Tratamento de dados pessoais em aplicativos públicos relacionados ao coronavírus no Ceará

Processing of personal data in public applications related to the coronavirus in Ceará

Helena Martins[a, *]

Katiele Gomes Ferreira[a]

Luciana Gouvêa Hage de Castro[a]

Daniel Paiva de Macedo Júnior[a]

Elizandro dos Anjos Araújo Lima[a]

RESUMO: A pesquisa analisa o tratamento de dados pessoais em aplicativos relacionados à pandemia do coronavírus adotados pelo Governo do Estado do Ceará. Parte do reconhecimento do crescimento da importância das tecnologias como mediadoras de diversas atividades no contexto da pandemia, inclusive para fins de proteção à saúde, bem como dos riscos associados à crescente vigilância por meio delas. Debruça-se, então, sobre a análise dos aplicativos Monitora Covid-19, Ceará App e 190 Ceará, observando-os quanto à: a) política sobre dados pessoais; b) tratamento quanto à necessidade e finalidade; c) autodeterminação, proteção e segurança. Os resultados apresentam fragilidades no que tange à proteção de dados e ausência de controle dos usuários. Aponta a necessidade de se garantir o direito à proteção de dados pessoais no Brasil e em suas unidades federativas como contraponto à vigilância e como forma de disputa dos sentidos da inserção das tecnologias na sociedade contemporânea, especialmente no atual contexto da pandemia.

Palavras-chave: Dados Pessoais; Proteção de Dados; Aplicativos; Coronavírus; Ceará.

ABSTRACT: The research analyzes the treatment of personal data in applications related to the coronavirus pandemic adopted by the State Government of Ceará. It is part of the recognition of the growing importance of technologies as mediators of various activities in the context of the pandemic, including for health protection purposes, as well as the risks associated with the growing surveillance through them. It is worth mentioning, then, the analysis of the applications Monitora Covid-19, Ceará App and 190 Ceará, observing them regarding: a) policy on personal data; b) treatment regarding the need and purpose; c) self-determination, protection and security. The results show weaknesses in terms of data protection and lack of user control. It points to the need to guarantee the right to personal data protection in Brazil and its federal units as a counterpoint to surveillance and as a means of disputing the directions of the insertion of technologies in contemporary society, especially in the current context of the pandemic.

Keywords: Personal Data; Data Protection; Applications; Coronavirus; Ceará.

[a] Laboratório de Pesquisa em Políticas, Tecnologia e Economia da Comunicação, Instituto de Cultura e Arte, Universidade Federal do Ceará, Fortaleza, CE, Brasil.

[*] Correspondência para/*Correspondence to*: Helena Martins. E-mail: helena.martins@ufc.br.

Recebido em/*Received*: 15/08/2020; Aprovado em/*Approved*: 05/12/2020.

ACELERAÇÃO DA MEDIAÇÃO TECNOLÓGICA NO CONTEXTO DA PANDEMIA

Iniciada no fim de 2019, a pandemia do novo coronavírus (covid-19) assumiu proporções mundiais logo no início de 2020, alcançando o Brasil, segundo informações oficiais do Ministério da Saúde (BRASIL, 2020), em fevereiro deste ano. As medidas de isolamento e distanciamento social recomendadas pela Organização Mundial da Saúde (OMS) e outros órgãos da área ampliaram a necessidade de utilização das tecnologias da informação e da comunicação, particularmente da internet, para a realização das mais diversas atividades sociais, tornando-se centrais em situações de teletrabalho e da educação à distância, para citarmos dois exemplos relevantes.

Em relação às medidas relacionadas ou, ao menos, justificadas como de proteção à saúde, *scanners* termais foram instalados em espaços públicos como estações de trens e, progressivamente, em ambientes privados como lojas, com o intuito de identificar a temperatura daqueles que os atravessam e proibir a presença de pessoas com febre, por ser este um indício de contaminação. Visando controlar a circulação de infectados, em países como a China proliferaram práticas de reconhecimento facial por câmeras, motivando concorrência entre empresas que disputam qual consegue ter maior capacidade de reconhecimento em casos de pessoas que usam máscaras. O uso da máscara, aliás, é igualmente monitorado por drones. Drones que também foram usados na capital da Espanha, Madri, para emitir mensagens para os cidadãos apelando para que fiquem em casa. A aglomeração de pessoas passou a ser monitorada por meio de tecnologias de georreferenciamento, muitas vezes associadas aos smartphones da população em geral.

Essas tecnologias não têm sido estranhas ao Brasil[1]. No país, no dia 23 de março foi anunciada parceria da Prefeitura do Município do Rio de Janeiro com a operadora TIM para controlar o deslocamento de pessoas durante a pandemia. A operadora emitiu comunicado informando que seria responsável por coletar dados, valendo-se de suas antenas de telefonia, e enviar informações online sobre o perfil da movimentação em toda a cidade do Rio. "Os órgãos públicos poderão avaliar a tendência de mobilidade dos bairros antes e depois da pandemia, entender se as pessoas estão respeitando a reclusão, analisar se um bairro ou uma região específica está sofrendo aumento populacional ou não e com isso subsidiar ações das autoridades competentes no que tange a contingenciamento da propagação do vírus", anunciou[2].

No mesmo sentido, a empresa In Loco passou a utilizar tecnologia embarcada em aplicativos de clientes, que são bancos e varejistas, originalmente coletados com o objetivo de processar dados marketing, antifraude e outros, para a construção do índice de isolamento social. Assim, "[...] os dados que já coletamos no funcionamento normal do negócio foram anonimizados e transformados em dados estatísticos e

[1] A controvérsia em torno da utilização do georreferenciamento motivou posicionamento da Agência Nacional de Telecomunicações (Anatel), em que pondera a "grande necessidade de transparência, acompanhamento constante e participação de atores que possam oferecer um controle externo, ou mesmo social, na construção do respaldo jurídico desejável, bem como para fins de auditoria da utilização ou manipulação dos dados". A Anatel opinou que "a coleta e o tratamento de dados estão sujeitos à legislação vigente e, sobretudo, aos ditames da Constituição Federal. A ponderação de tutela entre saúde e privacidade encontra-se no mais alto grau de nossa hierarquia normativa. A despeito da presente crise, o momento ainda comporta a possibilidade de harmonização entre os dois bens jurídicos, de forma motivada e transparente". Disponível em: https://www.anatel.gov.br/institucional/component/content/article/104-home-institucional/2561-posicionamento-da-anatel-a-respeito-da-utilizacao-de-rastreamento-de-usuarios-de-telecomunicacoes-no-ambito-de-medidas-no-combate-a-pandemia-de-covid-19. Acesso: 15 de jul. 2020.

[2] Disponível em: https://www.tim.com.br/sp/sobre-a-tim/sala-de-imprensa/press-releases/institucional/prefeitura-do-rio-fecha-parceria-com-a-tim-para-montar-mapa-de-deslocamento-na-cidade-durante-a-pandemia. Acesso: 15 de jul. 2020.

cartográficos que indicam o percentual de dispositivos móveis que permaneceram em determinada localidade, por bairro", informou a empresa à pesquisa[3]. A In Loco acrescentou que exigiu contratualmente "[...] que os aplicativos clientes façam referência expressa ao uso de nossa tecnologia, de forma inteligível e de fácil acesso, em linguagem clara e simples e sem cláusulas abusivas, informando a coleta de dados através da tecnologia Inloco e a finalidade do tratamento destes dados".

