Demócrito Reinaldo Filho: Prorrogação da LGPD é risco à sociedade

Edição extra do Diário Oficial da União foi publicada na noite do dia 29 de abril contendo o texto da Medida Provisória 959/2020, que prorroga a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) para o dia 3 de maio de 2021. A MP foi editada para facilitar o pagamento de benefícios instituídos como ajuda financeira para os brasileiros durante o período da pandemia do coronavírus — a Caixa Econômica Federal perde a exclusividade no pagamento dos benefícios, que agora podem ser recebidos também nas agências do Banco do Brasil —, mas destinou um único artigo para ampliar a)[1], que entraria em vigor em 16 de agosto deste ano.

A medida pegou a todos de surpresa, pois atropelou o

Congresso, onde tramita projeto de lei (PL 1179/2020), já aprovado pelo Senado e em análise na Câmara Federal, que prorroga a vigência da LGPD para janeiro de 2021 [2]. No dia 29, mesmo dia da publicação da MP, havia inclusive sido aprovado regime de urgência para tramitação do PL [3].

O adiamento da vigência da LGPD constitui *grave erro* e acentuado *risco* para a sociedade brasileira, no atual momento.

É bastante frágil o argumento de natureza econômica, utilizado pelos defensores da prorrogação da vigência da LGPD. Alega-se que as empresas brasileiras não tiveram tempo de se adaptar à lei e ainda serão obrigadas a realizar despesas para se adequar às suas exigências. Sobrecarregá-las num momento desses, em que se inicia uma recessão econômica profunda, como decorrência da crise de saúde, vai dificultar a recuperação da economia brasileira. As empresas terminarão sofrendo com as pesadas multas previstas na nova LGPD, inviabilizando a recuperação em tempos extremamente difíceis, concluem.

Essa visão não espelha a realidade, do ponto de vista jurídico. As empresas não deixarão de ser responsabilizadas pelos danos que causarem por manipulação ou uso indevido de dados pessoais durante o período da pandemia. O nosso ordenamento jurídico já dispõe de diversos instrumentos normativos que atribuem responsabilização por danos causados a consumidores de produtos e serviços. A Constituição, o Código Civil (Lei nº 10.406/2002), o CDC (Lei 8.078/90), o Marco Civil da Internet (Lei nº 12.965/2014) e a Lei 12.414/2011 (que disciplina bancos de dados com informações de crédito) são suficientes para atribuir dever de reparação por danos causados por qualquer empresa que, no desenvolvimento de atividade de tratamento de dados, cause danos a consumidores ou terceiros. Em caso de vazamento de informações, manipulação indevida de dados de saúde, compartilhamento não autorizado de dados ou qualquer acidente informacional, que ocorra durante o período ou logo após a pandemia, o controlador não conseguirá fugir à responsabilização pelos danos causados (quer sejam de ordem material ou moral). Poderá ser responsabilizado na esfera judicial e também sofrer a imposição de multas. É bom não esquecer que o artigo 12, II (c/c artigo 11), do Marco Civil (Lei nº 12.965/2014) prevê *"multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício"*, por acidente que ocorra "*em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet"*. Com base no Marco Civil e no CDC, o Procon-SP multou ano passado a Google e a Apple em R$ 10 milhões e R$ 7,7 milhões, respectivamente, pela distribuição de um aplicativo que compartilhava os dados dos usuários com terceiros [4].

As empresas tiveram, sim, tempo para se adaptar e conhecer o conteúdo da LGPD. O projeto de lei tramitou durante anos no congresso nacional até se transformar na Lei nº 13.709/2018 e, antes mesmo da iniciativa legislativa, o debate sobre a proteção de dados pessoais no Brasil já se tinha iniciado sob a coordenação do Ministério da Justiça. O prazo de *vacatio legis* estipulado inicialmente já foi bastante extenso —— de 18 meses a partir da publicação da lei [5]. Depois, foi estendido para 24 meses [6] e agora a MP o alongou para 32 meses e 18 dias. Nem códigos inteiros tiveram prazo de *vacatio* tão amplo. Se a prorrogação estipulada na MP 959/2020 for mantida, a LGPD se tornará a lei de maior *vacatio legis* na história do país, desde a instituição da República.

