

A LGPD E SUA APLICAÇÃO AO PODER PÚBLICO: UMA ANÁLISE SOBRE A IMPLANTAÇÃO DO SISTEMA DE MONITORAMENTO INTELIGENTE DE SÃO PAULO

Pedro de Alcântara Ribeiro Vilanova Júnior¹

SUMÁRIO: 1. Introdução; 2. Do regime jurídico de proteção de dados na era da informação. 3. Do tratamento de dados pessoais pela Administração e a realização do interesse público. 4. O Sistema de Monitoramento Inteligente do Governo de São Paulo e a aplicação da LGPD. 5. Conclusões. Referências.

RESUMO: O presente artigo tem como objetivo trazer considerações acerca das disposições da Lei Geral de Proteção de Dados – (LGPD – Lei nº 13.709, de 14 de agosto de 2018) e sua aplicação no Poder Público dentro de um contexto de constante inovação tecnológica. Com efeito, a chamada Era da Informação tornou fundamental a criação de regime legal sobre o processo de tratamento de dados pessoais. Não estando o Poder Público alheio a esse processo, deve estar atento à necessidade de adaptação às disposições da LGPD, destacando-se a essencialidade da advocacia pública nesse processo. Por fim, busca-se realizar uma análise de caso acerca da implementação do Sistema de Monitoramento Inteligente do Governo de São Paulo (SIMI-SP) e sua compatibilidade com as previsões da LGPD.

Palavras-chave: Tratamento de Dados Pessoais. Poder Público. LGPD. Era da Informação. Direito à Privacidade.

1 Procurador do Estado de São Paulo. Pós-graduando em Direito do Estado pela Escola Superior da Procuradoria-Geral do Estado de São Paulo.

1. INTRODUÇÃO

A sociedade moderna passa por um intenso processo de revolução tecnológica. Se, por um lado, tal marcha trouxe inúmeras facilidades ao bom desenvolvimento do convívio social e de produção de bens, por outro, o imenso fluxo de informação traz à tona a discussão sobre o controle de acesso e armazenamento dos dados transmitidos. Soma-se isso ao fato de que, cada vez mais, torna-se essencial a utilização de ferramentas virtuais, seja no âmbito pessoal, seja no contexto profissional e na Administração Pública. Constata-se uma tendência de substituição das relações – inclusive jurídicas – do suporte físico para o meio eletrônico, com velocidade de transmissão de conteúdo até então inimagináveis.

O intenso fluxo desses dados encontra-se comumente ligado a informações de índole pessoal, relacionando-se ao direito de intimidade e privacidade. Tais dados pessoais podem dizer respeito à vida pública, privada ou profissional do indivíduo, por meio do armazenamento de informações como fotos, vídeos, interações em redes sociais, deslocamentos captados pelo Sistema de Posicionamento Global (GPS), dentre vários outros meios, de modo que, mesmo sem identificação prévia do titular de tais dados, é possível falar-se em indivíduo identificável por meio da conjugação de sistemas de bancos de dados. As frequentes inovações tecnológicas possibilitam o desenvolvimento de *softwares* e computadores que são capazes de captar, armazenar e transmitir vultosa quantidade de dados pessoais com fins mercadológicos.

Ocorre que, quando se fala em captura e armazenamento de dados pessoais, muito se pensa em grandes corporações internacionais, que utilizam tais informações como produto no mercado, para obtenção de lucro. Não obstante esse enfoque seja de suma importância, destaca-se neste ensaio outro grande armazenador de dados pessoais: a Administração Pública, que, em tempos de moderna governança, captura, armazena e dispõe dos dados pessoais dos administrados.

Dentro deste debate, o presente ensaio pretende trazer reflexões acerca da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709, de 14 de agosto de 2018), e sua aplicação no Poder Público, que, seguindo a trilha da experiência internacional, tem por objetivo regulamentar o interdisciplinar tema do tratamento de dados pessoais.

