitos. *Espaço Jurídico: Journal of Law*, Chapecó, v. 16, n. 2, p. 601-636, 2015.

SAMPAIO, José Adércio L**.** *A Constituição Reinventada pela Jurisdição Constitucional.* Belo Horizonte: Del Rey, 2002.

SAMPAIO, José Adércio L. *Direito à Intimidade e à Vida Privada*. Belo Horizonte: Del Rey, 1997.

SCOTT, Paul F. Ouster clauses and national security: judicial review of the investigatory powers tribunal. *Public Law*, [S.I.], v. 2017, n. 3, p. 355-362, 2017.

SCOTT, Paul. F. Once More unto the Breach: R (Privacy International) v Investigatory Powers Tribunal**.** *Edinburgh Law Review*, Edinburgh, v. 24, n. 1, p. 103-109, 2020.

STONE, David. Saving America's Privacy Rights: Why Carpenter v. United States Was Wrongly Decided and Why Courts Should Be Promoting Legislative Reform Rather than Extending Existing Privacy Jurisprudence. *St. Mary's Law Journal*, San Antonio, v. 51, n. 4, p. 223-270, 2019.

SUBRAMANIAN, Nithya. The government has stopped even trying to justify mass surveillance as necessary for the public good**.** *ScroolIn*, [S.I.], 19 mar. 2020. Disponível em: https://scroll.in/article/956586/the-government-has-stopped-even-trying-to-justify-mass-surveillance-as-necessary-for-the-public-good. Acesso em: 25 mar. 2020.

TARROW, Sydney. *War, states, and contention:* A Comparative Historical Study. Ithaca: Cornell University Press, 2015.

UNIÃO EUROPEIA. European Commission for Democracy through Law. *Report on the Democratic Oversight of the Security Services (Venice Commission)*. Strasbourg, 02 de junho de 2007. Disponível em: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010. Acesso em: 11 mar. 2020.

WETZLING, Thorsten. *Germany's intelligence reform*: More surveillance, modest restraints and inefficient controls. Berlin: Stiftung Neue Verantwortung, 2017.

Recebido em 19 de agosto de 2020.
Aprovado em 17 de fevereiro de 2021.

Resumo: a sociedade digital criou os instrumentos para a vigilância massiva dos indivíduos pelo Estado, sob a retórica da securitização. O medo do terror ou do extermínio estaria a justificar esse novo papel estatal. Se as leis deixam lacunas normativas e semânticas de controle, a servirem mais para legitimar do que para limitar os órgãos de inteligência, o Judiciário parece ainda confuso em meio aos novos desafios e tentações de vigilância e o seu papel de proteção dos direitos fundamentais. O presente artigo analisa como o Judiciário respondeu a essa chamada de responsabilidade. Como metodologia procurou-se lançar um (primeiro) olhar sobre o problema e tentar responder se o Judiciário, como uma tradicional e requisitada garantia dos direitos, tem atendido às expectativas de prevenção e reparação. Avaliou-se o repertório de jurisprudência de alguns Estados, aqueles em que as questões já vieram à discussão judicial, seguindo-se, numa metodologia comparativa e indutiva, que se vale da revisão bibliográfica como ancoradouro da reflexão.
Palavras-chave: sociedade digital, Estado de vigilância, retórica de securitização, Judiciário.

Abstract: the digital society created the instruments for the mass surveillance of individuals by the State, under the rhetoric of securitization. Fear of terror or extermination justifis this new state role. If the laws leave normative and semantic control gaps, serving more to legitimize than to limit the intelligence agencies, the Judiciary still seems confused amid the new challenges and temptations of surveillance, and its role in protecting fundamental rights. This article analyzes how the Judiciary responded to this call for responsibility. As a methodology the article tried to take a (first) look at the problem and then to answer whether the Judiciary, as a traditional and requested guarantee of rights, has met expectations for prevention and repair. The repertoire of jurisprudence of some states was evaluated, those in which the issues have already come to judicial discussion, followed by a comparative and inductive methodology, which uses the bibliographic review as an anchor for reflection.
Keywords: digital society, surveillance State, securitization rhetoric, Judiciary.

Sugestão de citação: SAMPAIO, José Adércio Leite. As cortes e os desafios da era digital: a vigilância na jurisprudência comparada. *Revista Direito, Estado e Sociedade*, Ahead of print, 2021. DOI: https://doi.org/10.17808/des.0.1616.