Com a prorrogação da vigência da LGPD, as empresas continuarão a ser responsabilizadas, mas com base em legislação não especializada (em proteção de dados pessoais). Os intérpretes e julgadores trabalharão com princípios e normas mais abstratas, gerando mais insegurança jurídica. Por isso é muito importante para as próprias empresas, que desenvolvem atividades de tratamento de dados, que a LGPD entre em vigor. A nova LGPD traz diversos conceitos e estabelece os limites para uso dos dados pessoais. Assegura mais transparência e dá mais segurança para os controladores de sistemas informatizados, ao indicar as situações em que *dados sensíveis* podem ser tratados e para quais finalidades. No período da pandemia, é fundamental para o setor público e o setor privado poder contar com texto legal que esclareça o que pode e o que não pode ser feito em termos de coleta e processamento de dados de saúde. Postergar a entrada em vigor da LGPD nos deixará em um ambiente de insegurança jurídica, o que é pior para os negócios do que a própria pandemia.

No período da pandemia os mecanismos e ferramentas de vigilância disseminam-se numa velocidade nunca antes experimentada [7]. Para combater a expansão do coronavírus, empresas privadas estão desenvolvendo sistemas de monitoramento e realizando vasta coleta de informações pessoais. Assistimos a uma proliferação de aplicativos [8] e plataformas de coleta de dados de saúde, sem prévia autorização de órgãos sanitários ou teste de condições de segurança, proteção de dados e eficácia [9]. Dados de geolocalização estão sendo utilizados para mapeamento da concentração de pessoas e controle dos movimentos [10]. A privacidade das pessoas está em risco como nunca esteve antes, pois empresas privadas adquiriram o discurso que lhes faltava para se apropriar dos dados de saúde: o combate à pandemia.

Uma legislação para a proteção de dados é necessária para estabelecer as bases e limites do tratamento de dados, como atividade necessária para uma adequada biopolítica de combate à pandemia. Sem ela, as consequências nefastas da biovigilância serão sentidas no futuro, quando talvez não se tenha como revertê-las. Se as ferramentas de vigilância em massa (*mass surveillance*) proliferarem sem limites ou supervisão regulatória adequada, estaremos criando uma *doença social* muito maior e com efeitos inimagináveis para a sociedade futura.

A emergência da situação atual não significa que devamos sacrificar a privacidade. Proteção de dados e garantia da privacidade individual não são medidas incompatíveis com o combate à pandemia. Muito pelo contrário. As leis de proteção de dados que seguem o modelo europeu — como a nossa LGPD — são talhadas para lidar com situações como uma pandemia, inclusive dispensando o consentimento do titular dos dados quando for necessário à tutela da saúde [11]. Uma coisa não é excludente da outra. Pode-se combater a expansão da doença sem causar efeitos colaterais mais perversos, respeitando-se as normas de proteção de dados pessoais. Não é correto expandir os tentáculos da vigilância em nome da "saúde pública", com atividades de coleta e processamento de dados de forma massiva, sacrificando valores sociais e liberdades fundamentais. A tecnologia pode ser utilizada para a execução de políticas públicas, mas de maneira proporcional e suficiente para controlar a expansão do vírus, sem imolar a privacidade das pessoas.

Durante o período da pandemia, temos que ter equilíbrio suficiente para não descuidar do nosso futuro, da sociedade que vai emergir em seguida. Se não quisermos a construção das bases de uma *sociedade de controle*, em que cada pessoa é vigiada constantemente e seus dados são utilizados para fins comerciais e de controle comportamental, é preciso não ceder ao ímpeto de vulgarizar a proteção da privacidade. A humanidade experimenta um período sofrido e angustiante, mas a pandemia vai passar, ainda que deixe um rastro de dor e empobrecimento geral de parte da população. Outros países já controlaram a expansão do vírus e retomam as atividades sociais regulares. Não há dúvida de que o Brasil também passará a essa nova fase, ainda que com mais dificuldades por conta dos desníveis sociais que caracterizam nosso país. As políticas de combate ao vírus são conhecidas e irão fazer efeito, num prazo mais ou menos curto (dependendo do grau de acerto dos nossos governantes). Portanto, no momento nossos olhos devem estar voltados para o *day after*, o estilo de vida e as liberdades que queremos usufruir no amanhã.