Além disso, pretende-se realizar o estudo do caso da implementação do Sistema de Monitoramento Inteligente do Governo de São Paulo (SIMI-SP), desenvolvido com vistas à observação dos índices de isolamento social e definição da estratégia de

prevenção e combate à pandemia do coronavírus, por meio do Instituto de Pesquisas Tecnológicas (IPT), a fim de avaliar sua compatibilidade ao regramento legal de proteção de dados.

2. DO REGIME JURÍDICO DE PROTEÇÃO DE DADOS NA ERA DA INFORMAÇÃO

O professor de governança e regulação Viktor Mayer-Schönberger descreve a existência de quatro gerações referentes ao regime de proteção de dados. A primeira geração de normatividade era ligada a leis que buscavam refletir o então atual estágio da tecnologia, e tinha por finalidade apenas tratar da concessão de autorização para a criação de bancos de dados e do seu controle posterior pelos órgãos públicos².

Posteriormente, a chamada segunda geração teve como grande expoente a Lei Federal da República da Alemanha sobre a proteção de dados (*Bundesdatenschutzgesetz*), de 1977, e a lei francesa de 1978, nomeada de “*informatique et libertés*”, que tinham como foco mais a proteção da privacidade do que os fenômenos computacionais em si. Destaca-se, ainda nesse contexto, a decisão do Tribunal Constitucional da Alemanha Ocidental, em 1983, que declarou inconstitucional a lei que criava um censo estatístico e determinava a coleta de dados pessoais dos usuários para otimização de políticas públicas. Lecionam Regina Linden Ruaro, Daniel Piñeiro Rodriguez e Brunize Finger sobre a pioneira decisão judicial:

Este acontecimento é considerado o marco oficial em que surge da autodeterminação informativa, que seria, segundo a sentença, os direitos dos indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados. A partir desta ideia, o sujeito passa a poder decidir quando e sob que circunstâncias poderão dar conhecimento de seus dados pessoais.³

Uma terceira geração surge na década de 1970, indo além do foco de fornecimento ou não dos dados pessoais, mas visando à garantia da efetividade da liberdade de escolha, demandando efetiva participação do indivíduo e a autodeterminação informativa.

2 MAYER-SCHÖNBERGER, Viktor. 1997. apud MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital: Direito Privado e Internet*. 4. ed. Indaiatuba: Editora Foco, 2021, p. 42.

3 RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito da UFPR, Curitiba*, 2008, n. 47, p. 29-64.

Por fim, destaca-se o regime legal da quarta geração, que teve como expoente a Diretiva 95/46/CE do Parlamento Europeu, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à sua livre circulação. Tal geração caracteriza-se pela constatação de que o enfoque meramente individual da proteção de dados ignora a manifesta desvantagem do indivíduo perante as entidades que fazem a coleta dos dados pessoais. Desse modo, se propõe a dirimir tais desvantagens, buscando formatar instrumentos que elevem o próprio padrão coletivo de proteção.

O histórico do regime de proteção de dados pessoais reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto a sua adequação às novas tecnologias de informação⁴. Assim, tal proteção vai se moldando à medida que a capacidade de recolher, processar e utilizar informações se amplia de forma exponencial. Acerca da mudança de paradigma na captação de dados com o avanço tecnológico, Márcio Rafael Silva Laeber já alertava:

O desenvolvimento tecnológico permitiu a substituição das antigas fichas cadastrais manuais por arquivos eletrônicos que, dispostos em poderosos computadores e tratados por poderosos programas, são capazes de cruzar informações pessoais com precisão e eficiência jamais vistas.

