A PROTEÇÃO DE DADOS PESSOAIS DURANTE CRISES DE SAÚDE: LIÇÕES DO COMBATE A COVID-19 NA COREIA DO SUL E O DESENVOLVIMENTO DE MECANISMOS DE GOVERNANÇA DE DADOS LEGÍTIMOS

Ana Paula Assis Buosi[1]

Andressa de Figueiredo Farias[2]

João Araújo Monteiro Neto[3]

Resumo: O artigo investiga, sob uma abordagem crítica, a operação dos mecanismos legais que regulam as práticas de tratamento de dados pessoais durante o desenvolvimento de políticas que visam combater a pandemia do COVID-19 na Coréia do Sul. O artigo investiga, utilizando uma abordagem de estudo de caso e uma estrutura teórica sócio-jurídica, como a falta de práticas de governança projetadas para supervisionar o uso de dados pessoais, particularmente dados de saúde durante a pandemia do COVID-19, aumentou significativamente os riscos de má utilização desses dados e a ocorrência de tratamentos de dados discriminatórios, danosos e ilegais. No curso dessa análise, o trabalho também busca esclarecer a relação entre a autodeterminação informacional e a estruturação de mecanismos de governança de dados mais confiáveis que sejam capazes de traduzir para sua funcionalidade a legitimidade decorrente da autodeterminação informacional. O artigo foi estruturado em três seções.

[1]Mestranda em Direito Constitucional pela Universidade de Fortaleza. Advogada.
[2]Mestranda em Direito Constitucional pela Universidade de Fortaleza. Advogada.
[3]PhD em Direito pela Universidade de Kent no Reino Unido. Mestre em Direito Constitucional pela Universidade de Fortaleza.Advogado. Professor do Centro de Ciências Jurídicas da Universidade de Fortaleza.

Inicialmente apresenta a relação entre autodeterminação informacional e proteção de dados, particularmente durante emergências de saúde. Em seguida, analisa o uso de dados pessoais para combater a Covid-19 na Coréia do Sul, país considerado referência no que tange o controle da letalidade e transmissão do coronavírus. Por fim, em sua última seção, busca apresentar um modelo de valores de governança oriundos do sistema de governança da Internet e algorítmica. Conclui-se que esses elementos devem orientar o desenvolvimento de uma governança de dados capaz de promover o uso mais seguro e equilibrado de dados pessoais durante crises de saúde.

Palavras-Chave: Dados Pessoais; Governança; FAT; Coreia do Sul; COVID-19

Abstract: The paper investigates under a critical approach the operation of legal provisions regulating data processing practices during the development of policies aiming to fight the COVID-19 pandemic in South Korea. It uses a case study approach and a socio-legal theoretical framework to investigate how the lack of governance practices designed to oversight the use of personal data, particularly health data, during the COVID-19 pandemic increased significantly the risk of discrimination, harm and unlawful practices. It also questions the relation between informational self-determination and the need for more reliable data governance approaches. Structured under three sections the paper presents the relation between informational self-determination and data protection, particularly during health emergencies. It, then, analyses the use of personal data to fight the Covid19 in South Korea in order to extract insights to propose, on its last section, the translation of values applied to Internet and algorithmic governance onto a novel governance approach able to promote a saver and balanced use of personal data during health crisis.

Keywords: Personal Data; Governance; FAT; South Korea; COVID-19

Sumário: Introdução. 1. Autodeterminação informacional e dados pessoais. 2. O uso dos dados pessoais em tempos de pandemia – o caso da Coreia do Sul. 3. A proteção de dados pessoais em crises de saúde por meio da governança – aplicando a abordagem multisetorial FATE. Conclusão. Referências.

INTRODUÇÃO

reflexão sobre os impactos das novas tecnologias na sociedade não é recente. Entretanto, vem sendo cada vez mais influenciada pela velocidade com que novas tecnologias são desenvolvidas e se espalham globalmente. Independentemente de sua natureza, seja biomédica, espacial ou de informação e comunicação, à medida em que as novas tecnologias se integram ao cotidiano social novos problemas se manifestam (SALEMA, 2018).

O surgimento da Internet e das redes móveis celulares gerou novos problemas, em especial afetos à privacidade dos dados pessoais. O surgimento do Big Data – grande massa de dados, inclusive pessoais, produzidos em escala global, dotados de grande volume, velocidade de aquisição e variedade (NAZARÉ, 2018) – e do Data Mining – processo de conhecimento e de extração de informação a partir dos dados – levou as preocupações relacionadas à privacidade para patamares antes inimagináveis. Do direito de ser deixado só, caminhou-se para a necessidade de discussões sobre o poder das aplicações poderem "*gogglar"* nossa alma. A possibilidade de obter correlações, padrões e associações a partir dos dados, transformando-os em informação, bem como os problemas decorrentes do uso de algoritmos para

a tomada de decisões também levam a possíveis problemas éticos e legais. Os desafios transitam desde a efetividade da autodeterminação informacional até o risco de decisões enviesadas e discriminatórias que afetem a privacidade e a personalidade dos titulares dos dados pessoais.

A privacidade é um valor importante que de acordo com RÖSSLER (2015) e SOLOVE (2011) dita de forma muito direta como proteger as esferas autônomas da vida e como exercer o controle sobre o corpo, as comunicações e também os dados pessoais. Apesar de seu estado conceitual de desordem e de todos os debates teóricos, o aumento das políticas de vigilância (SOLOVE, 2011;) e o surgimento do "cidadão conhecido" (IGO, 2014), a privacidade ainda é considerada pela maioria da literatura legal como uma das pedras angulares das sociedades democráticas (GAVINSON, 1980). No entanto, com o passar do tempo, incrementou a sua matriz de influência conceitual e legal transformando-se no que BEVIER (1995) denominou de "*chameleon-like word*", abarcando os debates sobre áreas como sexualidade, controle de natalidade e informações pessoais.

Apesar da maioria da literatura jurídica tradicional enquadrar a privacidade como um direito "promotor ou capacitador" de outros direitos (Canatacci, 2015), alguns acadêmicos observaram que a privacidade também pode ser percebida como um mecanismo que fornece às pessoas a possibilidade de controlar o acesso, o uso ou a divulgação de aspectos de sua vida privada a outras pessoas ou ao governo. Debruçando-se sobre essa abordagem, POSNER (1981) apontou, de forma análoga, que a privacidade permite às pessoas ocultar informações sobre assuntos ou matérias que elas entendem que possam ser utilizadas em sua desvantagem. Essa percepção levou CATE (1997, 29) a identificar a privacidade como uma "construção antissocial que conflita com outros valores importantes da sociedade, tais como a liberdade de expressão, a prevenção e punição de condutas criminosas, bem como o desenho e a operação de políticas

públicas mais eficientes, especialmente em domínios como os de crises de segurança ou saúde.

Nos cenários de risco, o uso de informações protegidas pelo direito à privacidade costuma ser considerado mais aceitável, especialmente se o uso for direcionado ao combate a crimes graves, ao terrorismo, desastres naturais ou crises de saúde ou sanitárias, como a causada pela COVID-19. Nesses contextos, o tratamento de dados pessoais pode ser crucial para operar políticas públicas eficientes. Ao mesmo tempo, o tratamento indevido dessa informação pode expor seus titulares a possíveis danos e discriminações com impactos significativos em suas vidas.