A maior resistência às leis de proteção de dados provém das gigantes empresas de tecnologia, que consolidaram o que se convencionou chamar de "capitalismo de vigilância" — a nova forma de capitalismo que monetiza dados adquiridos por vigilância [12]. O mundo *online* é agora onde o capitalismo desenvolve novos mercados e obtém os meios para produzir novos serviços e produtos, através da extração de dados. Os dados são a nova forma de capital, no mesmo nível do capital financeiro, em termos de geração de novos produtos e serviços digitais. O capitalismo ficou focado na coleta e processamento de dados, usando mecanismos ilegítimos de mercantilização e controle de comportamento, com implicações significativas para a liberdade das pessoas e vulnerabilidade da privacidade individual. Somente as grandes corporações do setor tecnológico têm estrutura para monopolizar as atividades de coleta, processamento e armazenamento de dados em larga escala, gerando intensas concentrações de poder que ameaçam núcleos de valores como a liberdade e privacidade. Como protagonistas dessa nova espécie de capitalismo, as *Big Techs* reagem a qualquer iniciativa regulatória que considerem ameaça ao núcleo de suas atividades e, portanto, ao seu modelo lucrativo de negócios.

As poderosas empresas de tecnologia já controlam dados sobre nossos hábitos de consumo, nossos movimentos, nossas interações sociais, nossas preferências políticas e ideológicas, nossas finanças e histórico de crédito, e agora querem nossos *dados de saúde*. Como se disse, os dados são hoje o mais valioso recurso para a economia capitalista, a mais importante fonte de riqueza para as organizações. Mas não se pode permitir que dados sensíveis (dados de saúde) de milhões de brasileiros sejam apoderados por empresas privadas, sem qualquer supervisão ou limitação.

O atual momento justifica inclusive um aperfeiçoamento e reforço da legislação de proteção de dados, nunca um esvaziamento regulatório. As garantias de proteção à privacidade precisam ser constantemente atualizadas e reforçadas numa sociedade completamente dependente dos dados (*data-driven society*). No meio de uma crise de saúde pública que traz junto uma situação de ameaça à privacidade individual — em razão da coleta e uso indiscriminado de dados pessoais por ferramentas tecnológicas —, os governos devem adotar medidas para reforçar suas legislações, estabelecendo novas limitações e obrigações para os controladores de sistemas informatizados.

O Brasil caminha no sentido oposto ao de outros países, que estão reforçando ou atualizando suas legislações de proteção de dados. A pandemia do coronavírus tem servido como fator catalisador de esforços legislativos para elaboração e aperfeiçoamento de legislação de proteção à privacidade, e não o contrário. No último dia de abril, quatro senadores republicanos apresentaram no Senado dos Estados Unidos um projeto de lei para responsabilizar empresas pelo uso inadequado de dados de saúde, de geolocalização e outras informações utilizadas para combater a pandemia do coronavírus. O senador Roger Wicker, um republicano que representa o Estado do Mississippi e preside o Comitê do Comércio, juntamente com mais três senadores, patrocina o *Covid-19 Consumer Data Protection Act*, legislação que pretende atribuir aos cidadãos norte-americanos mais controle sobre seus dados de saúde e dados de geolocalização e de proximidade, que hoje estão sendo coletados e usados por ferramentas tecnológicas para conter o vírus [13]. Até autoridades da China, considerado um regime fechado e que desenvolveu um aparato de vigilância estatal, adotaram medidas de proteção de dados durante a pandemia. No início de fevereiro (dia 3), a Comissão Nacional de Saúde da China publicou documento indicando requisitos para a proteção de dados no contexto da Covid-19. O órgão responsável pela política de cibersegurança publicou, no dia seguinte, uma circular contendo diretrizes para assegurar proteção das informações pessoais durante o período da pandemia [14].

Como observa, a pandemia do coronavírus serviu como gatilho, em diversas localidades do globo, para que os legisladores tomassem consciência da importância de se preservar a privacidade no momento da crise de saúde e galvanizou esforços para iniciativas legislativas de adaptação e reforço das leis de proteção de dados. Aqui no Brasil, com a edição da MP 959/2020, andamos em sentido oposto, relegando a proteção dos *dados de saúde* dos brasileiros, em momento em que a privacidade está sob risco acentuado.

As empresas de tecnologia sempre tentaram avançar no setor de saúde pública, por meio de parcerias com hospitais e universidades, mas sofriam grande resistência por conta da natureza dos dados que poderiam recolher com iniciativas nessa área. Agora conseguiram na pandemia da Covid-19 o discurso que lhes faltava. No Brasil, sem a LGPD e sem a instalação da Agência Nacional de Proteção de dados (ANPD), será fácil abocanharem o último nicho que lhes era negado. O "capitalismo de vigilância" finalmente se apodera dos dados de saúde!