A evolução acelerada da informática e da telemática derrubaram fronteiras geográficas no transporte da informação, mormente com o surgimento da internet, permitindo, em curto espaço de tempo, relacionar dados contidos em diferentes bancos de dados em diferentes locais do mundo.⁵

O compartilhamento de dados, incluídos os pessoais, tem alcançado, com o avanço tecnológico, patamares inimagináveis. A coleta e tratamento têm ocorrido tanto em casos de fornecimento explícito, quando o indivíduo compartilha informações ou dados em mídias sociais, como também de forma implícita, por meio do consentimento realizado em termos de uso de política de privacidade de plataformas digitais ou de preenchimento de cadastros e criação de contas em aplicativos, *e-mails*, *e-commerce* e, até mesmo, por intermédio da chamada *Internet of Things* (IoT – “Internet das Coisas”), cuja interação tecnológica entre os indivíduos e seus bens gera lastro informativo a ser armazenado em bancos de dados digitais⁶.

4 DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral da Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia, 2006.

5 LAEBER, Márcio Rafael Silva. Proteção de dados pessoais: o direito à autodeterminação informativa. *Revista de Direito Bancário e do Mercado de Capitais*, São Paulo, v. 37, 2007.

6 AGUDO, Hugo Crivilim; TEIXEIRA, Tarcisio. As limitações da utilização de mecanismos de big data à luz da lei geral de proteção de dados pessoais. In: TEIXEIRA, Tarcisio; MAGRO, Américo Ribeiro. (Coord). **Proteção de dados: Fundamentos jurídicos**. 2. ed. Salvador: Editora JusPodivm, 2022, p. 229-265.

Nesse cenário, qualquer interação realizada em meio digital deixa informações que constituem bancos de dados, armazenados em plataformas e *softwares* a serem utilizados para as mais diversas finalidades, desde mercantil até comportamental.

No atual estágio de desenvolvimento tecnológico, tais bancos de dados, armazenados em determinada plataforma, são constantemente cruzados entre si. De modo que, além de gerar novas informações, geram um novo e gigantesco banco de dados online cujos conhecimentos comportamentais e de conhecimentos pessoais dos usuários alcançam patamares de difícil mensuração.

A este conjunto de informações, cruzadas entre si de forma fragmentada ou não, que formam tal imensurável banco de dados online, dá-se o nome de *Big Data*. Buscando conceituar tal instituto, dispõe a especialista espanhola Elena Gil González:

Big data es un término que alude al enorme crecimiento en el acceso y uso de información automatizada. Se refiere a las gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos. No es una tecnología en sí misma, sino más bien un planteamiento de trabajo para la obtención de valor y de beneficios como consecuencia del tratamiento de los grandes volúmenes de datos que se están generando día a día.⁷

Dentro desse contexto, a preocupação com o tratamento legal do processo de criação de bases de dados e a coleta, armazenamento e tratamento de informações pessoais denota tendência internacional, refletida no Brasil nos últimos anos. Com a aprovação do Marco Civil da Internet (Lei nº 12.965/2014), adentram ao ordenamento brasileiro as expressões “proteção da privacidade” e “proteção dos dados pessoais”, que são consagradas como princípios expressos da disciplina do uso da internet no Brasil. A normativa, entretanto, deixou de apresentar adequado regime jurídico sobre o tratamento de dados coletados, conforme discorre Thiago Vieira de Souza:

Em 2014, o Marco Civil da Internet entrou em vigor no Brasil, estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no país. Foi uma forma de reconhecer e regulamentar as novas relações jurídico-virtuais, em razão da existência de inúmeros usuários e provedores, bem como de empresas que trabalham online, dado que grande parte não estava adaptada à nova realidade digital. O MCI trata dos delitos praticados online (crimes cibernéticos) e da neutralidade da rede, estabelecendo direitos e garantias para liberdade de expressão, e, apesar de cuidar

7 GONZÁLEZ apud DONEDA, 2006, *op. cit.*

da privacidade, acabou restando uma lacuna sobre o tratamento de dados pessoais, pois não foi dada a devida atenção ao seu uso, destino, comercialização etc.⁸

Com o objetivo de conferir adequado regime jurídico ao tratamento de dados pessoais, foi aprovada a LGPD (Lei nº 13.709, de 14 de agosto de 2018). O novo marco representa tanto uma maior preocupação com a proteção de dados pessoais, quanto uma constatação de que o resguardo eficaz do indivíduo na era da informação está mais ligado a um padrão coletivo de proteção que a uma mera participação individual no aceite da transmissão dos dados pessoais. Nesse sentido:

Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre “recolhimento” e “divulgação”; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a “casa fortaleza”, que glorifica a privacidade e favorece o egocentrismo, e a “casa vitrine”, que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem.⁹

Nesse sentido, mais do que a titularidade dos dados pessoais transmitidos, a LGPD visa à garantia da possibilidade de monitoramento do titular acerca de suas informações, bem como sobre sua destinação e utilização.