Tanto a legislação européia (GDPR) quanto a legislação brasileira sobre proteção de dados pessoais estabelecem mecanismos legais que autorizam o uso de dados pessoais, incluindo dados sensíveis, sem o consentimento de seus titulares, nos casos em que o processamento é necessário quando alcançar interesses coletivos, como a proteção da saúde pública. De fato, essa foi a posição estabelecida pelo Conselho Europeu de Proteção de Dados (EDPB) em sua "Declaração sobre o tratamento de dados pessoais no contexto do surto de COVID-19", publicado em 19 de março de 2020, e no Civil Protection Portaria 630 do Departamento de Proteção Civil da Itália, o Aviso de Informações das Agências Régionales de Santé (ARS) da França. Limitar a proteção de dados para alcançar um interesse público é uma prática de limitação de privacidade que não é nova e pode ser observada na Lei Federal de Proteção de Dados da Alemanha e na Lei Brasileira de Proteção de Dados.

No entanto, nem as regras européias nem a lei brasileira tratam da implementação ou operação de um modelo de governança capaz de supervisionar essas operações de tratamento, nem tão pouco acompanhar o nível de conformidade dessas atividades às regras de proteção à privacidade dos titulares dos dados. Este artigo investiga como as práticas de governança podem contribuir para promover a privacidade durante o tratamento de

dados pessoais em emergências ou crises. Ele questiona como a governança pode funcionar como um elemento de representação da autodeterminação informacional nos processos de utilização de dados pessoais em tempos de crise, e também interroga quais valores devem orientar essas práticas de governança para que a governança de dados pessoais possa incorporar em sua operação a legitimidade decorrente da autodeterminação informacional?

Tomando emprestado idéias de estudos socio-legais, este artigo se desvia do caminho tradicional da pesquisa jurídica para conectar diferentes conjuntos de literaturas acadêmicas, como estudos sobre a governança da Internet, privacidade, proteção de dados, governança global e estudos de regulamentação para analisar, sob uma abordagem crítica a operação de disposições legais que regulam as práticas de tratamento de dados pessoais durante o desenvolvimento de políticas destinadas a combater a pandemia de COVID-19 na Coreia do Sul.

O artigo apresenta a relação entre autodeterminação informacional e proteção de dados, particularmente durante emergências de saúde. Em seguida, analisa o uso de dados pessoais para combater o Covid19 na Coréia do Sul e em sua última seção, busca apresentar um modelo de valores de governança oriundos do sistema de governança da Internet e algorítmica como elementos que devem orientar o desenvolvimento de uma governança de dados capaz de promover um uso mais seguro e equilibrado de dados pessoais durante crises de saúde.

1. AUTODETERMINAÇÃO INFORMACIONAL E DADOS PESSOAIS

O nascimento da ideia de privacidade está relacionado ao privilégio conferido à classe burguesa que, em virtude das transformações socioeconômicas resultantes da Revolução Industrial, tinha a possibilidade de viver distante da comunidade, afastando-se da vida e das atividades em comum (RODOTÀ, 2008,

p. 26-27). Assim, em um primeiro momento, o direito à privacidade, além de estar associado à tutela da propriedade, foi pensado como "o direito de ser deixado só" (WARREN; BRANDEIS, 1890, p. 193), havendo uma preocupação contra qualquer invasão indesejada que representasse um risco para a privacidade do indivíduo (WARREN; BRANDEIS, 1890, p. 206).

Posteriormente, a mudança das possibilidades e das modalidades de tratamento das informações aumentou os riscos para a privacidade (RODOTÀ, 2008, p. 43), de modo que, em 1983, o Tribunal Alemão, em decisão relativa à Lei do Censo, contribuiu para uma nova percepção de privacidade. Na época, uma lei acerca do censo demográfico que seria realizado despertou o debate social em virtude do risco que poderia trazer à proteção de dados dos cidadãos, tendo em vista que as informações deveriam ser coletadas, sob a supervisão das autoridades locais, por 600.000 (seiscentos mil) colecionadores. Existia o receio de que os dados pudessem ser vinculados aos indivíduos, pois havia mais de 160 (cento e sessenta) perguntas a serem respondidas no questionário. Além disso, os dados não eram usados apenas para fins estatísticos, mas também para comparação e correção de residentes registradores (HORNUNG; SCHNABEL, 2009, p. 85).

Na decisão, o Tribunal Alemão considerou a lei inconstitucional, mas isso não significou a não realização do censo demográfico. Depois, outra lei foi editada, e o censo ocorreu em 1987 (HORNUNG; SCHNABEL, 2009, p. 85). Na ocasião, o Tribunal desenvolveu o conceito de autodeterminação informacional, que representa "[...] o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" (RODOTÀ, 2008, p. 110), de modo que a privacidade, como conceito dinâmico que é, passou a não mais ser considerada apenas sob uma perspectiva negativa ("direito de ser deixado só"), mas também sob uma dimensão positiva, passando a demandar uma atuação positiva no sentido de proteger garantias atinentes à circulação de dados pessoais

(BODIN DE MORAES; QUEIROZ, 2019).

Em relação à proteção de dados, é possível perceber que se passou de uma situação pessoa-informação-sigilo para uma de pessoa-informação-circulação-controle, de modo que os dados coletados não são mais mantidos em segredo e sim postos em circulação. Sendo assim deve o cidadão desempenhar um papel ativo no manuseio de suas informações. Isso ocorre porque, na sociedade atual, em virtude do uso de computadores no tratamento dos dados pessoais, não é mais possível que o indivíduo seja considerado mero fornecedor de informações, tendo em vista que tais dados são responsáveis por produzir novos centros de poder ou legitimar os pré-existentes. Dessa forma, torna-se evidente a necessidade do cidadão exercer qualquer tipo de controle, de modo que haja o equilíbrio dessa nova distribuição de poder (RODOTÀ, 2008).

Contrariamente ao que se observa hoje, nem sempre foi possível perceber, nos ordenamentos jurídicos, a presença de instrumentos regulatórios que tratassem especificamente da proteção de dados pessoais. Ao longo das três gerações de leis que abordam essa temática, houve a mudança de um "[...] enfoque mais técnico e restrito até a abertura a técnicas mais específicas, aplicáveis às tecnologias adotadas para o tratamento de dados" (DONEDA, 2014, p. 142). Inicialmente, os instrumentos regulatórios enfatizavam a autorização que deveria ser concedida para os centros de processamentos de dados, que concentrariam a coleta e a gestão dos dados pessoais. Depois, na segunda geração de leis, foi possível observar uma maior preocupação com a privacidade e a proteção de dados pessoais do cidadão, que deveria exercê-los sob a forma de liberdade negativa, período do qual a autodeterminação informacional foi resultado (DONEDA, 2014, p. 142). Na terceira geração de leis, o enfoque passou a ser a garantia ao cidadão para exercer, de maneira efetiva, essa liberdade negativa (DONEDA, 2014, p. 143).

Um dos primeiros instrumentos regulatórios no que diz

respeito à proteção de dados foram as Linhas-Guias da OCDE, de 1980, além de ter sido um dos mais influentes em relação à temática, servindo de substrato para as demais legislações que surgiram depois. Importante considerar que nesse documento havia a preocupação de atingir dois objetivos concomitantes, quais sejam o de proteção da privacidade e do fluxo de transfronteiriço de dados pessoais (MENDES; BIONI, 2019, p. 160). Posteriormente, é possível destacar o Regulamento Europeu de Proteção de Dados Pessoais (RGPD), aplicável a partir de 25 de maio de 2018, que foi o resultado de uma necessidade de maior uniformização da proteção de dados na Europa. Importante característica desse instrumento regulatório, além dos princípios básicos que regem a proteção de dados e do direito ao esquecimento, é a necessariedade de que só pode haver o tratamento de dados se existir base legal que o ampare (MENDES; BIONI, 2019, p. 170). Isso ocorre porque, hoje, mesmo as informações mais irrelevantes, se associadas entre si ou a outras, resultam em dados importantes acerca do cidadão. Nesse mesmo sentido, a Lei Geral de Proteção de Dados (LGPD) preocupou-se em adotar um conceito expansionista de dado pessoal (BIONI, 2020). Dessa forma, dado pessoal é caracterizado como a informação relacionada a uma pessoa identificada ou identificável, conforme o disposto pelo art. 5º, inciso I.