Na área da Saúde propriamente, em março, foi assinado protocolo[4] entre o Ministério da Ciência, Tecnologia, Inovações e Telecomunicações (MCTIC), Hospital das Forças Armadas (HFA), o Ministério da Defesa, o Instituto Laura Fressatto e a Rede Nacional de Ensino e Pesquisa (RNP) a fim de disseminar a utilização da inteligência artificial, por exemplo, para identificar quadros de infecção com antecedência por meio de dados de pacientes cruzados por robôs. Em abril, o Senado aprovou o Projeto de Lei 696/2020 que liberou o uso da telemedicina durante a pandemia de COVID-19 no Brasil[5].

Os exemplos mostram que a pandemia levou ao aceleramento da inserção das tecnologias na sociedade. Um processo que tem origem ainda na década de 1970, quando a reestruturação produtiva do capitalismo deu centralidade ao que passou a ser chamado de novas tecnologias da informação e da comunicação (TIC) como base técnica do novo regime de acumulação, definido por Harvey (2012) como da acumulação flexível. Neste trabalho, seguindo o entendimento de Bolaño (2000), optamos por tratar esse período como o da Terceira Revolução Industrial. Embora considere o desenvolvimento tecnológico, este autor, ao analisar a indústria cultural e a informação no capitalismo, toma como elemento central a incorporação do elemento subjetivo na produção do capital e a intelectualização geral dos processos de trabalho na indústria e no setor de serviços.

Em sua compreensão, evidenciam essa mudança a codificação dos conhecimentos por tecnologias computacionais e a ampliação da mercantilização de setores como a cultura e, inclusive, a saúde. Interessante notar que o autor não deixou de reconhecer as possibilidades distintas da exploração mercantil na "economia do conhecimento". É ilustrativo seu trabalho sobre o Projeto Genoma do Câncer, sobre o qual pondera que aponta "[...] para uma forma de organização pública da produção, diferente obviamente da utopia de uma sociedade de produção tecnologicamente avançada, que Marx chamaria 'reino da liberdade', mas distinta também da pura exploração mercantil privada do capitalismo histórico" (BOLAÑO, 2005). Não obstante, não tem sido esse o tipo de configuração predominante. Desde meados dos anos 1990, tem crescido o processo de incorporação das tecnologias informacionais e particularmente da internet à dinâmica mercantil.

Para negar tanto o determinismo quanto a neutralidade tecnológica, é preciso voltar a Williams (2016), para quem a adoção de uma tecnologia responde menos a uma questão de necessidade dos usuários do que a uma adequação à determinada formação social. As tecnologias estão ligadas, detalha o autor, à intencionalidade dos grupos que têm a possibilidade de impor decisões, atrair recursos, obter

[3] Perguntas foram enviadas e respondidas pela In Loco em maio de 2020. A empresa informou não ser possível, devido a cláusulas contratuais, informar quais empresas e em quais estados atua.

[4] Disponível em: http://www.mctic.gov.br/mctic/opencms/salaImprensa/noticias/arquivos/2020/03/Acordo_dissemina_uso_da_Inteligencia_Artificial_na_area_da_saude.html. Acesso: 15 de jul. 2020.

[5] Disponível em: https://www12.senado.leg.br/noticias/materias/2020/03/31/senado-aprova-uso-da-telemedicina-durante-pandemia-de-covid-19. Acesso: 15 de jul. 2020.

permissão oficial e, ainda, estimular a operação de uma tecnologia, resultando, portanto, de pressões e limites existentes no interior de determinada sociedade. Nas últimas duas décadas, têm sido utilizadas sobretudo para gerar novos produtos e serviços, como os multimidia e, mais recentemente, os ligados ao tratamento de dados, alargando as possibilidades do capital em um momento de crise (CHESNAIS, 1996; MARTINS, 2018).

Pelo exposto, é possível sustentar que a pandemia do coronavírus não cria, mas acelera as transformações tecnológicas que estão associadas à reestruturação do sistema, à sua resposta à crise econômica mundial e, parte disso, à adoção de tecnologias em cada vez mais setores da vida social, muitas vezes de forma a potencializar a produção de lucros a partir da precarização do trabalho ou da exploração de dados. Exemplo disso é a aprovação da Lei da Telemedicina, aprovada no Brasil em abril de 2020, de forma bastante genérica, fomentando a realização de procedimentos de forma precária, ainda que apresentados como soluções para o momento (e, mais recentemente, como algo que perdurará mesmo após a pandemia). Morozov (2020) concorda com essa visão e aponta que, no contexto da pandemia, tem sido fomentado o que ele chama de "solucionismo tecnológico". "Em sua versão mais simples, sustenta que como não há alternativas (ou tempo, ou dinheiro), o melhor que podemos fazer é colocar curativos digitais sobre os danos. Os solucionistas implantam tecnologia para evitar a política; defendem medidas "pós-ideológicas" que mantém girando as engrenagens do capitalismo global", aponta.

O estudioso alerta que o "solucionismo" oculta questões como o crescente vigilantismo. Zuboff (2018, p. 49), ao formular o conceito de capitalismo de vigilância como "[...] nova forma de capitalismo de informação procura prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado", menciona essa dupla utilização de dados no tempo presente. Primeiro, como instrumento para a tentativa de redução da aleatoriedade na realização das mercadorias, com as novas formas de definir o público-alvo, obter informações sobre suas predileções e desenvolver campanhas. Segundo, como ferramenta para vigilância e controle, dinâmicas sempre presentes no desenvolvimento capitalista e que têm sido atualizadas e ampliadas, pois têm se tornado mais difusas e generalizadas.

A possibilidade desse tipo de vigilância, que é praticada por Estados, corporações e mesmo entre os cidadãos, está relacionada à lógica da exposição nas redes sociais e à presença constante de dispositivos móveis no cotidiano da população. A importância do *smartphone*, particularmente, fica nítida quando observados os dados sobre acesso à internet no Brasil. Segundo a pesquisa TIC Domicílios 2018, lançada em meados de 2019, 85% dos usuários de Internet da classe D e E acessam a rede exclusivamente pelo celular, 2% apenas pelo computador e 13% se conectam tanto pelo aparelho móvel quanto pelo computador. Tal cenário justifica a observação de aplicativos que funcionam a partir desses dispositivos e o questionamento sobre a forma como têm sido usados na sociedade.

Em meio a esse cenário, buscamos compreender as dinâmicas de captura e tratamento de dados pessoais em aplicativos produzidos pelo poder público e que se relacionam com a temática da pandemia. Aqui, delimitamos recorte territorial em torno do Estado do Ceará, terceiro em número de registro de mortos em função da covid-19, estando

atrás apenas de São Paulo e Rio de Janeiro[6], e analisamos os termos de uso dos aplicativos a Monitora Covid-19, Ceará App e 190 Ceará.