O marco legal visa dar concretude ao mandamento constitucional esculpido no artigo 5º, inciso X da Constituição da República, que consagra o direito à inviolabilidade, à vida privada, à honra e à imagem. Tal direito à intimidade perfaz-se, especialmente, na possibilidade de manter determinados dados pessoais sensíveis sob sigilo. Nesse sentido:

Mais do que a titularidade dos dados pessoais, o que a LGPD pretende garantir é o domínio e a possibilidade de monitoramento do titular sobre os seus dados pessoais e sobre os tratamentos que sobre eles são realizados. Esses direitos do titular de acesso aos seus dados pessoais, de conhecimento de seus dados pessoais e

8 SOUZA, Thiago Vieira de. *A proteção de dados pessoais como direito fundamental e a [in]civildade do uso de cookies*. 2018. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal de Uberlândia, Uberlândia, 2018.

9 RODOTA, 2018, apud COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. *Revista Brasileira de Direito Civil em Perspectiva*, Belém, 2019, v. 5, n. 2, p. 22-41. Disponível em: <https://www.indexlaw.org/index.php/direitocivil/article/view/5778/pdf>. Acesso em: 20 out. 2020.

de controle sobre tratamento de seus dados pessoais passam a integrar a categoria dos direitos da personalidade.

Desse modo, a LGPD foi aprovada com 65 artigos, visando à regulação direta ou indireta da proteção da privacidade e dos dados pessoais, trazendo disposições acerca do tratamento de dados de pessoas naturais e jurídicas de direito público ou privado, por meio físico ou digital, buscando garantir a tutela dos dados com fundamento na privacidade, autodeterminação informativa, liberdade de expressão, de informação, de comunicação e de opinião.

3. DO TRATAMENTO DE DADOS PESSOAIS PELA ADMINISTRAÇÃO E A REALIZAÇÃO DO INTERESSE PÚBLICO

A LGPD dedica todo o capítulo IV à disposição acerca do tratamento de dados pessoais pelo Poder Público, estabelecendo que deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Dispõe, ainda, como condições para tal tratamento, que sejam informadas pela pessoa jurídica detentora as hipóteses em que realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, bem como que seja indicado um encarregado pelo tratamento quando realizadas operações de dados pessoais.

Seguindo tal linha de controle das operações realizadas, o artigo 50 do diploma legal estabelece a necessidade de implantação de “Boas Práticas e de Governança” pelos agentes de tratamento (controladores e operadores) de dados pessoais. Estabelece, ainda, que, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para seus respectivos titulares, o controlador poderá implementar programa de governança em privacidade, prevendo, ainda, requisitos mínimos para este.

Destaca-se que, não obstante a utilização da expressão “poderá”, que, a princípio indicaria uma faculdade, há entendimento de que tal previsão constitui um dever do Poder Público como controlador de dados pessoais. Nesse sentido, dispõe André Luiz Bäuml Tesser:

Assim, embora o verbo utilizado pelo legislador (“poderá”) pareça indicar uma mera possibilidade, não parece haver dúvidas de que essa é uma obrigação do Poder Público enquanto controlador dos dados, em especial em razão da sensibilidade dos dados tratados, do volume de operações nesse sentido e da própria potencialidade dos danos que podem ser causados aos titulares.¹⁰

Em que pese respeitado entendimento, a conclusão mais adequada do dispositivo parece não ser no sentido de obrigatoriedade apriorística em todo e qualquer caso de tratamento de dados pela Administração. Isso porque o Poder Público lida com o tratamento de dados pessoais sob diversas óticas, bem como por diversos órgãos de seu ordenamento, de diferentes realidades estruturais, de modo que a aplicação dos requisitos de sensibilidade dos dados tratados e a probabilidade e gravidade dos danos para seus titulares deverão ser sopesados dentro da hipótese concreta.