A LGPD cuidou ainda de diferenciar dado pessoal de dados sensíveis, art. 5º, inciso II, elencando o consentimento como a base legal apta ao tratamento dessas informações específicas. No entanto, é possível ainda que esses mesmos dados possam ser tratados independente da referida base legal, como disciplina o art. 11, inciso II, alíneas "b", "e" e "f", nos casos de execução de políticas públicas, proteção à vida e tutela da saúde em procedimentos realizados por profissionais da saúde. Com o advento da pandemia causada pelo novo coronavírus, essas especificações legais somaram-se ao conteúdo disciplinado pela Lei de nº 13.979/2020 para fins de contigenciamento da rápida

disseminação da enfermidade. Assim, conforme o art. 6º e seus parágrafos, o compartilhamento de dados pessoais poderia ser realizado entre as entidades da administração pública, em todas as suas esferas administrativas, e as pessoas jurídicas de direito privado com o propósito de identificar infectados pela doença e promoção de políticas públicas.

A discussão sobre a privacidade de dados pessoais tornou-se necessária no momento de crise sanitária. Recente decisão proferida pelo Supremo Tribunal de Federal (STF), em sede de Medida Cautelar, argumentou-se sobre privacidade, autodeterminação e o compartilhamento de dados dos cidadãos brasileiros, semelhante ao ocorrido no Tribunal Alemão em 1983. No cenário pandêmico, foi editada a Medida Provisória (MP) de nº 954/2020 determinando que as empresas de telefonia fixa e móvel compartilhassem os dados de todos os seus usuários com o Instituto de Brasileiro de Geografia e Estatística (IBGE). As informações seriam disponibilizadas em meio eletrônico abrangendo nome, número de telefone e endereços de pessoas físicas e jurídicas. Antes que a referida MP vigorasse, partidos políticos e o Conselho Federal da Ordem dos Advogados do Brasil propuseram as Ações Direitas de Inconstitucionalidade de nº 6387, 6388, 6389, 6390 e 6393 com o desiderato de suspender os seus efeitos. O enfrentamento da questão ficou a cargo do julgamento da Ministra Rosa Weber referendado posteriormente pelo voto de dez ministros. O voto divergente que indeferiu as liminares argumentou ser competência do Congresso Nacional a apreciação dos requisitos para normatização da matéria.

No bojo do voto da Ministra Relatora, o direito à proteção de dados ganhou contornos constitucionais protetivos de direito fundamental. Ainda que o referido direito não esteja expressamente protegido constitucionalmente, da interpretação dos dispositivos constitucionais art. 5º, incisos X e XII é possível inferir que a MP ofende a existência que o direito à privacidade assegura à tutela do livre desenvolvimento da personalidade.

Apesar de o ato normativo especificar quais dados seriam coletados, não houve uma preocupação do legislador em delimitar "[...] o objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados" (BRASIL, 2020, p. 9). Mesmo que a intenção do legislador fosse a elaboração de políticas públicas para o enfrentamento da pandemia, não se informou quais seriam os tipos de pesquisa realizados com os dados pessoais dos cidadãos e o motivo específico para a ocorrência do compartilhamento, uma vez que o Censo Demográfico do ano de 2021 realizado pelo IBGE foi adiado em decorrência do coronavírus.

Tais circunstâncias nos moldes delimitados pela MP colidem com as boas práticas e os princípios preconizados pela LGPD. Ainda que esteja pendente a sua vigência, a LGPD se coloca no cenário de proteção de dados como norteador de práticas e condutas já em vigor. Os efeitos irradiantes do diploma legal podem ser ilustrados ao longo da presente decisão. Tanto a privacidade quanto a autodeterminação informativa foram elencadas como fundamentos disciplinadores da proteção de dados, art. 2º, incisos I e II. Sabe-se também que os princípios estipulados pelo art. 6º da referida lei legitimam as atividades de tratamento de dados pessoais. Observa-se que a finalidade, inciso I, não foi delineada especificando como os dados seriam utilizados. A necessidade, inciso III, não foi especificada limitando o tratamento das informações ao mínimo necessário para que o propósito da ação governamental fosse adequado, inciso II. Ademais, não restou transparente, inciso VI, como seria garantido ao indivíduo o controle sobre as suas informações. Tampouco estabeleceu-se medidas técnicas e administrativas, inciso VII, que salvaguardassem os dados pessoais. Finalmente, não se demonstrou a adoção de medidas de responsabilização e prestação de contas, inciso X, comprovadoras do cumprimento e da eficácia das normas protetivas de dados pessoais.

Demais a mais, para além da observação dos princípios anteriores, é necessário verificar qual base legal, art. 7º e seus incisos, é a mais adequada para que o tratamento do dado seja realizado. *In casu*, o tratamento e compartilhamento de informações pela administração à execução de políticas públicas, inciso III, deverá observar condições específicas. Nesse sentido, a obrigação de prestar informações claras sobre as práticas executadas pela autoridade deverá estar discriminada em veículos de informação de fácil acesso à população, art. 23, inciso I. Além disso, há a necessidade de se indicar o encarregado do tratamento das informações, art. 23, inciso III. Não o bastante, os dados necessitam ser mantidos em formato interoperável e estruturado para que seu uso seja compartilhado com finalidade de execução de políticas públicas, arts. 25 e 26. Apesar da urgência do panorama delimitado pela crise sanitária, a maioria dos ministros entendeu que os efeitos decorrentes da MP na coleta dos dados da população implicariam no "(...) atropelo de garantias fundamentais consagradas na Constituição" (BRASIL, 2020, p. 12).

Assim, é possível perceber uma perspectiva protetiva da privacidade presente nos instrumentos regulatórios pertencentes às diferentes gerações de leis que tratam da temática da proteção de dados. Na realidade, esse entendimento já estava presente desde o início da preocupação com o conceito de privacidade, que, inicialmente, foi definido como "o direito de ser deixado só". Tal possibilidade continuou presente com a elaboração da ideia de autodeterminação informativa pelo Tribunal Constitucional Alemão, tendo em vista que, com a preocupação acerca do controle que o cidadão exerceria sobre a circulação de informações a seu respeito, fica evidente o fato de que "[...] cada registro que se revela como pessoal é merecedor de proteção" (MENDES, 2018, p. 191).

Observando o uso de dados pessoais no combate à pandemia, o European Data Protection Board (EDPB) em seu "*Statement on the processing of personal data in the context of the*

COVID-19 outbreak" estabeleceu orientações para o uso de dados pessoais no enfrentamento da pandemia. Neste contexto limitador de liberdades, dentre as diretrizes apontadas destacam-se a necessidade de se respeitar: os princípios da proporcionalidade, finalidade e confidencialidade; as bases legais de tratamento; e os direitos do titular dos dados. O documento expressa ainda a necessidade de adotar técnicas menos prejudiciais à privacidade desses titulares. "Mesmo possuindo mecanismos protetivos vigentes e uma estrutura mínima de governança, vários países europeus enfrentam questionamentos sobre o escopo, a licitude e fiscalização do uso dos dados pessoais" (BUOSI; XAVIER JÚNIOR; MONTEIRO NETO, 2020, p. 17). Uma das questões mais relevantes decorrentes desses processos de avaliação repousa justamente na ausência de estruturas e parâmetros de governança desses dados.