Trata-se, portanto, de um estudo de caso, definido por Yin (2010, p. 32) como "uma inquirição empírica que investiga um fenômeno contemporâneo dentro de um contexto da vida real, quando a fronteira entre o fenômeno e o contexto não é claramente evidente e onde múltiplas fontes de evidência são utilizadas". É precisamente neste momento em que nos encontramos, daí a relevância de, mais que um estudo quantitativo, observar práticas emergentes de forma qualitativa. Ainda que devamos considerar as desigualdades no acesso e mesmo questões culturais que ainda dificultam a utilização de *apps* no Brasil e, particularmente, no Ceará, os números mostram que os aplicativos são relevantes. Na Play Store, loja da Google, o Ceará App e o 190 Ceará já foram baixados, cada um, mais de 10 mil vezes. O Monitora Covid-19, utilizado também em outros estados nordestinos, por sua vez, mais de 100 mil vezes[7].

Quanto à problematização, diante das urgências postas pela pandemia e da proliferação de ideias "solucionistas", a biopolítica vigilantista pode ganhar lastro e legitimidade, daí a necessidade de lançarmos um olhar crítico sobre as práticas de coleta. Olhar que se baseia no que Fuchs (2011, p. 111) chama de conceito negativo de vigilância, que não a trata como uma qualidade ontológica de todas as sociedades, mas como "[...] inerentemente associada à violência e à dominação", sendo indissociável das estruturas de poder. Uma situação que, por outro lado, tem fomentado resistências e afirmações de direitos, como à proteção de dados pessoais, tomado aqui como parâmetro para a observação do tratamento efetivado a partir dos aplicativos. Nesse sentido, questionamos: como se dá o tratamento de dados pessoais de usuários de aplicativos públicos relacionados à covid-19 no Ceará, tendo em vista a necessária proteção de dados e os riscos associados à vigilância?

Para lidar com a questão exposta, tomando a caracterização conjuntural tratada com um composto da tessitura de sentidos e intencionalidades sobre as coisas, nos apoiamos na metodologia de Carvalho (2018) para análise de textualidades midiáticas ao sobrepor uma dinâmica de compreensão do contexto e da mídia de formas isoladas a partir de um escrutínio com perguntas orientadoras para, em seguida, reagrupá-las e fazer leituras mais amplas que os significados expressos do ponto de vista da linguística e, nisto, entrar numa seara da política, da sociologia para pensar lógicas de poder a partir dos conteúdos e dos símbolos em face aos aparatos e à realidade observável.

Para a interpretação das informações coletadas, passamos à fase da categorização, que consiste em "[…] uma operação de classificação de elementos constitutivos de um conjunto, por diferenciação e, seguidamente, por reagrupamento segundo o gênero (analogia), com os critérios previamente definidos" (BARDIN, 1977, p. 117). Formulamos, então, três categorias: (1) Política sobre dados pessoais; (2) Tratamento quanto à necessidade e finalidade; (3) Autodeterminação, proteção e segurança.

Foram aplicados questionários relacionados a cada categoria. Em relação à Política sobre dados pessoais, questionamos: i) Responsável(is) pelo desenvolvimento do aplicativo e parceiros; ii) Existência de Política de Privacidade ou Termos de uso; iii) Se há menção à proteção de dados na Política de Privacidade ou Termos de uso e como; e iv) Se na Política de Privacidade ou Termos de uso são detalhadas as finalidades do

[6] De acordo com o Ministério da Saúde, no dia 10 de agosto, os números de mortos nos estados mais afetados estavam assim distribuídos: São Paulo (25.151), Rio de Janeiro (14.108), Ceará (7.979), Pernambuco (6.970) e Pará (5.893).

[7] Dados relativos aos downloads feitos até o dia 1 de ago. 2020.

tratamento de dados. Em relação ao (2) Tratamento quanto à necessidade e finalidade: i) Permissões requeridas para acesso; ii) Dados pessoais utilizados conforme o app; iii) Dados pessoais utilizados conforme o Lumen; iv) Se consentimento é solicitado para a aplicação em geral ou para funções específicas; v) Se há possibilidade de tratamento posterior dos dados para outras finalidades. Quanto à (3) Autodeterminação, proteção e segurança, investigamos se: i) Titulares dos dados podem ou não ter acesso ao que está sendo coletado sobre eles; ii) Se dados são compartilhados com terceiros e quais; iii) Se há prazo definido para guarda ou exclusão dos dados; iv) Se o código do app é aberto ou fechado.

Em termos de técnicas de pesquisa, além da revisão de literatura, que viabilizou a definição do marco teórico e a construção conceitual da pesquisa, inclusive das categorias de análise supracitadas, para a coleta de informações foram observadas as próprias aplicações, tendo em vista o design tecnológico que apresentam. Buscamos, ademais, enfrentar um desafio marcante para as pesquisas sobre tais aplicações: a opacidade. Para confirmar ou confrontar as informações apresentadas quanto à utilização de dados, valemo-nos também da utilização do aplicativo Lumen Privacy Monitor. Trata-se de um software para celulares disponível gratuitamente na Google Play Store para uso em celulares do tipo Android. Segundo a descrição do próprio desenvolvedor disponível na página de download, "O Lumen é um projeto de pesquisa acadêmica liderado pelo Instituto Internacional de Ciência da Computação (ICSI), UC Berkeley e IMDEA Networks para iluminar o ecossistema móvel com informações reais do usuário. É patrocinado pela NSF (National Science Foundation) e pelo Data Transparency Lab"[8].

No Brasil, tem sido utilizado por grupos de pesquisa como o Internet Lab[9], que o utilizou para mapear as permissões envolvidas nos aplicativos e classificá-las quanto ao risco que implicam para a/o usuária/o, o que também será feito aqui, a partir de diálogo com o trabalho daquele grupo. Para realizar sua checagem de dados o Lumen cria uma conexão via VPN para capturar o tráfego de dados e, por meio de uma série de telas, faz a mensuração dessas informações indicando possíveis fragilidades, bem como identificando servidores para os quais os dados são direcionados com ou sem notificação e consentimento do usuário. Para a presente pesquisa, foram avaliadas as já mencionadas aplicações governamentais desenvolvidas para combate à covid-19, segundo critérios de privacidade de dados e rede, conforme dados colhidos e analisados a partir do uso da ferramenta de monitoramento Lumen Privacy Monitor, instalado em um aparelho de celular da marca Samsung com sistema Android, modelo SM-A105M.

A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: PRINCÍPIOS, APLICAÇÃO À SAÚDE E *VACATIO LEGIS*

Doneda (2011, p. 100-101) explica que, entre os anos 1970 e 1980, como expressão do fortalecimento da concepção da autonomia da proteção de dados pessoais e de sua consideração como direito fundamental, diversas legislações, em âmbito mundial, baseiam-se em medidas que passaram a ser referidas como *Fair Information Principles*,

[8] Informações também estão disponíveis em: <https://www.icsi.berkeley.edu/icsi/projects/networking/haystack>. Acesso: 10 ago. 2020.