O regramento dispõe, ainda, sobre alguns conceitos relacionados ao tratamento de dados pela Administração. Primeiramente, traz a definição de órgão de pesquisa (artigo 5º, XVIII) como institutos de pesquisa da:

Administração Pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituídas sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.¹¹

Mais à frente, o artigo 7º da LGPD estabelece um rol taxativo de hipóteses em que será permitido realizar o processamento de dados pessoais. Para os fins desta pesquisa, importa destacar o disposto no inciso III, que traz a hipótese de utilização de dados “pela Administração Pública para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres”.

Importante, aqui, fazer remissão ao disposto no art. 5º, X, que determina que tratamento é qualquer “operação realizada com dados pessoais”. A lei, portanto, traz conceito deveras amplo, que envolve todas as transações tais informações particulares, desde a coleta delas, passando pelo seu armazenamento, até o seu descarte.

10 TESSER, André Luiz Bäuml. Premissas fundamentais de um adequado e efetivo programa de privacidade e proteção de dados pessoais na administração pública: uma análise das necessidades e possibilidade a partir da LGPD. In: PIRONTI, Rodrigo. (Coord.). *Lei Geral de Proteção de dados no Setor Público*. Belo Horizonte: Fórum, 2022.

11 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados (LGPD)*. Brasília, DF: Presidência da República [2020]. Casa Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 mai. 2022.

Conforme disposto no artigo 26, o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da Lei.

Veja-se, portanto, que o tratamento de dados pessoais pela Administração está intimamente ligado ao conceito de execução de políticas públicas. Essas podem ser definidas como programas de ação governamental que buscam coordenar os meios que estão à disposição do Estado para a concretização de objetivos socialmente relevantes e politicamente determinados, normalmente relacionadas à materialização de direitos sociais constitucionalmente assegurados¹². Do próprio conceito invocado, depreende-se a tutela finalística a que se dirige uma política pública, trazendo em si a ideia de uma ação a ser executada com vistas à realização do bem comum.

Assim, o regramento parte da dicotomia de interesse público e privado, refletida no sacrifício, em certa medida, do direito individual à intimidade, consagrado constitucionalmente, em prol da necessidade de compartilhamento de dados pessoais para fins de instrumentalizar política pública prevista em lei ou regulamento, com fim último na realização do interesse público. Sobre tal dicotomia, Maria Sylvania Zanella Di Pietro discorre que:

As normas de direito público, embora protejam reflexamente o interesse individual, tem o objetivo primordial de atender ao interesse público, ao bem-estar coletivo. Além disso, pode-se dizer que o direito público somente começou a se desenvolver quando, depois de superados o primado do Direito Civil (que durou muitos séculos) e o individualismo que tomou conta dos vários setores da ciência, inclusive a do Direito, substituiu-se a ideia do homem com fim único do direito (própria do individualismo) pelo princípio que hoje serve de fundamento para todo o direito público e que vincula a Administração em todas as suas decisões: o de que os interesses públicos tem supremacia sobre os individuais.¹³

Certo é que, apresentada tal dicotomia, cabe ao legislador, em abstrato, ou ao administrador, frente ao caso concreto, ter por finalidade alcançar solução ótima que realize ao máximo cada um dos interesses públicos em jogo, tendo por balizas as circunstâncias peculiares do caso posto, assim como os valores constitucionais

12 CARVALHO, Cláudio Oliveira de. Políticas Públicas e Gestão Urbana Ambiental. *Revista de Direito Ambiental*, São Paulo, v. 26, n. 7, p. 277-289, 2002.