Nesse cenário, compreender os elementos estruturais e orientadores da governança de dados pessoais em tempos de crise, em especial a vivenciada atualmente, demonstra-se relevante o desenvolvimento de um sistema de regulamentação do uso de dados que seja capaz de balancear o manuseio das informações e dos direitos dos titulares. Buscando delimitar a problemática, pondera-se a respeito dos elementos capazes de sustentar o desenvolvimento de mecanismos de governança aplicados à matéria. Tendo em vista os mecanismos de controle implementados pela Coreia do Sul para fins de contigenciamento do surto pandêmico, bem como sua discussão constitucional sobreo alcance da privacidade e da autodeterminação informacional, foram avaliados seus movimentos regulatórios envolvendo o uso de dados pessoais no combate à crise.

2. O USO DOS DADOS PESSOAIS EM TEMPOS DE PANDEMIA - O CASO DA COREIA DO SUL

A pandemia exteriorizou como cada país lidou com a

conjuntura de crise sanitária. Em momentos de tensão social, os indivíduos tendem a flexibilizar direitos e garantias conquistados para que a situação se estabilize, e isso, muitas vezes, significa um maior compartilhamento de informações acerca dos cidadãos. Em contrapartida, a perspectiva protetiva da privacidade e a autodeterminação informacional acabam por ser flexibilizadas, o que ocorre com o auxílio do próprio cidadão, por meio do fornecimento de dados pessoais para a Administração Pública. O problema é que, considerando a disparidade de poder existente, geralmente, o indivíduo não "[...] percebe o sentido que a coleta de informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados [...]" (RODOTÀ, 2008, p. 37). Para tanto, a legislação europeia (RGPD) e a LGPD autorizam situações excepcionais dessa natureza, desde que o procedimento seja proporcional, esteja amparado por salvaguardas e contemple finalidades direcionadas (ALMEIDA *et al.*, 2020).

Essas flexibilizações relativas à privacidade não são medidas exclusivas adotadas por países ocidentais. Notícias veiculadas sobre o controle da pandemia indicam que países do leste asiático encontraram nas soluções digitais medidas eficazes de combate à doença. De acordo com a análise no site da Universidade Johns Hopkins, 2020, o contingenciamento da enfermidade não está associado a um fenômeno estritamente territorial. Apesar disso, identifica-se que alguns países do leste asiático como Coreia do Sul, Singapura, Taiwan, China e Japão adotaram estratégias digitais bem sucedidas de rastreamento de pessoas infectadas, implementação de quarentenas digitais e manuseio de suprimentos para o controle da COVID-19. Conforme o *dashboard* disponibilizado pela instituição superior de ensino, no dia 29 de junho de 2020, a Coreia contabilizava 14.251 casos confirmados e 300 mortes, enquanto Singapura tinha 51.531 casos e 27 falecimentos. Por sua vez, Taiwan apresentou 467 confirmações e 7 mortes, China com 87.108 casos e 4.658 mortes e Japão

com 33.351 casos e 1.001 mortes. Instigam os números apresentados quando comparados com Israel, 66.805 casos e 491 mortes, e Alemanha, 208.160 diagnósticos e 9.135 mortes, países ocidentais exemplares no controle da doença.

Uma outra hipótese que justifica a eficiência das medidas adotadas durante o surto de COVID-19 pelo leste asiático remonta ao aprendizado com as experiências anteriores semelhantes. No século XXI, os orientais presenciaram epidemias como a Síndrome Respiratória Aguda Grave (SARS), 2003, (WANG *et al.*, 2020) e a Síndrome Respiratória do Médio Oriente (MERS), 2015. Tais surtos propiciaram mudanças nos sistemas de saúde para fins de monitoramento e resposta a eventos dessa natureza. Especificamente a MERS afetou sobremaneira a Coreia do Sul. Há época, o diagnóstico de 166 pessoas infectadas impactou a vida de uma população de 50 milhões de habitantes. Além do setor de saúde, os efeitos da epidemia alcançaram diversas áreas como o turismo e o ensino, reduzindo, inclusive, o produto interno bruto anual. Para tanto, autoridades governamentais determinaram-se a estudar medidas efetivas que pudessem reduzir o risco de incidentes semelhantes no futuro (COWLING *et al.*, 2015).

A experiência vivenciada pela MERS fez com que o país repensasse os limites protetivos que a sua legislação oferecia à privacidade no que tange o consentimento dos seus cidadãos. Tal fato é ilustrado pelas alterações realizadas na Lei de Controle e Prevenção de Doenças Contagiosas (CDPCA) (PARK; CHOI; KO, 2020). A mudança no comportamento da legislação também foi impulsionada pelo fato da Coreia ser uma das grandes potências mundiais em tecnologia da informação com um intenso fluxo de dados. Ambos os cenários oportunizaram com que medidas governamentais fossem implementadas para que houvesse mudanças na perspectiva legal. Salienta-se ainda que um interesse maior da população por questões relativas à privacidade foi relevante para que existissem mudanças no cenário de

leis e regulamentos. (KO *et al.*, 2017).

Identificada como uma das leis de privacidade de dados com requisitos mais rigorosos do mundo, a Lei de Proteção de Informações Pessoais (PIPA), promulgada no ano de 2011, possui diretrizes gerais e traz conceitos importantes para a regulação de dados, como informações pessoais e consentimento. Ressalte-se que anterior a sua existência, diversos documentos legais setoriais existiam como forma de regulamentar o tratamento de dados pessoais. O descumprimento legal dos requisitos rigorosos a respeito do processamento das informações estava sujeito a significativas penalidades civis e criminais. Ainda que o seu caráter fosse protetivo e informativo para fins de conscientização social, a PIPA não inibiu que violações legais aos dados dos cidadãos ocorressem. No ano de 2014, um grande vazamento de informações sobre cartões de crédito de diversos usuários ocasionou uma grande comoção nacional (KO *et al.*, 2017).

Peculiaridades sobre o tratamento de dados pessoais sensíveis e a importância do direito à autodeterminação são observados também no país oriental. Os processadores de dados pessoais são proibidos, *a priori*, de manusear informações relativas à saúde e vida sexual, às opiniões políticas e ideologias, a convicções religiosas e filiação a sindicato. Excepcionalmente esses profissionais estarão autorizados a tratar as referidas informações se houver uma prerrogativa legal que os autorize ou ainda que seja obtido um consentimento específico para o tratamento. O Tribunal Constitucional Coreano, à semelhança do brasileiro, ressaltou a autodeterminação como o aspecto mais relevante sobre proteção de dados pessoais. O caso paradigmático fundamentou-se na argumentação de que a coleta e utilização de impressões digitais dos cidadãos tratar-se-ia de uma restrição à autodeterminação informacional. A decisão é anterior à promulgação da PIPA, porém foi a primeira vez em que ocorreu a discussão sobre o fato de o direito à privacidade estar compreendido dentro do rol de direitos fundamentais constitucionais. É

exatamente nessas circunstâncias protetivas que o consentimento e o poder do cidadão de influenciar no conteúdo de suas informações foi delineado na elaboração da PIPA (KO *et al.*, 2017).

Como já mencionado, ações relativas ao enfrentamento da pandemia do coronavírus pela Coreia alcançaram destaque mundial. Além de ser um dos países mais próximos da China, as medidas para contenção do surto foram rápidas, decisivas e não houve a necessidade de que as fronteiras geográficas fossem fechadas. O empenho em testar o maior número de cidadãos, a adoção de medidas de vigilância por meio de aplicativos, a colaboração entre setores públicos e privados (Johns Hopkins University, 2020), a agilidade para o enfrentamento da crise sanitária e o espírito de colaboração pactuados entre os sul-coreanos fizeram com que o país tivesse um resultado bem sucedido, em termos de saúde, e surpreendesse as demais nações (MOON, 2020).