[9] Ver, por exemplo, a pesquisa *COVID-19: Apps do governo e seus riscos à privacidade*, disponível em: <https://www.internetlab.org.br/pt/privacidade-e-vigilancia/covid-19-apps-do-governo-e-seus-riscos/ >. Acesso: 08 ago. 2020.

que o autor resume em cinco pontos: publicidade ou transparência, exatidão, finalidade, livre acesso e segurança física e lógica. Cita como exemplos disso as constituições da Espanha (1978) e de Portugal (1976). Documentos como a Convenção de Strasbourg e as *Guidelines* da OCDE, ambas do início dos anos 1980, também fazem referência expressa à proteção dos dados pessoais, vinculando-a à proteção dos direitos humanos e das liberdades fundamentais, e mesmo como pressuposto do estado democrático, segundo o autor. Tais textos inauguram a observação do tema sob o prisma dos direitos fundamentais, o que será desenvolvido, especialmente, pela União Europeia ao longo dos anos 1990.

Apesar dessa crescente importância, no Brasil, até 2018 não havia regra que tratasse explicitamente dos princípios da proteção dos dados pessoais. A tutela dos dados tinha como fundamento a Constituição Federal (BRASIL, 1988), que determina a proteção da personalidade e reconhece o direito à privacidade, considerando invioláveis a vida privada e a intimidade e também o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal como articula o parágrafo XII do Artigo 5°. Além disso, a Carta Magna determina a concessão de habeas data "a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo tal qual expresso no parágrafo LXXII do Artigo 5°. Doneda (2011, p. 103) acrescenta que, na legislação infraconstitucional, o Código de Defesa do Consumidor estabelece direitos em relação às informações presentes em bancos de dados e cadastros, "[...] implementando uma sistemática baseada nos Fair Information Principles à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro".

Nova referência à proteção de dados foi feita na Lei n° 12.965/2014 do Marco Civil da Internet (BRASIL, 2014), que dispõe, no artigo 3°, III, que a disciplina do uso da internet no Brasil tem com um dos princípios a "proteção dos dados pessoais, na forma da lei". A inclusão desse dispositivo ampliou a pressão para a criação de norma específica sobre o tema, que vinha sendo discutida pelo Ministério da Justiça desde 2007. Em 2011 e em 2015, a pasta realizou consultas públicas sobre o Anteprojeto de Lei de Proteção de Dados Pessoais. No Congresso Nacional, diversas audiências públicas versaram sobre o tema, que também foi objeto da campanha 'Seus dados são você', iniciada em 2017 por um conjunto de organizações da sociedade civil organizadas em torno da Coalizão Direitos na Rede.

Não é o caso, aqui, de detalhar a tramitação da proposta, mas é importante ter em vista que, ao longo dos anos de debate sobre a Lei Geral de Proteção de Dados Pessoais, finalmente aprovada em agosto de 2018, amadureceu-se como central a necessidade de consentimento da pessoa detentora do dado para o tratamento dele, o que significa que o titular deverá manifestar de forma livre, informada e inequívoca que concorda com o tratamento de seus dados pessoais – e apenas para uma finalidade determinada. Houve, portanto, a consolidação de uma visão garantista presente em outras normas, como na *General Data Protection Regulation* (GDPR) da União Europeia, que influenciou fortemente as discussões no Brasil.

No caso da Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018), ela está fundamentada, conforme o artigo 2°, no respeito à privacidade; na autodeterminação informativa; na liberdade de expressão, de informação, de comunicação e de opinião;

na inviolabilidade da intimidade, da honra e da imagem; no desenvolvimento econômico e tecnológico e a inovação; na livre iniciativa, a livre concorrência e a defesa do consumidor; e nos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

De acordo com o artigo 6°, as atividades de tratamento de dados pessoais deverão observar a boa-fé e dez princípios explicitados no texto, entre os quais destacamos, para fins deste trabalho: finalidade do tratamento dos dados para propósitos legítimos, específicos, explícitos e informados ao titular; necessidade, que consiste na limitação do tratamento ao mínimo necessário; livre acesso, que é a garantia de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; e segurança, definida como a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

A regra dispõe que o cidadão tem o direito a obter, a qualquer momento, informação das entidades públicas e privadas com as quais o controlador dos dados, como uma plataforma de rede social, realizou uso compartilhado de dados. Motivada pela preocupação com a segurança deles, detalha ainda, em um capítulo específico, regras para a transferência internacional de informações pessoais, ação que é limitada a poucas situações e cuja concretização só pode ocorrer para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais, medida que deverá ser avaliada pela Autoridade Nacional de Proteção de Dados. Fixa ainda, no Artigo 16, que os dados pessoais serão eliminados após o término de seu tratamento.

A Lei (BRASIL, 2018) não se aplica ao tratamento de dados para fins exclusivo segurança pública; defesa nacional; segurança do Estado; ou atividades de investigação e repressão de infrações penais tal qual pondera o Artigo 4°. Não obstante, vincula o tratamento nesses casos considerados excepcionais ao atendimento dos princípios gerais de proteção e os direitos do titular previstos na lei. Outro ponto polêmico ao longo da tramitação foi exatamente o uso de dados na área da saúde. Em primeiro lugar, porque dados de saúde são considerados sensíveis[10]. Assim, seu tratamento deve se dar nos termos do artigo 11, apenas "I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas" e "II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável" para, entre outros pontos, tutela da saúde.

Quanto à tutela da saúde, a redação originalmente aprovada dizia que o tratamento de dados sensíveis poderia ser realizado na hipótese de "procedimento realizado por profissionais da área da saúde ou por entidades sanitárias" como definido no inciso 'f' do artigo 7°. Uma Medida Provisória (MP 869/2018) apresentada no fim de 2018 e convertida em lei em 2019 alterou também esse trecho, que vigora agora com a seguinte redação: "f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária". A inclusão de "serviços de saúde" amplia o rol de agentes aos quais é permitido o tratamento de dados.

[10] Nos termos do artigo 5° da Le Geral de Proteção de Dados: "II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

A alteração também se deu no quarto parágrafo que, por sua vez, detalha quando não pode haver tratamento. A redação original "é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nos casos de portabilidade de dados quando consentido pelo titular" foi substituída por: "é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a **prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde**, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados" (grifo nosso), nos termos da redação dada pela Lei nº 13.853 (BRASIL, 2019). Como se vê, houve o alargamento da utilização de dados, o que beneficia os agentes que hoje conformam um mercado em franco desenvolvimento e com muito potencial de expansão.

As mudanças fragilizam, em nossa opinião, a proteção de dados, mas ainda assim o tratamento está vinculado aos princípios, à observação da proporcionalidade, da necessidade e de direitos do titular definidos pela lei. Sancionada em 14 de agosto de 2018, a LGPD deveria ter entrado em vigor em fevereiro de 2020. Entretanto, quando da edição da MP 869/2018, esse prazo foi ampliado em seis meses, para agosto de 2020, e a lei acabou entrando em vigor efetivamente no dia 18 de setembro. O vácuo desde a aprovação prejudicou a consolidação da perspectiva da proteção de dados no país.

Em fevereiro de 2020, em apenas três dias, foi proposta pelo governo federal, aprovada pelo Congresso Nacional, sancionada e publicada pela Presidência da República a Lei 13.979/2020, que dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus. A lei, já motivada, portanto, pela pandemia, traz medidas sobre tratamento de dados, entre as quais a obrigação de compartilhamento, entre órgãos e entidades da administração pública federal, estadual, distrital e municipal, de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção pelo novo coronavírus, com a finalidade exclusiva de evitar a sua propagação como reforça o 6º artigo da legislação.

