PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS DURANTE A PANDEMIA DA COVID-19

Marcos Ehrhardt Júnior[1]

Gabriela Buarque Pereira Silva[2]

Nem máscara, nem álcool gel: em outros países, a vigilância tecnológica tem sido uma das principais medidas de combate ao surto da COVID-19. Em que medida a legislação sobre proteção de dados vem sendo observada e quais os desafios para a tutela da privacidade ao final da pandemia?

urante a ocorrência de uma crise, especialmente num contexto em que muitas vezes não existem precedentes claros acerca de que medidas devem ser adotadas para o seu enfrentamento, é comum nos valermos de todas as ferramentas que estejam ao nosso dispor sem que tenhamos tempo de refletir com mais cuidado sobre os impactos de decisões tomadas no calor dos fatos. Para gerenciar uma crise que trouxe consigo efeitos deletérios para além da saúde, atingindo a economia e a gestão pública, a urgência na adoção de medidas não pode ignorar direitos fundamentais, entre os quais, para os fins desta reflexão, destaca-se a privacidade.

Que medidas vêm sendo adotadas em outros países para combater a difusão do vírus?

Se no campo das decisões médicas, acompanhar o

[1] Advogado. Doutor em Direito pela Universidade Federal de Pernambuco (UFPE). Professor de Direito Civil da Universidade Federal de Alagoas (UFAL) e do Centro Universitário CESMAC. Editor da Revista Fórum de Direito Civil (RFDC). Vice-Presidente do Instituto Brasileiro de Direito Civil (IBDCIVIL). Presidente da Comissão de Enunciados do Instituto Brasileiro de Direito de Família (IBDFAM).
[2] Advogada. Mestranda em Direito Público pela Universidade Federal de Alagoas.

desenrolar da pandemia em outras nações tem sido fator decisivo para o enfrentamento do problema em território nacional, há de se destacar que noutras áreas, especialmente no que concerne aos avanços tecnológicos[3], precisamos de um pouco de cautela.

Como o tratamento de dados pessoais impacta no combate ao coronavírus?

Do intenso noticiário a respeito do combate à pandemia, é possível extrair algumas informações relevantes. Cingapura emitiu diretrizes consultivas esclarecendo que os dados pessoais podem ser coletados, usados ou divulgados, sem o consentimento, para fins de proteção de saúde dos habitantes, rastreamento de contatos e outras medidas de resposta.

Na Itália, um decreto-lei emitido em 9 de março de 2020 autorizou o compartilhamento de dados entre as autoridades de saúde e a comunidade civil para gerenciar a emergência.

A inteligência artificial também vem rastreando padrões espaciais da patologia. Uma empresa canadense chamada *BlueDot* coleta dados multilíngues de bases de dados oficiais da saúde pública para prever potenciais surtos[4].

Pesquisadores da *Harvard Medical School* coletam dados autorizados e dados de mídias sociais para explorar tendências geográficas da doença[5].

Na China, drones já estão sendo utilizados para alertar a população a usar máscaras[6]; placas e tecnologias de reconhecimento fácil vêm rastreando pessoas e pedindo que se mantenham em isolamento[7], além da implantação de *scanners*

[3] Disponível em: https://www.withersworldwide.com/en-gb/insight/in-this-time-of-covid-19-does-personal-data-privacy-get-thrown-out-the-window. Acesso em: 21 mar. 2020.

[4] Disponível em: https://www.wired.com/story/ai-epidemiologist-wuhan-public-health-warnings/. Acesso em: 22 mar. 2020.

[5] Disponível em: https://www.wired.com/story/how-ai-tracking-coronavirus-outbreak/. Acesso em: 22 mar. 2020.

[6] Disponível em: https://globalnews.ca/news/6535353/china-coronavirus-drones-quarantine/. Acesso em: 22 mar. 2020.

[7] Disponível em: https://www.reuters.com/article/us-china-health-

infravermelhos em estações de trem e aeroportos, que detectam indivíduos com febre[8]. A China também implementou um aplicativo que classifica as pessoas segundo riscos de contágio e determina quem deve ficar em quarentena, além de enviar dados à polícia chinesa[9]. A empresa responsável pelo aplicativo e as autoridades não explicam como exatamente o sistema funciona, não sendo possível, no momento, avaliar com mais profundidade a dinâmica de utilização dos dados pessoais naquele país, que nos últimos anos vem se destacando na utilização de ferramentas de tratamento de dados biométricos para as mais diversas finalidades, em geral, estabelecidas e controladas pelo governo central[10].

surveillance/coronavirus-brings-chinas-surveillance-state-out-of-the-shadows-idUSKBN2011HO. Acesso em: 22 mar. 2020.