Atinente às respostas legais e políticas, a República da Coreia tratou em desenvolver um aplicativo personalizado para que as pessoas infectadas pela COVID-19 e em quarentena relatassem o seu estado de saúde com regularidade. Além disso, foram utilizados dados agregados relativos à localização dos indivíduos para que se identificassem possíveis focos de contaminação nas comunidades. A tutela relativa à privacidade e ao tratamento diferenciado dos dados sensíveis de saúde não foram preocupações do governo e nem da sociedade porque as modificações legislativas realizadas pela CDPCA sobrepõem-se tanto à PIPA quanto a outras leis setoriais que tratam de privacidade. Dessa forma, foi possível a coleta de dados de localização, registros de imigração, imagens de televisão em circuito fechado, informações sobre circuitos de trânsito, dados relativos à identificação pessoal e prescrição e registros médicos. O fluxo desses registros transitou entre entidades governamentais, sistemas nacionais de seguros de saúde e "outros sistemas". Essas práticas

sistematizadas oportunizaram aos Centros de Controle e Prevenção de Doenças da Coreia (KCDC) desenvolverem o Sistema de Suporte de Vigilância Epidemiológica COVID-19, com base nas práticas de *contact tracing*. (PARK; CHOI; KO, 2020).

O *contact tracing* é uma prática habitual realizada pelos sistemas de vigilância sanitária para o controle de doenças contagiosas como por exemplo tuberculose, ebola, coronavírus, dentre outras. Tratam-se de medidas eficientes adotadas que visam interromper a cadeia de transmissão da enfermidade. Para tanto, é necessário que se identifique de forma rápida os indivíduos suspeitos de contaminação ou confirmados. Também é importante a adoção de medidas de prevenção e controle como, por exemplo, o isolamento e a quarentena. A prática desenvolve-se no sentido de tanto informar os indivíduos sobre os cuidados necessários para a recuperação quanto manter as autoridades sanitárias notificadas a respeito do estado de saúde da população monitorada. O diferenciador do momento é que os mecanismos de controle são realizados com o auxílio de aplicativos digitais. A comunicação entre os envolvidos ocorre por meio de "[...] lembretes comuns (que) incluem mensagens de texto, mensagem em aplicativos de mensagens ou chamadas telefônicas automatizadas." (ANVISA, 2020, p. 12).

No caso da Coreia, uma estrutura de governança já existente composta pelos KCDC alinharam-se desde o início da pandemia. Todos os pacientes que relataram sintomas semelhantes aos desenvolvidos em decorrência da COVID-19 realizaram o teste PCR e as informações foram compartilhadas com os KCDC. O primeiro caso confirmado pelo laboratório foi colocado em um *cluster*. Os contatos de alto risco foram testados com frequência. Grupos que não possuíam risco considerável só eram testados quando desenvolviam alguma manifestação sintomática. Finalmente, os contatos assintomáticos, mas com grande probabilidade de desenvolver a doença se "auto-colocaram em quarentena" durante 14 dias e eram monitorados por agentes de

saúde duas vezes ao dia. Uma das conclusões que o *Center for Disease Control and Prevention* (CDC) concluiu da análise de 59.073 contatos de 5.706 pacientes, entre os meses de janeiro a março, concluiu sobre a importância do rastreamento de contatos para a prevenção de futuras doenças semelhantes (PARK *et al.*, 2020).

Apesar dos benefícios originários dos controles de vigilância epidemiológica, o excesso de informação demonstrou falhas nos sistemas de informações. Houve a exposição de informações pessoais de alguns usuários. Além disso, os mecanismos de anonimização e pseudoanonimização não foram suficientes para que os indivíduos não fossem identificados, levando alguns a experienciar circunstâncias de desprezo público. Problemas dessa ordem também afetaram pessoas jurídicas. Centros comerciais e restaurantes em que indivíduos infectados transitaram foram expostos, o que acabou por ocasionar prejuízos econômicos. O detalhamento das informações desnecessariamente divulgadas fez com que a Comissão Nacional de Direitos Humanos da Coreia emitisse recomendações com o propósito de resguardar a privacidade dos cidadãos (PARK; CHOI; KO, 2020). A experiência mostra a necessidade de que mecanismos de tecnologia da informação devem se adequar com a finalidade de evitar desastres dessa natureza e que podem ter repercussões tão dolorosas ou duradoura quanto os próprios efeitos da pandemia. Tem-se claro que os mecanismos aplicados ao *contact tracing* para fins de monitoramento não devem se tornar instrumentos de vigilância. O foco da prática é o controle da enfermidade e não das pessoas.

O compartilhamento de dados e informações entre pessoas, instituições e organizações deve ser proposto por meio de uma governança responsável. Há que existir transparência e empoderamento dos usuários, independentemente da existência de um cenário de crise. Dessa forma, "Modelos de governança de dados mais justos, responsáveis e sustentáveis, que protejam e

defendam princípios éticos e regulatórios, ampliam a confiança dos indivíduos e da sociedade [...]" (ALMEIDA *et al.*, 2020, p. 2491). Mesmo em situações excepcionais, é necessário o delineamento de uma metodologia propositiva para que os fins sejam legítimos.

Analisando esse contexto controverso, é importante identificar quais são os métodos usados pelas diferentes autoridades governamentais para monitorar e processar dados confidenciais, considerando o contexto de crise sanitária causada pela COVID-19. A compreensão desses aspectos pode ser crucial para o desenvolvimento de políticas e modelos de governança capazes de proteger os titulares de dados em uma nova crise de saúde, minimizando, dessa forma, possíveis efeitos nocivos das atividades de monitoramento de informações.

Associado a isso, a combinação do multissetorialismo com indicações das práticas de governança FATE (Fairness, Accountability, Transparency, Expertise) permite a estruturação de um mecanismo capaz de garantir a usabilidade dos dados e, simultaneamente, garantir a adoção de práticas capazes de respeitar os direitos dos titulares dos dados e a operacionalidade de medidas para minimizar os riscos do compartilhamento de atividades.

3. A PROTEÇÃO DE DADOS PESSOAIS EM CRISES DE SAÚDE POR MEIO DA GOVERNANÇA - APLICANDO A ABORDAGEM MULTISETORIAL FATE

A decisão inovadora do Tribunal Constitucional Federal da Alemanha, declarando a Lei do Censo Demográfico parcialmente inconstitucional, instituiu o direito da autodeterminação informacional (HORNUNG; SCHNABEL, 2009) e estabeleceu os fundamentos da maioria dos instrumentos legais que tratam da temática da proteção de dados. Compreendido como o direito de exercer o controle e a proteção sobre os próprios dados

pessoais contra o tratamento indesejado ou ilegal praticado por terceiros (RODOTÀ, 2008), a noção de autodeterminação informacional também engloba aspectos que devem ser observados durante o desenvolvimento de estruturas de governança aplicadas ao tratamento de dados pessoais, particularmente aqueles relacionados a contextos extraordinários como a pandemia causada pela COVID-19.

A Convenção 108 do Conselho da Europa e as Diretrizes de Recomendação da OCDE sobre a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais (1980) incorporam um conjunto de princípios para proteger o direito à autodeterminação informativa. Essas recomendações devem também ser utilizadas para orientar o desenvolvimento de estruturas de governança capazes de instrumentalizar a proteção em dos dados dos titulares, inclusive em operações controversas como as decorrentes de situações de emergência. Princípios como a limitação de objetivos, segurança e transparência são elementos-chave que orientam o exercício do direito de autodeterminação informacional.