Também tendo como justificativa a pandemia, em abril o Senado aprovou o Projeto de Lei 1.179/20, que trata do Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado no período da pandemia da Covid-19 e adia o início de vigência da LGPD para 1º de janeiro de 2021, com a ressalva de que os artigos relativos às sanções só entrarão em vigor em agosto de 2021. A proposta chegou à Câmara dos Deputados no dia 13 de abril. No dia 14, o Ministério Público Federal - MPF divulgou nota técnica sobre o tema, alertando:

> No cenário atual da Pandemia do COVID-19, a garantia da saúde pública e da aplicação de medidas sanitárias não significa abrir mão de direitos de proteção de dados pessoais e de privacidade. [...] Por isso, o arcabouço legal da LGPD robustece a rede regulatória, trazendo a transparência necessária ao controle social e facilitando o respeito às decisões tomadas no âmbito sanitário. Quanto mais transparência, mais confiança a sociedade tem na informação e, em tempos de crise da saúde pública, maior adesão é esperada nas medidas de salvaguarda da saúde. Além disso, as medidas excepcionais, que mitigam a privacidade para a garantia da saúde

> pública, devem ser claras, temporárias e restritas a sua finalidade (MPF, 2020, p. 02)[11].

Apesar do alerta, a proposta foi aprovada e em 10 de junho de 2020 foi sancionada a Lei nº 14.010, adiando a vigência da LGPD, que entrou em vigor em setembro de 2020. Ao longo desta análise, estávamos, portanto, em um período de *vacacio legis*, mas isso não significa inexistência de regramentos. Consiste, a nosso ver, em prazo para adaptação à lei, que deve, portanto, ser orientadora das práticas que passam a ser adotadas a partir de sua aprovação. Nesse sentido, sustentamos que, apesar do adiamento da vigência da LGPD, é imperativo que o Poder Público e os demais agentes adaptem-se a seus termos, desenvolvendo e estimulando a proteção de dados pessoais no Brasil.

APLICATIVOS RELACIONADOS AO COMBATE AO CORONAVÍRUS NO CEARÁ

Neste ponto, passaremos à análise dos aplicativos, tendo em vista a problemática e as categorias desenvolvidas para o estudo, quais sejam: (1) Política sobre dados pessoais; (2) Tratamento quanto à necessidade e finalidade; (3) Autodeterminação, proteção e segurança.

Monitora Covid-19

Construído a partir da Fundação Estatal Saúde da Família (FESF-SUS) da Bahia, em parceria com a Secretaria de Ciência, Tecnologia e Inovação (SECTI), a Secretaria de Saúde do Estado da Bahia (SESAB) e empresas (Novetech e Core), o Monitora Covid-19 foi lançado inicialmente pelo Governo da Bahia. Depois, foi celebrado Convênio de Cooperação Técnica com a FESF para disponibilização do app para todos os estados nordestinos interessados. Começou a ser utilizado no Ceará no mês de maio. Nas primeiras 24h, 422 pessoas baixaram, se cadastraram e responderam os questionários do aplicativo[12].

O Monitora Covid-19 apresenta como principais funcionalidades: classificação de risco automática das pessoas em isolamento; monitoramento em tempo real das condições clínicas dos pacientes em casa, por meio de chat; canal de comunicação permanente dos profissionais de saúde e as pessoas em sofrimento clínico e/ou psíquico; monitoramento georreferenciado das condições das pessoas e oferta de informação de qualidade e dentro da realidade de cada pessoa. Além disso, o está conectado à Plataforma Eletrônica da Saúde (iPES), o que permitirá a integração das informações aportadas no App ao Registro Eletrônico de Saúde do cidadão.

O Monitora Covid-19 teve sua última atualização em 22 de maio de 2020, versão considerada nesta análise. Ela dispõe de Termos de Uso, em que há referência à proteção de dados pessoais, conforme exposto no item 6, que trata de leis, regulamentos, direitos e deveres. Do texto, merece destaque o subitem 6.2, que detalha que o aplicativo "[...] respeita a sua privacidade e estará adaptado à Lei 13.709/18 LGPD e regulamentações futuras da ANPD [Autoridade Nacional de Proteção de Dados] e serão regidos e interpretados de acordo com as leis internas do Brasil".

[11] Disponível em: <https://www.conjur.com.br/dl/nota-tecnica-lgpd.pdf>. Acesso: 05 ago. 2020.

[12] Disponível em: <https://g1.globo.com/ce/ceara/noticia/2020/05/08/aplicativo-monitora-covid-19-comeca-a-funcionar-no-ceara-e-tem-422-cadastros-em-24-horas.ghtml>. Acesso: 10 ago. 2020.

Outro trecho do documento Termos de Uso informa sobre o uso das informações concedidas pelos usuários. Diz o item 7.4: "Todas as informações fornecidas por utilizadores ou profissionais de saúde são protegidas, de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei N° 13.709, de 14 de agosto de 2018". Também há detalhamento das finalidades no tratamento de dados, onde os usuários são informados sobre as possibilidades de uso das informações por órgãos de pesquisa voltados para saúde, como disposto no item 7.5 e no item 8 e seus subitens, que detalham política de garantia de sigilo e anonimato. O subitem 8.1 afirma sobre isso: "Será garantido o sigilo e anonimato de todas as informações produzidas pelo utilizador no 'MONITORA COVID-19', exceto exigência de lei, ou para tratar de questões de descumprimento.". Assim, em relação à política sobre dados pessoais, vemos que ela está disponível e faz referência à LGPD. Não obstante, não é fácil acessá-la. Apenas após o cadastro de uma conta é que são apresentados os Termos de Uso.

Em relação ao tratamento quanto à necessidade e finalidade, as seguintes permissões são requeridas para acesso: câmera (tirar fotos e gravar vídeos), local (acessar localização precisa por GPS e localização aproximada com base na rede); microfone (gravar áudio); armazenamento (modificar ou apagar conteúdos do cartão de memória, ler conteúdo do cartão SD); outras (executar serviços em primeiro plano, executar na inicialização, ler notificação do dispositivo, ver conexões de rede, impedir modo de inatividade do telefone, ver conexões WI-FI, receber dados da internet, controlar vibração, ter acesso total à rede, API de referência de instalação do Google Play, alterar as suas configurações de áudio, parear com dispositivos Bluetooth).

Além dos mencionados nas permissões e que não aparecem de forma explícita na plataforma, para usar o app é preciso se cadastrar. Então, os seguintes dados pessoais são solicitados: nome completo, CPF, cartão SUS (opcional), data de nascimento, nome da mãe (caso seja conhecida), sexo, e-mail, telefone celular, CEP, bairro, endereço completo, cidade e estado em que a pessoa está. Também são coletados dados sobre a situação de saúde no momento em que o usuário informa sobre comorbidades e quando atualiza o quadro de sintomas, segundo o aplicativo.

Ao utilizar a ferramenta de monitoramento Lumen Privacy Monitor, foi identificado que a aplicação acessava os seguintes pontos compreendidos como fragilidades: acesso à localização precisa do aparelho; permissão para fazer ligações; acesso ao hardware de impressão digital no aparelho. As duas primeiras situações identificadas pelo Lumen foram sinalizadas durante a instalação do aplicativo, que apresentou tela com solicitação de permissão do usuário, no entanto, o terceiro item, de acesso ao hardware de impressão digital do aparelho, não foi pedida nenhuma autorização, o que configura um tráfego de dados não informado, embora de baixo risco, conforme categorização feita pelo Lumen.