[1] Artigo 4º A Lei nº 13.709, de 14 de agosto de 2018 passa a vigorar com as seguintes alterações:

"Artigo 65…….

……

II – em 3 de maio de 2021, quanto aos demais artigos." (NR)

[2] O PL 1179/2020 cria o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19), e, entre outras medidas, adia a vigência da LGPD para janeiro de 2021 e a aplicação de multas e sanções para agosto de 2021.

[3] Cf. notícia publicada no site *Convergência Digital*, em 30/4/20, acessível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/startigohtm?UserActiveTemplate=site&infoid=5

[4] Ver notícia no *G1*, publicada em 30/8/19, acessível em: https://g1.globo.com/sp/sao-paulo/noticia/2019/08/30/procon-sp-aplica-multas-milionarias-em-google-a-apple-por-aplicativo-que-envelhece-rostos.ghtml

[5] A Lei Geral de Proteção de Dados foi sancionada em 14 de agosto de 2018, publicada no Diário Oficial da União em 15 de agosto de 2018, e republicada parcialmente no mesmo dia, em edição extra. O início da vigência seria em 18 meses desde a publicação.

[6] A Lei 13.853/19 modificou o inc. II do artigo 65 da Lei 13.709/18, prevendo a entrada em vigor desta última em 24 meses após a data de sua publicação.

[7] A esse respeito, sugerimos a leitura de nosso artigo “COMO OS PAÍSES ASIÁTICOS UTILIZAM A TECNOLOGIA PARA COMBATER A EPIDEMIA DO CORONAVÍRUS – A transição do 'capitalismo de vigilância' para a 'vigilância totalitária'"?, publicado na **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 25, nº 6120, 3 abr. 2020. Disponível em: https://jus.com.br/artigos/80616

[8] Muitos desses aplicativos estão sendo distribuídos nas “lojas” (plataformas de distribuição) das grandes empresas de Internet, como a *App Store* (da Apple) e a *Google Play* (da Alphabet).

[9] Sugerimos a leitura de nosso artigo “RASTREAMENTO DE CONTATOS MEDIANTE APLICATIVOS: proposta de um modelo para o Brasil na nova fase de combate ao coronavírus”, artigo publicado no site Juristas, em 24 de abril de 2020, acessível em: https://juristas.com.br/2020/04/24/rastreamento-contatos-auxilio-aplicativos/

[10] Para entender como os dados de geolocalização podem ser utilizados na política de enfrentamento ao coronavírus, sugerimos a leitura de nosso artigo “A UTILIZAÇÃO DE DADOS DE GEOLOCALIZAÇÃO NO COMBATE À PANDEMIA DO CORONAVÍRUS – A necessidade de adoção de salvaguardas regulatórias, publicado na Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 25, nº 6116, 30 mar. 2020. Disponível em: https://jus.com.br/artigos/80679

[11] O artigo 11, II, f, da LGPD (Lei 13.709/2018), admite o tratamento de dados sensíveis mesmo sem o consentimento do titular, quando a atividade for necessária para “tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária”.

[12] Capitalismo de vigilância (*surveillance capitalism*) é um termo usado e popularizado pela acadêmica Shoshana Zuboff, que denota um novo gênero de capitalismo que monetiza dados adquiridos por vigilância. Para quem se interessar mais pelo tema, sugerimos a leitura de seu livro "Big other: surveillance capitalism and the prospects of an information civilization" (Social Science Research Network. Journal of Information Technology. 2015).

[13] Ver notícia publicada no site especializado em assuntos legais Law360, sob o título “Sens. float Privacy Bill to protect data in COVID-19 era”, em 30.04.20, acessível em: https://www.law360.com/technology/articles/1269228/sens-float-privacy-bill-to-protect-data-in-covid-19-era?nl_pk=df30baa8-1fc8-4548-8460-1e2ae87982e5&utm_source=newsletter&utm_medium=email&utm_campaign=technology

[14] Ver notícia publicada sob o título "Personal data protection in the time of coronavirus (Covid-19)" , em 25/2/ 20, acessível em: https://www.dataprotectionreport.com/2020/02/personal-data-protection-in-the-time-of-coronavirus-covid-19/

Date Created
15/05/2020