Um sistema de governança, estruturado sob esse conjunto de princípios-padrão, pode traduzir, em suas atividades, a perspectiva protetora do direito à autodeterminação informacional e minimizar riscos e danos ao titular dos dados. Para isso, é necessário o envolvimento de todos os atores interessados no processamento de dados, trabalhando sob uma lógica multissetorial a partir de uma abordagem alinhada aos padrões FATE (Fairness, Accountability Transparencya and Expertise) que normalmente são utilizados nos processos de governança técnica da criação de artefatos computacionais como algoritmos.

O primeiro elemento, o multissetorialismo, remonta a alguns trabalhos exploratórios de governança econômica e desenvolvimento sustentável publicados na década de 1990 e no início dos anos 2000. Embora as práticas multissetoriais possam ser atribuídas a outros regimes de governança internacional no

âmbito dos direitos humanos, da segurança internacional (LA CHAPELE, 2007) e da proteção ambiental (HEMMATI, 2002), elas surgem a partir de uma abordagem dominante alinhada a um conjunto complexo de interesses, agendas e implicações que envolvem a crescente dependência de tecnologia, particularmente no regime da governança e regulação da Internet (CARR, 2015, p. 641), tendo como principais valores:

> - Openness, Transparency and Accessibility: The processes and discussions need to be open to participation of all actors interested, it also requisite to have clear and public engaging rules that need to be accessible to all involved;
> - Credibility and Accountability: The actors engaged on the decision-making process should have been recognized by their credibility and knowledge-based leadership, and must be responsible and accountable to the communities involved in the policy-shaping process;
> - Consensus-based: need to build a decision-making process grounded on process and practices that enable consensus to develop among those engaged in the decision-making phase (WAZ; WEISER, 2013).

O segundo elemento desse modelo de governança responsável de dados pessoais tem sua inspiração no corpo de trabalho desenvolvido no campo de aprendizado de máquina e governança algorítmica, organizado na sigla FAT (Fairness, Accountability, Transparency). WACHTER. et al. (2019, 59) observa que "os conceitos fundamentais da ciência da computação - como abstração e design modular - são usados para definir noções de justiça e discriminação, produzir algoritmos de aprendizado que reconhecem a justiça e intervir em diferentes estágios do processo. um pipeline de tomada de decisão para produzir resultados "justos"". Embora seja um conceito muito nebuloso e

de a ciência da computação lutar para estabelecer métricas confiáveis do que normalmente o sistema legal conceitua sob uma estrutura contextual (WACHTER; MITTELSTADT; RUSSELL, 2020), a tradução de uma perspectiva geral de fainess para uma estrutura de governança de dados pessoais pode ser observada como uma necessidade de as atividades de tratamento não estabelecerem resultados discriminatórios e legais (SELBST *et al.*, 2019).

Dentro das dimensões delineadas pelo FAT encontram-se os elementos responsabilidade (accountability) e transparência (transparency), uma vez que "[...] prestar contas é concordar em sujeitar-se a relações de escrutínio externo que podem ter consequências [...]" (BLACK, 2008, p.150). Essa relação dialética baseada na interdependência entre quem presta contas e quem recebe, é caracterizada principalmente pela possibilidade de as atividades de elaboração de políticas serem avaliadas externamente e, nos casos de irregularidades, os responsáveis estarem sujeitos a sanções. Esse processo, conforme indicado por SCHOLTE (2011, p. 17) e TAKE (2012a, p. 503), baseia-se em três fatores: a) a existência de instrumentos e mecanismos de coordenação e controle do processo de tomada de decisão; b) instrumentos para supervisionar e avaliar como as regras, protocolos e padrões são implementados; e c) divulgação de informações sobre as atividades de formulação de políticas, que devem ser seguidas pelo tomador de decisões, especialmente no que tange a explicar e justificar suas decisões (BOVENS, 2007).

Um elemento importante que apoia a legitimidade da responsabilidade dos formuladores de políticas (CHAN; PATTBERG, 2008) é a capacidade desses atores de compartilhar informações contendo os elementos que sustentam suas decisões e ações. A transparência é um elemento essencial e autônomo interconectado à prestação de contas. Um processo de elaboração de políticas aberto e transparente constitui um elemento importante para apoiar a legitimidade da governança,

particularmente em acordos que abrangem atores não estatais (ELMS; PHILLIPS, 2009), uma vez que permite que as partes interessadas tenham acesso a informações críticas (BLACK, 2008) sobre as decisões tomadas, avalie a adequação da decisão (BEMSTEIN; CASHORE, 2007) e seja capaz de responsabilizar os tomadores de decisão inadequadas (MENA; PALAZZO, 2012).

Quando estruturas ou processos de governança têm um nível mais alto de transparência e disponibilizam ao público e a todos os atores interessados, acesso aos motivos que sustentaram suas decisões em condições oportunas e de baixo custo (KEOHANE, 2011, BUCHANAN; KEOHANE, 2006; GUPTA, 2008), tem-se um processo de prestação de contas mais efetivo e capaz de responsabilizar àqueles que agiram de forma desviada: somente as partes interessadas plenamente informadas podem compreender, monitorar e questionar o processo de formulação de políticas (TAKE, 2012a, p. 502; HAUFLER, 2006).

O último elemento, conhecimento e capacidade técnica (Expertise), captura o papel desempenhado pelo conhecimento dos participantes nos processos de formulação de políticas. Os formuladores de políticas devem refletir em suas decisões "o estado da arte do conhecimento técnico-científico" (TAKE, 2012a, p. 503). Espera-se que sistemas de governança eficientes e legítimos fundamentem suas políticas e instrumentos regulatórios nos processos de elaboração de políticas com base em informações precisas, descobertas científicas, conhecimento técnico e conhecimento externo desenvolvidos e compartilhados pelas partes interessadas. Uma característica essencial dos processos de elaboração de políticas legítimos e eficientes é a capacidade de usar o conhecimento para adaptar soluções a problemas complexos. A maneira como os formuladores de políticas atraem, usam e traduzem conhecimentos em resultados de políticas tangíveis é um elemento central que informa e diferencia os processos de formulação de políticas modernos e eficientes.

Com base nos argumentos apresentados acima, esse artigo sugere que, em circunstâncias excepcionais como a resultante da pandemia causada pela COVID-19, a abordagem mais adequada para proteger as esferas de informações pessoais, não se fundam na utilização de uma narrativa legal restritivista que mantenha os dados inacessíveis.

Enquanto algumas posturas indicam que um "certo nível inacessibilidade seja um dos fatores mais importantes para a operação do direito à privacidade" (ALLEN, 1988), Sustenta-se que, excepcionalmente, o mais adequado para proteger as esferas informacionais pessoais seria a pratica de *governability* e legitimidade regulatória (BLACK, 2008). As práticas, estruturadas em um mecanismo multisetorial de governança FATE (Fair, Accountable, Transparent and Expertise-based) possibilitam o desenvolvimento de um *framework* apto a exercer a governança em processos futuros de tratamento de dados pessoais, uma vez que uma estrutura baseada nesses valores fornece uma orientação mais equilibrada e protetora para as atividades de tratamento de dados pessoais.