Ao se cadastrar, há a pergunta: "Para a equipe clínica possa entrar em contato com você e lhe oferecer o atendimento adequado precisamos de seu contato e localização, você autoriza o contato conosco?". Após aceitar, é apresentada uma tela com os Termos de uso e, na parte inferior da tela, sem precisar que o usuário realmente leia ou role a barra até o fim do texto, há que assinalar "eu li e concordo com os termos de uso" e aceitar ou recusar. Os botões são grandes, bastante visíveis e de tamanhos iguais. Após "aceitar", aparece a mensagem: "permitir que Monitora Covid-19 acesse a localização deste dispositivo". Se sim, o usuário é registrado "com sucesso".

Além da aceitação geral, não há solicitações não para cada finalidade. Exemplo dessa opção pelo consentimento geral, vemos que os dados de geolocalização são coletados no momento em que o usuário dá permissão ao app para acessar sua localização e, a partir de então, sempre que o usuário atualiza os dados clínicos, os dados de

localização são coletados, explica na página de perguntas frequentes ("FAQ"). Há tratamento posterior para a realização de pesquisas, mas, segundo informa, os dados não são utilizados para tais fins de forma individualizada, mas agregada, com "caráter populacional".

Não há informações sobre compartilhamento de dados com terceiros. Os titulares não têm acesso ao que é coletado sobre eles. Também não há prazo definido para guarda ou exclusão dos dados. Assim, o ponto mais frágil no que tange à proteção de dados reside na categoria Autodeterminação, proteção e segurança. O aplicativo tem código fechado e não é permitido o conhecimento ou manejo do escopo algorítmico que o orienta.

Ceará App

O Ceará App foi desenvolvido pelo Governo do Ceará, por meio do Laboratório de Inovação e Dados (Íris) e da Secretaria da Saúde do Estado (Sesa), e está atualmente vinculado à Casa Civil. Inicialmente vinculado aos serviços de saúde, o app deve se tornar um espaço de convergência de serviços digitais do governo. "Estamos partindo agora com a Secretaria da Saúde, mas teremos uma série de ferramentas que irá compor essa grande plataforma de transformação digital. Iremos adicionar de forma permanente outros serviços para que o Ceará App transforme-se na principal porta de entrada na relação entre o cidadão e o Governo do Estado", informou Élcio Batista, secretário-chefe da Casa Civil do Governo do Ceará[13].

No item 13 da política de privacidade, menciona parceiros, mas não detalha quem são. É orientado por uma política intitulada "Termos e Condições de Uso"[14]. Nela, faz menção às "leis nacionais", sem citar a LGPD expressamente. Devemos destacar que o texto informa que o aplicativo utiliza o Google Analytcs para coleta e processamento de dados conforme a política do Google, e que, ao aceitar a política do Ceará App, o usuário está concordando com os termos do Google. Essa relação tem impacto no tratamento por parte de terceiros, pois no mesmo item em que menciona a relação, informa que seus parceiros poderão fazer uso dos dados dos usuários e também que o Ceará App não se responsabiliza pelo que a empresa Google irá fazer com esses dados. Nos termos do texto: "Quaisquer usos feitos pelo Google ou seus parceiros dos Dados do Usuário coletados por meio dessas ferramentas serão de responsabilidade única e exclusiva do Google, sendo o Ceará APP® isenta de quaisquer responsabilidades resultantes de tal uso".

Quanto às finalidades, detalha que os dados são coletados para:

> (i) Identificação, autenticação e autorização; (ii) Atender adequadamente às solicitações e dúvidas; (iii) Manter atualizados cadastros para fins de contato por telefone, correio eletrônico, SMS, mala direta ou por outros meios de comunicação; (iv) Aperfeiçoar o uso e a experiência interativa durante navegação nos sites, aplicativos e serviços prestados pelo Ceará APP®; (v) Efetuar estatísticas, estudos, pesquisas e levantamentos pertinentes às atividades e comportamentos do Usuário ao utilizar os sites, aplicativos e serviços prestados pelo Ceará APP®, realizando tais

[13] Disponível em: <https://www.ceara.gov.br/2020/05/26/governo-lanca-ceara-app-com-servicos-de-saude/>. Acesso: 10 ago. 2020.

[14] Disponível em: <https://www.ceara.gov.br/termos-e-condicoes-de-uso-ceara-app/>. Acesso: 10 ago. 2020.

> operações de forma anonimizada com Dados Anonimizados; (vi) Promover os serviços do Ceará APP®, além de informar sobre novidades, funcionalidades, conteúdos, notícias e demais informações relevantes para a manutenção do relacionamento com o Ceará APP®; (vii) Resguardar o Ceará APP® de direitos e obrigações relacionadas ao uso dos sites, aplicativos e serviços prestados pelo Ceará APP®; (viii) Colaborar e/ou cumprir ordem judicial ou requisição por autoridade administrativa; (ix) Gerenciar riscos e detectar, prevenir e/ou remediar fraudes ou outras atividades potencialmente ilegais ou proibidas, além de violações de políticas ou termos de uso aplicáveis.

Além disso, inclui entre as finalidades o envio de emails institucionais e compartilhamento de dados. Diz o texto:

> Ao aceitar a Política de Privacidade, Você está ciente de que o Ceará APP® poderá compartilhar os dados coletados por meio da plataforma nas seguintes situações: (i) se fundamental à prestação dos Serviços pelo Ceará APP®; (ii) a fim de proteger os interesses do Ceará APP®, em qualquer tipo de conflito, incluindo ações judiciais; (iii) no caso de operações societárias envolvendo o Ceará APP®, tendo em vista que, neste caso, a transferência das informações será necessária para a continuidade dos serviços; (iv) mediante ordem judicial ou pelo requerimento de autoridades administrativas que detenham competência legal para sua requisição; ou, ainda, para (v) utilização para fins públicos de tomada de decisão analítica.

Além do problema de vincular um serviço público à política de uma plataforma corporativa, a Google, sem que os cidadãos tenham opção de utilizar o aplicativo com proteção, vemos que o uso de dados é bastante abrangente. Exemplificam isso os itens "colaborar e/ou cumprir ordem judicial ou requisição por autoridade administrativa", pois requisição com as autoridades administrativas é mais abrangente e usado adicionalmente à relação de cumprimento de ordem judicial, portanto abre margem para questionamento sobre a disponibilidade de dados para outras áreas do próprio governo, e "utilização para fins públicos de tomada de decisão analítica", já que não está expressamente informado que os dados serão anonimizados. Vê-se, portanto, a existência de fragilidades no tocante à proteção de dados já na política do app, seja pela relação com o Google ou com a administração.