[8] Disponível em: https://www.scmp.com/tech/policy/article/3049215/ai-firms-deploy-fever-detection-systems-beijing-help-fight-coronavirus. Acesso em: 22 mar. 2020.

[9] Disponível em: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. Acesso em: 22 mar. 2020.

[10] Neste ponto, interessante destacar matéria publicada no jornal El País, com o seguinte título "*O coronavírus de hoje e o mundo de amanhã, segundo o filósofo Byung-Chul Han*", que compara o modo ocidental de se comportar perante as mais diversas formas de vigilância digital com a perspectiva oriental: "(...) A consciência crítica diante da vigilância digital é praticamente inexistente na Ásia. Já quase não se fala de proteção de dados, incluindo Estados liberais como o Japão e a Coreia. Ninguém se irrita pelo frenesi das autoridades em recopilar dados. Enquanto isso a China introduziu um sistema de crédito social inimaginável aos europeus, que permite uma valorização e avaliação exaustiva das pessoas. Cada um deve ser avaliado em consequência de sua conduta social. Na China não há nenhum momento da vida cotidiana que não esteja submetido à observação. Cada clique, cada compra, cada contato, cada atividade nas redes sociais são controlados. Quem atravessa no sinal vermelho, quem tem contato com críticos do regime e quem coloca comentários críticos nas redes sociais perde pontos. A vida, então, pode chegar a se tornar muito perigosa. Pelo contrário, quem compra pela Internet alimentos saudáveis e lê jornais que apoiam o regime ganha pontos. Quem tem pontuação suficiente obtém um visto de viagem e créditos baratos. Pelo contrário, quem cai abaixo de um determinado número de pontos pode perder seu trabalho. Na China essa vigilância social é possível porque ocorre uma irrestrita troca de dados entre os fornecedores da Internet e de telefonia celular e as autoridades. Praticamente não existe a proteção de dados. No vocabulário dos chineses não há o termo "esfera privada". Disponível em https://brasil.elpais.com/ideas/2020-03-22/o-coronavirus-de-hoje-e-o-mundo-de-

Em Taiwan e Israel, *smartphones* foram programados para notificar as autoridades públicas se os pacientes não estiverem observando a quarentena[11], em um sistema de rastreamento.

Na Coreia do Sul, foram divulgados os dados de viagens de 29 pacientes confirmados, compilados por meio de bases de celulares, cartões de crédito e câmeras de segurança[12].

Nessa breve digressão, é possível perceber que o tratamento dos dados pessoais está sendo utilizado para geolocalização, identificação e rastreamento de pacientes, gerenciamento do risco de contágio, entre outras atividades, com a finalidade de melhorar os instrumentos de combate à pandemia.

Nos Estados Unidos, por sua vez, existe a Lei de Portabilidade e Responsabilidade dos Seguros de Saúde[13], que exige a criação de padrões nacionais para proteger informações confidenciais de saúde do paciente. Recentemente, o Departamento de Saúde dos EUA publicou um boletim informando que as entidades responsáveis pela proteção das informações pessoais de saúde devem observar as regras de privacidade e que situações de emergência não são capazes de anular tais garantias individuais[14]. Nesse ponto, Ohio aprovou um protocolo para proteger os locais de origem dos pacientes,

amanha-segundo-o-filosofo-byung-chul-han.html?rel=mas. Acesso em: 24 mar 2020.

[11] Disponível em: https://www.telegraph.co.uk/news/2020/02/03/taiwan-uses-smartphones-monitor-patients-quarantined-virus-scare/. Acesso em: 22 mar. 2020 e https://platform.dataguidance.com/news/israel-government-approves-mobile-tracking-monitor-coronavirus-quarantine-enforcement. Acesso em: 22 mar. 2020.

[12] Disponível em: https://www.dailymail.co.uk/news/article-8011197/South-Korea-tracks-coronavirus-patients-locations-using-phone-data-publishes-online.html. Acesso em: 22 mar. 2020.

[13] Health Insurance Portability and Accountability Act de 1996 – HIPAA, Disponível em: https://www.cdc.gov/phlp/publications/topic/hipaa.html. Acesso em: 22 mar. 2020.

[14] Disponível em: https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf. Acesso em: 22 mar. 2020.

enquanto seus casos estão sob investigação[15].

Nesse contexto, vale indagar: a divulgação dos dados pessoais, sem autorização do paciente, poderia ser direcionada às autoridades de saúde pública para impedir ameaças sanitárias?