CONCLUSÃO

Esse artigo utilizou referenciais socio-legais críticos para analisar, sob um prisma multidisciplinar combinando literaturas legais, estudos sobre a privacidade, proteção de dados e governança e regulamentação para investigar a operação do sistema regulatório aplicado as práticas de tratamento de dados pessoais durante o desenvolvimento de políticas destinadas a combater a pandemia de COVID-19 na Coreia do Sul. Estruturado em três sessões o artigo apresenta a relação entre autodeterminação informacional e proteção de dados, particularmente durante emergências de saúde. Em seguida, analisa o uso de dados pessoais para combater o Covid19 na Coréia do Sul e em sua última seção, busca apresentar um modelo de valores de governança

oriundos do sistema de governança da Internet e algorítmica como elementos que devem orientar o desenvolvimento de uma governança de dados capaz de promover um uso mais seguro e equilibrado de dados pessoais durante crises de saúde.

A pesquisa realizada contribui potencialmente não apenas para os estudos relacionados a proteção de dados pessoais e privacidade, mas também pode influenciar o desenvolvimento de outras pesquisas capazes de demonstra a utilidade do modelo de governança FATE em outras áreas como finanças e meio ambiente. Combinando elementos teóricos do o campo da proteção de dados pessoais, privacidade e FAT, o artigo propõe o desenvolvimento de um modelo de governança baseado na equidade-justiça, responsabilização, transparência e expertise-conhecimento técnico, bem como na adoção de um critério de legitimação multissetorial como vetor principal da promoção da autodeterminação informacional e da proteção de dados pessoais.

A indicação de um modelo detalhado de governança fornece aos formuladores de políticas um importante ponto de partida para desenvolver instrumentos para projetar e operar modelos de governança capazes de balancear a necessidade de acesso aos dados pessoais com a proteção dos direitos e garantias dos titulares. Esse é um mecanismo importante que apoia o desenvolvimento de operações de formulação de políticas mais eficazes que também são capazes de produzir menos danos aos titulares de dados. O modelo proposto também permite que os formuladores de políticas analisem se seu processo de governança já incorpora esses valores padrão ou se pode ser modelado para incorporar a abordagem FATE.

Do ponto de vista teórico o artigo sugere que o estabelecimento de modelos de governança que incorporem em sua operação uma abordagem multisetorial fundada nos valores FATE funciona como um elemento capaz de transladar (LATOUR, 1999) ou num recorte teórico mais robusto *enact* (LAW, 1992), para suas atividades os elementos da autodeterminação

informacional que são mitigados quando do tratamento de dados pessoais em face do interesse do bem público. Entendendo que para Latour (2000), transladar significa deslocar objetivos, interesses, seres humanos, valores, ou como aponta Callon (1986) um processo no qual as partes envolvidas (atores) no caso em estudo o Estado e os titulares dos dados pessoais, interagem e manobram em negociações e delimitações para que, em determinado momento, algo seja pontuado como, por exemplo, conhecimento, conhecimento organizacional (CAMILLIS; ANTONELLO, 2016), ou legitimidade, o desenvolvimento de um sistema de governança de dados pessoais pautado em valores legítimos pode ser o depositário desse processo de tradução da autodeterminação informacional individual para uma autodeterminação informacional coletiva que seja concretizada via uma governança participativa e FATE.

O desenho e a execução de políticas públicas em situações de crise ou emergência como a experimentada no contexto da COVID-19, a proteção de dados pessoais tem sua prática obscurecida pelas buscas do interesse público. Equilibrar as necessidades de ter acesso aos dados necessários para a definição e execução de políticas e os possíveis danos infligidos aos titulares dos dados pessoais será sempre uma tarefa muito complexa e sensível. Encontrar o balanço adequado entre esses valores somente será possível através do desenvolvimento de estruturas de governança justas, responsáveis, transparentes, e baseadas em conhecimento técnico, que sejam capazes de traduzir através de seus valores coletivos todos os princípios que fundamentam o direito à autodeterminação informacional. Uma governança multisetorial e ancorada nos valores FATE é a chave para promover o exercício da autodeterminação informacional mesmo em momentos restritivos, mesmo nas horas mais escuras.

REFERÊNCIAS

ALLEN, Anita. Uneasy Access: Privacy for Women in a Free Society. Rowman & Littlefield, 1988.

ALMEIDA, Bethania de Araujo et al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. Ciência & Saúde Coletiva, [S.L.], v. 25, n. 1, p. 2487-2492, jun. 2020. FapUNIFESP (SciELO). http://dx.doi.org/10.1590/1413-81232020256.1.11792020.

ANVISA - Agência Nacional de Vigilância Sanitária. NOTA TÉCNICA GVIMS/GGTES/ANVISA N° 07/2020: orientações para a prevenção da transmissão de Covid-19 dentro dos serviços de saúde. Brasília: 2020. 33 p. Disponível em: http://portal.anvisa.gov.br/documents/33852/271858/NOTA+T%C3%89CNICA+-GIMS-GGTES-ANVISA+N%C2%BA+07-2020/f487f506-1eba-451f-bccd-06b8f1b0fed6. Acesso em: 30 jul. 2020.

BIONI, Bruno. Dados "anônimos" como antítese de dados pessoais: o filtro da razoabilidade. Disponível em: http://genjuridico.com.br/2019/10/11/dados-anonimos-antitese-dados-pessoais/. Acesso em: 15 abr. 2020.

BLACK, J., 2008. Constructing and contesting legitimacy and accountability in polycentric regulatory regimes. Regulation & Governance. 2 (2), pp. 137-164.

BUOSI, Ana Paula Assis; XAVIER JÚNIOR, Silvio Gonçalves; MONTEIRO NETO, João Araújo. A governança do compartilhamento de dados pessoais em tempos de crise: desafios e perspectiva. In: BIONI, Bruno Ricardo et al.

Os dados e o vírus: pandemia, proteção de dados e democracia. São Paulo: Reticências Creative Design Studio, 2020. p. 13-21. Disponível em: https://d335luupugsy2.cloudfront.net/cms/files/108127/1595880357EBOOK_OS_DADOS_E_O_VRUS_PANDEMIA_PROTEO_DE_DADOS_E_DEMOCRACIA_-_CAPA_ESPECIAL.pdf. Acesso em: 31 jul. 2020.

BEMSTEIN, S., & CASHORE, B., 2007. Can non-state global governance be legitimate? An analytical framework. *Regulation & Governance.* 1. pp. 347-71.

BOVENS, M., 2007. Analysing and Assessing Accountability: A Conceptual Framework. *European Law Journa*l. 13.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 28 jul. 2020.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal nº 6.387, de 24 de abril de 2020. Brasília, 2020. Disponível em: https://bit.ly/3fapKEt. Acesso em: 28 jul. 2020.

BUCHANAN, A., & KEOHANE, R.O., 2006. The Legitimacy of Global Governance Institutions. *Ethics & International Affairs*. 20. pp. 405–437.

CANNATACI, Joseph. The Individual and Privacy: Volume I (The Library of Essays on Law and Privacy, Vol. 1. Routledge, 2015.

CATE, Fred H. Privacy in the Information Age, 29, 1997.

CARR, M., 2015. Power Plays in Global Internet Governance. *Millennium: Journal of International Studies.* 43(2), pp. 640 –659

CHAN, S., & Pattberg, P., 2008. Private Rule-Making and the Politics of Accountability: Analyzing Global Forest Governance. *Global Environmental Politics* 8(3), pp.

103–121.

COWLING, B J; PARK, M; FANG, V J; WU, P; LEUNG, G M; WU, J T. Preliminary epidemiological assessment of MERS-CoV outbreak in South Korea, May to June 2015. Eurosurveillance, [S.L.], v. 20, n. 25, p. 1-13, 25 jun. 2015. European Centre for Disease Control and Prevention (ECDC). http://dx.doi.org/10.2807/1560-7917.es2015.20.25.21163.

DONEDA, Danilo. A proteção da privacidade e de dados pessoais no Brasil. Revista Observatório Itaú Cultural, São Paulo, n. 16, p. 136-150, jan./jun. 2014.