Em relação ao Tratamento quanto à necessidade e finalidade, o aplicativo foi lançado sem detalhamento das permissões requeridas para acesso. Na versão 1.2.0, atualizada em 15 de junho, a lista foi incluída. Consistem em permissões requisitadas: acesso ao local (GPS e rede), modificar ou excluir o conteúdo do cartão SD, ler conteúdo do cartão SD, ler as configurações de sincronização, executar serviço em primeiro plano, acessar configurações de Bluetooth, executar na iniciação, verificação de licença do Google Play, ver conexões de rede, impedir modo de inatividade do telefone, ver conexões Wi-fi, receber dados de internet, controlar vibração, ativar e desativar sincronização, ter acesso total à rede, recuperar apps em execução, API de referência de instalação do Google Play, parear com dispositivos Bluetooth, acessar comandos extras do provedor de localização e reconhecimento de atividade.

O aplicativo informa que coleta três tipos de dados: aqueles fornecidos efetivamente pelo usuário ao utilizar o app, tais como navegação, utilização do plantão médico, nome e sobrenome, gênero, sintomas de saúde, CPF, endereço de e-mail, endereço postal, número de telefone, data de nascimento e quaisquer outros dados fornecidos quando há o cadastro do usuário, bem como durante as suas atividades no Ceará App;

os gerados automaticamente quando da navegação e/ou utilização do aplicativo – por exemplo, por meio de cookies, tecnologias que armazenam informações sobre atividades do usuário na internet; e dados de geolocalização, como informações sobre navegador e sistema operacional do dispositivo, endereço IP, páginas acessadas dentro ou fora do CEARÁ APP, links e botões clicados. Os últimos mencionados mostram que a coleta se dá efetivamente para além do próprio dispositivo e não necessariamente relacionada ao que ele oferta como serviço.

Durante teste realizado com o uso do aplicativo Ceará App a partir do Lumen, foram identificadas as seguintes situações: acesso à localização precisa do aparelho; tentativa de acesso à contas logadas no aparelho; ler o estado do celular; acessar o hardware de impressão digital no aparelho. Dessas fragilidades, apenas o acesso à localização do aparelho possui solicitação de permissão. A informação, portanto, não é explícita, embora nos Termos de Uso o desenvolvedor informe que poderá ter acesso aos demais dados. Não é solicitado consentimento por função específica.

Quanto à (3) Autodeterminação, proteção e segurança, não informa se titulares dos dados podem ter acesso ao que está sendo coletado sobre eles, ao passo que confirma que os dados do usuário podem ser utilizados por um terceiro, Google. Sobre outros parceiros, não informa quem são, apenas menciona que pode fornecer informações para parceiros. Não é informado sobre nenhum prazo para a exclusão dos dados. O código do aplicativo é fechado.

190 CEARÁ

O aplicativo 190 Ceará foi lançado em 2017 como uma iniciativa da Secretaria da Segurança Pública e Defesa Social do Ceará. Em abril de 2020, foram feitas alterações a fim de ampliar as funcionalidades em face ao contexto pandêmico e permitir a realização de denúncias de aglomerações, ramificadas pelo formato em festas, bares e vivências em espaços públicos, e notificações de comércio aberto, subdividido nas categorias de restaurantes, bares, boates e comércio de modo mais amplo.

É certo que o aplicativo possui Termos de Uso, mas a política de dados, como vimos também no caso anteriormente abordado, se dá nas ausências, dado que não há informações específicas sobre as medidas de proteção dos dados e a única garantia conferida está na menção de sigilo aos dados que, ao serem confrontados com as questões sobre finalidades do tratamento, informa apenas que os dados enviados serão usados pela polícia e apenas por ela.

Para cadastro, o aplicativo requisita informações obrigatórias do usuário em dados que explicitam o nome completo, email, telefone, data de nascimento, numeração de registro em CPF e RG e, por fim, a pactuação de uma senha para acesso ao sistema. Para funcionamento, demanda a instalação em aparelho móvel com sistema Android ou IOS e conectado em rede 3G, 4G ou WI-FI - sem delimitação de potência de transmissão de dados. Solicita para uso, ainda, acesso ao GPS e outras informações enviadas do dispositivo, ainda que desligado.

A única solicitação para uso de dispositivos do smartphone está na liberação de localização do dispositivo via GPS para ação geral do aplicativo e, por sua vez, não demanda autorizações em ações específicas. Entretanto, ainda sem autorização expressa e assegurada na aceitação dos termos de uso, o 190 Ceará realiza leitura e escrita na memória externa; leitura do estado do telefone; controle da vibração do aparelho; impedimento que o telefone entre em modo de espera; e, por fim, acesso completo à rede, incluindo exibição de conexões.

O teste realizado com o aplicativo 190 Ceará identificou fragilidades nos seguintes aspectos: acesso à localização precisa do aparelho; ler o estado do celular; acessar o hardware de impressão digital no aparelho. O aplicativo apresentou solicitação de permissão apenas para o pedido de acesso à localização do aparelho, os demais itens só foram identificados a partir do monitoramento com o Lumen, o que mostra, uma vez mais, que opera de forma opaca.

Sobre Autodeterminação, proteção e segurança, observamos que o usuário não pode ter acesso aos dados sobre ele produzidos, cabendo apenas a polícia a possibilidade de contato com as informações. Nessa mesma determinação, fica subentendida a vedação de acesso da informação a terceiros. Não há menção sobre períodos de guarda ou exclusão de dados que, deste modo, podem ser utilizados das mais variadas formas, dado que não há exposição dos métodos de tratamento ou interesses que o orientam. O aplicativo possui código fechado e consta de uma Cláusula de Engenharia, onde: 'você concorda em não desmontar, compilar, usar engenharia reversa ou tentar de outra forma obter acesso ao código fonte'.

CONCLUSÕES

Pautada pela lógica comercial e dirigida também por interesses políticos, a inserção das tecnologias na sociedade atualmente não tem se dado como fruto de debate público e não é pensada para o atendimento de demandas da coletividade. Como exposto no momento da pandemia do coronavírus, as dimensões que têm ganhado relevância são: o uso das tecnologias para a promoção de produtos e também para a ampliação do controle e da vigilância, ainda que muitas vezes esses processos caminhem ao lado da oferta de serviços ou mesmo de possibilidades de comunicação importantes, como a conexão para estudar e trabalhar ou o monitoramento para proteger a saúde.

No Brasil, a construção da LGDP inaugura um processo de proteção que, embora vigoroso nos últimos anos, com a ampliação da discussão sobre o tema, está longe de ser assegurado no país. Não temos internalizado esse direito, nem chegou a ser constituída autoridade responsável por zelar, implementar e fiscalizar o cumprimento da lei. Assim, o crescimento da utilização de dados se dá em um contexto de fragilidades no que tange à garantia do direito à proteção de dados no Brasil. Além disso, já na elaboração da lei essa proteção foi flexibilizada inclusive, a nosso ver, em áreas extremamente sensíveis, como segurança pública e saúde.

Se esses limites já existiam e significavam riscos à efetivação de direitos em tal seara, o adiamento do início da vigência da LGPD fragilizou ainda mais a possibilidade de garantia de privacidade e proteção de dados pessoais. As urgências e preocupações associadas à pandemia foram utilizadas para argumentar pelo adiamento e também para naturalizar a captura e o tratamento de dados, no período analisado. Com isso, nossos corpos e mentes estão mais controlados por governos e mesmo por empresas privadas, o que foi apresentado, ao longo do trabalho, como um problema importante para as sociedades e os indivíduos, que se tornam mais suscetíveis a práticas diversas de controle.