A construção de possíveis respostas para a questão, para os fins deste artigo, deve ficar restrita à experiência brasileira. Temos a particularidade de que nossa Lei Geral de Proteção de Dados (LGPD) ainda se acha em *vacatio legis*, no que se refere aos direitos do titular dos dados e alcance da proteção legislativa[16]. Considerando o texto atual da Lei nº 13.709/18 e as projeções de que a pandemia perdurará por alguns meses, é possível que a entrada em vigor da LGPD ainda ocorra num cenário de crise na saúde.

Para quem vem se preparando para se adequar à nova legislação, deve-se destacar que a LGPD classifica como dados sensíveis (art. 5º, II) aqueles que são referentes à saúde e determina que seu tratamento (art. 11) somente poderá ocorrer quando o titular consentir, de forma expressa e destacada, para finalidades bem específicas.

Na sequência, são disciplinadas situações em que o tratamento dos dados sensíveis poderá ocorrer sem o consentimento do seu titular, tais como quando for indispensável ao cumprimento de obrigação legal ou regulatória, à execução de políticas públicas, à realização de estudos por órgão de pesquisa, à proteção da vida ou da incolumidade física do titular ou de terceiro e à garantia da prevenção à fraude e à segurança do titular, entre outras.

---

[15] Disponível em: https://wtov9.com/news/local/new-privacy-protocol-in-place-as-coronavirus-concerns-heighten. Acesso em: 22 mar. 2020.

[16] A LGPD foi publicada no DOU de 15.8.2018 e disciplina no seu art. 65 que seus artigos 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B entraram em vigor em 28 de dezembro de 2018. Quanto aos demais dispositivos, o inciso II do referido artigo estabelece prazo de dormência de 24 (vinte e quatro) meses após a data de sua publicação.

No ponto que interessa para a nossa reflexão, a LGPD também eximirá a necessidade do prévio consentimento quando estiver em evidência a tutela da saúde, exclusivamente em procedimento realizado por profissionais da área, serviços de saúde ou autoridade sanitária.

Mesmo sem a LGPD estar em vigor, é possível fundamentar a necessidade de proteção dos dados pessoais, na proteção conferida à intimidade e à vida privada das pessoas, consagrada no inciso X do art. 5º da Constituição Federal e reiterada no art. 21 do Código Civil, que assegura sua inviolabilidade e a possibilidade de se buscar tutela inibitória quando necessário.

Junte-se a isso a incidência do Marco Civil da Internet (Lei 12.965/14), para situações em que a coleta de dados ocorrer mediante utilização da rede mundial de computadores, pois entre os seus princípios encontramos a proteção da privacidade e a proteção dos dados pessoais (art. 3º), com a possibilidade de responsabilização dos agentes de acordo com suas atividades.

Em fevereiro de 2020 foi publicada a Lei n. 13.979/20, que dispõe acerca de medidas para o enfrentamento da emergência de saúde pública de importância internacional, decorrente do coronavírus. Em seu art. 6º, o referido diploma legal dispõe que é obrigatório o 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 coronavírus, com a finalidade exclusiva de evitar a sua propagação, estendendo tal obrigação às pessoas jurídicas de direito privado quando os dados forem solicitados por autoridade sanitária.

Também dispõe que o Ministério da Saúde manterá dados públicos e atualizados sobre os casos confirmados, suspeitos e em investigação, relativos à situação de emergência pública sanitária, resguardando o direito ao sigilo das informações pessoais. O art. 1º, nos parágrafos segundo e

terceiro, determina, ainda, que ato do Ministro de Estado da Saúde disporá sobre a duração da situação de emergência de saúde pública de que trata a lei, não podendo tal prazo ser superior ao declarado pela Organização Mundial de Saúde.

Nesse contexto, a Portaria 356/10 do Ministério da Saúde estipulou, em seu art. 12, que o encerramento da aplicação das medidas fica condicionado à avaliação de risco realizada pela Secretaria de Vigilância em Saúde do Ministério da Saúde sobre a situação de Emergência de Saúde Pública de Importância Nacional. Naturalmente, ainda não se sabe quanto tempo essa crise vai perdurar e, por conseguinte, por quanto tempo as medidas serão tomadas.

No que tange ao compartilhamento de dados, verifica-se que não há muita divergência em relação ao que prevê a LGPD, porquanto esta excepciona o acesso aos dados sensíveis, mesmo sem o consentimento, nos casos em que houver necessidade de tutela da saúde do titular ou de terceiros. Ademais, a nova legislação também dispõe que a utilização será restrita à finalidade de evitar a propagação do vírus e que, na hipótese de divulgação dos dados sobre casos confirmados, suspeitos e em investigação, será resguardado o direito ao sigilo das informações pessoais.