DRAKE, W., 2011. Multistakeholderism: External Limitations and Internal Limits. MIND: Multistakeholder Internet Dialog, Collaboratory Discussion Paper Series No. 2. Berlin: Internet Policymaking Collaboratory, pp. 68-72.

EDPB - European Data Protection Board. Statement on the processing of personal data in the context of the COVID-19 outbreak. Disponível em: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf. Acesso em: 15 abr. 2020.

ELMS, H., & PHILLIPS, R. A., 2009. Private security companies and institutional legitimacy: Corporate and stakeholder responsibility. *Business Ethics Quarterly*. 19. pp. 403-32.

GROSS, Hyman. Th concepto f Privacy, New York University Law Review, 34, 1967.

GUPTA, A., 2008. Transparency under Scrutiny: Information Disclosure in Global Environmental Governance. *Global Environmental Politics*. 8 (2), pp. 1–7.

HAUflER, V., 2006. The Transparency Principle and the Regulation of Corporations. In: Schuppert, G.F., (ed.) *Global Governance and the Role of Non-State Actors.* pp. 47–62.

HEMMATI, M., 2002. *Multi-stakeholder Processes for Governance and Sustainability Beyond Deadlock and Conflict.* London, Earthscan Publications.

HORNUNG, Gerrit; SCHNABEL, Christoph. Data protection in Germany I: the population census decision and the right to informational self-determination. Computer Law & Security Report, [S.L.], v. 25, n. 1, p. 84-88, 2009.

IBGE - Instituto Brasileiro de Geografia e Estatística. Censo 2020 adiado para 2021. Disponível em: https://bit.ly/2X4Qj7S. Acesso em: 28 jul. 2020.

Johns Hopkins University. COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU). Disponível em: https://www.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6. Acesso em: 29 jul. 2020.

Johns Hopkins University. East Asia offers mixed lessons in COVID-19 response. Disponível em: https://hub.jhu.edu/2020/05/13/east-asian-response-to-coronavirus/. Acesso em: 29 jul. 2020.

KEOHANE, R. O., 2011. Global Governance and Legitimacy. *Review of International Political Economy*. 18, pp. 99–109.

KO, Haksoo; LEITNER, John; KIM, Eunsoo; JEONG, Jonggu. Structure and enforcement of data privacy law in South Korea. International Data Privacy Law, [S.L.], v. 7, n. 2, p. 100-114, 24 abr. 2017. Oxford University Press (OUP). http://dx.doi.org/10.1093/idpl/ipx004.

LA CHAPELLE, B., 2007. Towards Multi-Stakeholder Governance – The Internet Governance Forum as Laboratory. In The Power of Ideas: Internet Governance in a global Multi-Stakeholder Environment. Berlin, pp. 256–70.

MENA, S., & PALAZZO, G., 2012. Input and Output Legitimacy of Multi-Stakeholder Initiatives. *Business Ethics*

Quarterly, 22 (3), pp. 527-556.

MENDES, Laura Schertel; BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: mapeando convergências na direção de um nível de equivalência. Revista de Direito do Consumidor, São Paulo, v. 124, [s.n.], p. 157-180, jul./ago. 2019.

MENDES, L. S. F. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. Direitos Fundamentais e Justiça, Belo Horizonte, v. 12, n. 39, p. 185-216, jul./dez. 2018.

MOON, M. Jae. Fighting COVID -19 with Agility, Transparency, and Participation: wicked policy problems and new governance challenges. Public Administration Review, [S.L.], v. 80, n. 4, p. 651-656, 20 maio 2020. Wiley. http://dx.doi.org/10.1111/puar.13214.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. In: CZYMMECK, Anja (ed.). Proteção de dados pessoais: privacidade versus avanço tecnológico. Rio de Janeiro: Fundação Konrad Adanauer, 2019. p. 113-135.

NAZARÉ, M.H. Big Data e desafios éticos. In: NEVES, M.C.P.; CARVALHO, M.G. Ética Aplicada – Novas Tecnologias. Lisboa: Edições 70, 2018, p. 315-331.

PARK, Sangchul; CHOI, Gina Jeehyun; KO, Haksoo. Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies. Jama, [S.L.], v. 323, n. 21, p. 2129-2130, 2 jun. 2020. American Medical Association (AMA). http://dx.doi.org/10.1001/jama.2020.6602.

PARK, Young Joon; CHOE, Young June; PARK, Ok; PARK, Shin Young; KIM, Young-Man; KIM, Jieun; KWEON,

Sanghui; WOO, Yeonhee; GWACK, Jin; KIM, Seong Sun et al. Contact Tracing during Coronavirus Disease Outbreak, South Korea, 2020. Emerging Infectious Diseases, [S.L.], v. 26, n. 10, out. 2020. Centers for Disease Control and Prevention (CDC). http://dx.doi.org/10.3201/eid2610.201315. Disponível em: https://wwwnc.cdc.gov/eid/article/26/10/20-1315_article#suggestedcitation. Acesso em: 29 jul. 2020.

RACHELS, James. "Why Privacy is Important" in Philosophical Dimensions of Privacy: Na Anthology. Ferdinand Schoeman, Ed., 1984

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

RÖSSLER, Beate. The Value of Privacy. Polity Press, 2005.

TAKE, I., 2012a. Regulating the Internet infrastructure: A comparative appraisal of the legitimacy of ICANN, ITU, and the WSIS. *Regulation and Governance.* [Online] Available at: https://doi.org/10.1111/j.1748-5991.2012.01151.x [Accessed 02 April 2015].

TAKE, I., 2012b. Global Governance Put to Test. A Comparative Study of the Legitimacy of International, Transnational and Private Forms of Governance. *Swiss Political Science Review*, Special Issue 18(2), pp. 220–248.

SALEMA, C. Tecnologias de Informação e Comunicação. In: NEVES, M.C.P.; CARVALHO, M.G. Ética Aplicada – Novas Tecnologias. Lisboa: Edições 70, 2018, p. 135-165.

SCHOLTE, J.A., 2011. (ed) Global Governance, Accountability and Civil Society. In: Building Global Democracy? Civil Society and Accountable. *Global Governance*. pp. 8–41.

SELBST, Andrew D. DANAH Boyd, Sorelle A. FRIEDLER,

Suresh Venkatasubramanian, and Janet Vertesi. 2019. Fairness and Abstraction in Sociotechnical

SOLOVE, Daniel J. Understanding Privacy. HUP, 2009.

STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Disponível em: https://bit.ly/32YF2cZ. Acesso em: 27 jul. 2020.

SCHWARTZ, Paul M. and SOLOVE, Daniel J., The PII Problem: Privacy and a New Concept of Personally Identifiable Information (December 5, 2011). New York University Law Review, Vol. 86, p. 1814, 2011, Available at SSRN: https://ssrn.com/abstract=1909366

WACHTER, Sandra and Mittelstadt, Brent and Russell, Chris, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI (March 3, 2020). Available at SSRN: https://ssrn.com/abstract=3547922 or http://dx.doi.org/10.2139/ssrn.3547922

WANG, Chen et al. A novel coronavirus outbreak of global health concern. The Lancet, [S.L.], v. 395, n. 10223, p. 470-473, fev. 2020. Elsevier BV. http://dx.doi.org/10.1016/s0140-6736(20)30185-9.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. Harvard Law Review. 1890.

WAZ, J., &WEISER, P., 2013. Internet Governance: The Role of Multistakeholder Organizations. *Journal of Telecommunications and High Technology Law*, 10 (2). [Online] Available at: SSRN: https://ssrn.com/abstract=2195167 or http://dx.doi.org/10.2139/ssrn.2195167