Essas questões aparecem quando analisados os aplicativos utilizados pelo governo do Ceará. Ainda que se considere que a presença deles no cotidiano da população é diminuta, sua importância reside no fato de expressar a crescente utilização e a mediação tecnológica de serviços públicos.

O detalhamento de cada aplicativo mostrou que, de forma geral, há referência à política sobre dados pessoais, mas muitas vezes de forma genérica, tanto que, ao observamos o tratamento quanto à necessidade e finalidade, verificamos muitas fragilidades. Entre elas, merecem ser citadas a lógica do consentimento genérico e pouco informado, a captura de mais informações do que as estritamente necessárias para o provimento dos serviços e mesmo a possibilidade de tratamento posterior por agentes que, em alguns casos, não são sequer detalhados.

Em todos os aplicativos estudados, há mais dados coletados do que os informados, como vimos ao utilizar a ferramenta de monitoramento Lumen Privacy Monitor. Quanto a isso, aspecto positivo é que as fragilizadas percebidas são pequenas. Neste aspecto, a coleta de dados se realiza sem ciência prévia do usuário sobre as informações a serem extraídas, situações que entram em confronto com o Marco Civil da Internet (referência), no parágrafo VIII do 7º Artigo, que confere ao usuário o direito 'de informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais' que somente poderão ser utilizados para finalidades especificadas ao usuário, justificadas e em conformidade com a lei.

O Monitora Covid-19 é o que mais parece adequado às prescrições da LGPD, que menciona com detalhamento maior do que nos demais casos, mas seria necessário melhorar a exposição dos termos de uso para torná-los mais acessíveis aos usuários. Pesa o fato de que muitos dados coletados (como CPF, endereço detalhado, e-mail) o são já no cadastro, dados que podem vir a ser necessários apenas no momento da utilização de determinado serviço (não de todos, aliás). Assim, ainda que mais cauteloso, acaba também favorecendo a produção e disponibilização de muitas informações, sem que haja controle do usuário sobre esse processo.

No caso do Ceará App, há muitas fragilidades na política,sendo a mais grave o fato de submeter os usuários de um aplicativo que pretende mediar diversos serviços públicos à plataforma Google, por ser haver relação com o Google Analytcs, sem possibilidade de negar essa disponibilização das informações. Entendemos como um problema grave o fato de o governo acabar fazendo com que o cidadão concorde obrigatoriamente com os termos do Google, o que levanta questões sobre a autonomia do poder público frente a plataforma. Também não há nitidez quanto aos dados capturados nem mesmo em relação às finalidades, existindo abertura para usos posteriores e por parte de outros agentes.

O 190 Ceará, focado na dinâmica de segurança pública, tem alto nível de opacidade e o ponto de maior objetividade e transparência está na vedação ao conhecimento e manejo do código, da lógica e da tessitura tecnológica que compõe o aplicativo. Relega ao usuário um total desconhecimento sobre os dados a serem construídos e, a nosso ver, infringe a lei ao coletar dados sem que o usuário possua ciência das informações a serem extraídas pelo dispositivo. Este último, por sua vez, se configura como um mecanismo permanente de coleta de dados pois esta funcionalidade permanece ainda que desligado e, esta situação, estabelece para o usuário uma situação profunda de vigilância que, nos termos do que Zuboff (2018, p. 48) vai considerar como uma expressão da "lógica hegemônica da acumulação em nosso tempo".

Nos aplicativos analisados, a conjunção comum onde o usuário não é sujeito de leitura e conhecimento das informações compiladas sobre si revela a relação desigual expressa por Zuboff (2018), em que, à medida que os fornecedores das aplicações dispõem de total transparência dos usuários e domínio dos registros de experiências nas plataformas virtuais, estabelecem sigilo absoluto sobre as produções, os lucros - sejam financeiros ou sociais - e as possibilidades advindas da posse de nossos dados, em ação assegurada por ordenamento jurídico, que revela uma justaposição de poder.

Ao contrário disso, para que haja esforços no sentido da promoção do direito à proteção de dados e de sua efetivação, seria recomendável adotar a solicitação de consentimento por serviço, o que ajudaria a não haver naturalização das práticas de coleta. Esse conjunto de questões e a falta de práticas que fomentem a autodeterminação, garantam transparência, proteção e segurança fazem com que concluamos apontando a necessidade de revisão das formas de operação dos aplicativos, de modo que possam ser guiados tanto pela busca pela prestação de serviços quanto pela garantia de direitos.

REFERÊNCIAS

BARDIN, Laurence. *Análise de conteúdo.* Lisboa: Edições 70, 1977.

BOLAÑO, César Ricardo Siqueira. *Indústria cultural, informação e capitalismo.* São Paulo: Hucitec, 2000.

BOLAÑO, C. O projeto Genoma Humano da FAPESP: modelo para a economia do conhecimento?. *In:* ENCONTRO ANUAL DA ANPOCS, 29., 2005, Caxambu. *Anais*... São Paulo: ANPOCS, 2005.

BRASIL (1988). Constituição da República Federativa do Brasil. Brasília: Senado, 1988.

BRASIL. Lei nº 12.965 de 23 de abril de 2014: estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União,* seção 1, 2014.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018: dispõe sobre a proteção de dados pessoais e altera a Lei nº ,12.965 de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União,* seção 1, 2018.

BRASIL. Medida provisória nº 869 de 27 de dezembro de 2018: altera a Lei nº ,13.709 de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados. *Diário Oficial da União,* seção 1, 2018.

BRASIL. Ministério da Saúde. Centro de Operações de Emergência em Saúde Pública para Infecção Humana pelo novo coronavírus. *Boletim Epidemiológico Coronavírus, Brasília,* n. 2 , fev. 2020. Disponível em: saude.gov.br/boletins-epidemiologicos. Acesso em: 08 ago. 2020.

CHESNAIS, François. *A mundialização do capital.* São Paulo: Xamã, 1996.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico,* Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

FUCHS, Christian. Como podemos definir vigilância?. *MATRIZes,* n. 1, p. 109-135, 2011.

HARVEY, David. *Condição pós-moderna.* 23. ed. São Paulo: Edições Loyola, 2012.

MARTINS, Helena. *O mercado de comunicações brasileiro no contexto da convergência:* análise das estratégias do Grupo Globo e da América Móvil. 2018. 369 f.: il. Tese (Doutorado em Comunicação) - Universidade de Brasília, Brasília, 2018.

MOROZOV, Evgeny. Solucionismo, nova aposta das elites globais. *Revista IHU Online.* Disponível em: http://www.ihu.unisinos.br/78-noticias/598364-solucionismo-nova-aposta-das-elites-globais. Acesso em: 2020.

WILLIAMS, Raymond. *Televisão:* tecnologia e forma cultural. São Paulo; Belo Horizonte: Boitempo; PUC Minas, 2016.

YIN, Robert K. *Estudo de caso:* planejamento de métodos. 4. ed. Porto Alegre: Bookman, 2010.

ZUBOFF, S. Big other: capitalismo de vigilância e perspectivas para uma civilização da informação. *In:* BRUNO, F. *et al.* (orgs.) *Tecnopolíticas da vigilância.* São Paulo: Boitempo, 2018.