Da leitura dos dispositivos legais acima apontados, fica evidente que é indispensável compatibilizar a necessária proteção dos dados pessoais sensíveis, tais como informações relativas ao estado de saúde das pessoas, com o premente interesse público de adotar todas as medidas disponíveis para o combate da pandemia. Há de se prestigiar uma perspectiva de coexistência dos interesses em jogo e não de exclusão de qualquer dos polos da equação. Proteger o interesse coletivo não implica excluir a necessária proteção da pessoa natural, especialmente num estado de grave vulnerabilidade por esta acometida de uma nova doença ou pela mera suspeita de contágio, que já provoca abalos em seu bem-estar psíquico.

Diante de novos textos legislativos e de um contexto fático de crise que se altera muito rapidamente, ainda restam algumas preocupações a consignar. A Lei nº 13.979/20 determina que será obrigatório o compartilhamento de dados essenciais à identificação de pessoas infectadas ou com suspeita de infecção, sem elencar ou exemplificar quais dados seriam esses, o que ocasiona insegurança jurídica em relação ao titular, que pode ter uma universalidade de dados pessoais compartilhados sem que sequer tenha ciência disso.

O cenário caótico criado pela propagação do vírus tem acarretado cada vez mais a adoção de escolhas trágicas, que sacrificam interesses relativos à privacidade em prol da salvaguarda da saúde pública, optando-se por uma lógica de "tudo ou nada" que não se mostra adequada aos desafios de uma sociedade cada vez mais complexa. Não é preciso escolher soluções extremas sem levar em consideração princípios que há anos são desenvolvidos pela doutrina e jurisprudência e que foram incorporados ao texto da LGPD (art. 6º).

Qualquer atividade de tratamento de dados pessoais deverá observar a *boa-fé objetiva* e a *finalidade* do tratamento, vale dizer, sua realização, propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Apenas a finalidade não é suficiente. É preciso compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento, o que impõe a exigência de *adequação*.

Mesmo com tratamento adequado e existindo propósitos legítimos, ainda resta avaliar a *necessidade* do tratamento, que deve se limitar ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos. Considerando os dados pessoais como extensão dos direitos de personalidade da pessoa natural, devem-se garantir aos titulares dos dados informações claras,

precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (responsáveis pela coleta e utilização dos dados), como expressão da *transparência* que deve ser mantida em operações deste tipo.

Não se pode transigir quanto à impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. A lógica da *não discriminação* é inegociável e deve vir acompanhada da necessária *responsabilização* e *prestação de contas*, que ocorre com a demonstração, por parte do agente responsável pelo tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas, a fim de prevenir a ocorrência de danos, em especial aqueles decorrentes de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de informações pessoais.

No Brasil, a discussão sobre a privacidade ainda não chegou ao mesmo nível de profundidade dos outros países, tendo em vista que atualmente o aparato estatal não tem o mesmo grau de sofisticação para lograr objetivos massivos de vigilância.

Mas não se ignora que se trata de processo desafiador. A admissão de tais medidas como ferramenta para o salvamento de vidas não pode ser afastada, máxime no panorama de extrema incerteza em que a pandemia se situa e do elevado número de mortes já ocasionadas em razão do vírus. Deixar as tecnologias que temos inutilizadas em face de uma situação de calamidade pública parece não fazer muito sentido.

O mais importante é que não nos esqueçamos de impor balizas a essas medidas, seja em termos de duração, seja em termos de supervisão legal e utilização de modo uniforme das informações coletadas, para que posteriormente tais dados não sejam utilizados com outros fins e a situação de emergência não nos faça recair em posterior excesso.

Torna-se crucial, então, definir parâmetros de

transparência, principalmente quando da ocasião do envolvimento de empresas privadas do ramo tecnológico, que podem ver a oportunidade de, com espeque no argumento de eventuais avanços no combate ao vírus por meio do tratamento de dados, beneficiar-se nessa atividade num futuro próximo, sem possibilidade de se sindicar precisamente quais informações foram fornecidas durante o combate à pandemia.

A incógnita que se impõe é se as salvaguardas previstas na legislação atualmente em vigor, especialmente as leis e portarias criadas no momento da crise, serão suficientes para conter eventuais abusos que podem acontecer com o uso dos dados sensíveis num contexto de pós-pandemia.

Dados de localização, reconhecimento facial e rastreamento estão sendo utilizados como possíveis soluções para conter a difusão do vírus. O problema surge quando constatamos que, no meio de um cenário de tanto caos, é necessário parar para traçar fronteiras na utilização e no controle dessas ferramentas. O que será feito com esses dados após a contenção do surto?

Medidas de vigilância realmente são eficazes para limitar a propagação da patologia?

Os titulares terão ciência desse tratamento?

Como será feita a custódia?

São questionamentos que inquietam e que ainda não têm uma resposta formulada, sobretudo em razão da priorização estatal na resolução da crise pandêmica e da ausência de uma efetiva governança de dados no país, a despeito de mais de um ano de existência da Autoridade Nacional de Proteção de Dados.

Ocorre que não é incomum que situações extremadas de crise deem abertura à paulatina restrição de interesses jurídicos, sob o fundamento da necessidade de contenção de algum problema específico. Nesse ponto, eventos terroristas têm contribuído, por exemplo, com a consolidação de aparatos de

vigilância estatal[17].

O fundamento central da proteção dos dados pessoais, isto é, a autodeterminação informativa e o consentimento, cede espaço para a necessidade de contenção da pandemia, tendo em vista que a solicitação de autorização esbarraria em dificuldades operacionais e temporais que inviabilizariam a eficácia das medidas pretendidas.

Mesmo quando se analisa o art. 4º da LGPD, que afasta sua aplicação ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional ou atividades de investigação e repressão de infrações penais (ver inciso III), hipóteses que podem, por analogia, ser interpretadas para o contexto da pandemia, há de se destacar que as medidas adotadas nessas situações devem ser proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular, consoante preconiza o § 1º do referido artigo. Não fosse o suficiente, o § 2º do art. 4º da LGPD veda o tratamento de tais dados por pessoa de direito privado, salvo se ocorrer sob a tutela de pessoa jurídica de direito público, assegurado o acompanhamento da Autoridade Nacional de Proteção de Dados.

É necessário pensar em métodos razoáveis de segurança que impeçam acessos não autorizados, coleta, uso, divulgação, cópia, modificação, descarte ou riscos análogos, bem como a necessidade de interrupção do tratamento assim que seja razoável supor que o objetivo para o qual foram coletados não mais subsiste.

A situação se agrava ainda mais quando se constata que a pandemia é contemporânea ao que se chama de infodemia[18],

---

[17] Disponível em: https://noticias.uol.com.br/ultimas-noticias/efe/2019/10/08/macron-pede-uma-sociedade-da-vigilancia-contra-o-terrorismo.htm. (Acesso em: 21 mar. 2020/0 e em https://www.wired.com/2011/09/911-surveillance/ Acesso em: 21 mar. 2020.

[18] Disponível em: https://www.technologyreview.com/s/615184/the-coronavirus-is-

isto é, uma superabundância de informações que dificulta a localização de fontes e de orientações confiáveis àqueles que necessitam, especialmente num contexto digital repleto de *fake news.*

As aplicações tecnológicas atualmente disponíveis têm o potencial de rastrear localizações em tempo real ou metadados que demonstram padrões de comportamento e informações íntimas e que, uma vez admitidas na vida cotidiana, torna-se cada vez mais difícil afastá-las. Dessa forma, ainda que seja admissível a utilização dos dados pessoais, de modo excepcional, temporário e urgente, para a tutela da saúde pública, é fundamental que sejam priorizadas ações de pesquisa, diagnóstico e tratamento efetivos que forneçam ao sistema de saúde infraestrutura para zelar pelos pacientes e minimizar a ocorrência do vírus, sob pena de nos acomodarmos numa posição de vigilância, obsessão e assédio social que ameaça devassar a privacidade e segregar indivíduos.

As políticas públicas sempre devem buscar um equilíbrio entre as liberdades civis e o interesse coletivo, intentando primar pela proporcionalidade. Se a situação de calamidade traz ameaças que tornam legítima a restrição temporária e excepcional da privacidade, esta deve ser cientificamente justificada e proporcional às necessidades. Nossa saúde e nossa democracia dependem disso.

Neste ponto, é preciso dividir uma inquietação: é possível utilizar dados pessoais temporariamente para gerenciamento de crise sem acarretar, a longo prazo, uma erosão sistemática nas garantais fundamentais dos indivíduos? A resposta será construída nos próximos anos, depois que tivermos ultrapassado as graves consequências do período mais intenso da pandemia da COVID-19.

---

the-first-true-social-media-infodemic/. Acesso em: 22 mar. 2020.