13 DI PIETRO, Maria Sylvania Zanella. *Direito Administrativo*. 19ª. edição. São Paulo: Editora Atlas, 2006.

aplicáveis. Por meio desse exercício de ponderação, tem-se aquilo que se pode nomear de melhor interesse público, ou seja, o fim legítimo que orienta a atuação da Administração Pública¹⁴.

Dessa forma, a realização do interesse público não significa, em caso de aparente conflito, necessariamente a subjugação integral do interesse privado. A realização deste também deve ser buscada em um processo de ponderação que possibilite a realização dos interesses envolvidos na maior extensão possível.

4. O SISTEMA DE MONITORAMENTO INTELIGENTE DO GOVERNO DE SÃO PAULO E A APLICAÇÃO DA LGPD

Em 30 de janeiro de 2020, a Organização Mundial de Saúde (OMS) declarou que o surto do novo coronavírus constituía Emergência de Saúde Pública de Importância Internacional (ESPII). Ato contínuo, no âmbito do Estado de São Paulo, foi publicado o Decreto nº 64.879, de 20 de março de 2020, que reconheceu o estado de calamidade pública, decorrente da pandemia de COVID-19 no estado.

Certo é que, desde 27 de fevereiro de 2020, com a criação do Centro de Contingência do Coronavírus para monitorar e coordenar ações contra a propagação do SarsCov-2, o Estado de São Paulo vem, de forma técnica, adotando medidas para mitigação de danos provocados pela pandemia de COVID-19.

Outrossim, foi consolidado pela comunidade científica que o distanciamento social é política estatal de suma importância a ser adotada no combate à proliferação da doença. Cita-se como exemplo artigo publicado em abril de 2020 na Revista científica *The Lancet*, em que pesquisadores da Universidade de Hong Kong verificaram a eficácia de medidas restritivas implementadas desde 23 de janeiro de 2020 em quatro cidades e 10 províncias na China. O estudo concluiu que tais providências reduziram consideravelmente a taxa de infecção não somente por casos importados, mas também por contaminação local¹⁵.

14 ARAGÃO, Alexandre Santos de; SARMENTO, Daniel; BINENBOJM, Gustavo; ÁVILA, Humberto; SCHIER, Paulo Ricardo. *Interesses Públicos versus Interesses Privados: desconstruindo o princípio de supremacia do interesse público*. Rio de Janeiro: Editora Lúmen Júris, 2007.

15 XU, Shunqing; LI, Yuanyuan. Beware of the second wave of COVID-19. *The Lancet*, London, 2020, v. 395, p. 1321-1322. Disponível em: [https://www.thelancet.com/pdfs/journals/lancet/PIIS0140-6736\(20\)30845-X.pdf](https://www.thelancet.com/pdfs/journals/lancet/PIIS0140-6736(20)30845-X.pdf). Acesso em: 2 jun. 2022.

Em âmbito nacional, foi aprovada a Lei nº 13.979, de 6 de fevereiro de 2020, que dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus. No artigo 3º, o diploma determina que, para o combate à emergência de saúde pública de importância internacional, as autoridades poderão adotar, no âmbito de suas competências, entre outras, medidas de isolamento e quarentena.

Com vistas a instrumentalizar a política de isolamento social necessária ao enfrentamento da doença, foram adotadas no Estado de São Paulo diversas medidas administrativas a fim de diminuir a circulação de pessoas para atividades não essenciais, das quais destacam-se: a suspensão do atendimento presencial de todas as atividades e serviços públicos que não são considerados essenciais e a suspensão de eventos públicos estaduais que venham a agrupar pessoas em qualquer número.

Para além de tais medidas, visando ao monitoramento dos índices de isolamento social, o IPT, empresa pública constituída para desempenho de atividades científicas e tecnológicas, firmou Acordo de Cooperação Técnica com a empresa Telefônica Brasil S.A., que teve como objetivo regulamentar a forma de acesso das informações providas pela plataforma *Big Data* pelo IPT, para apoiar os órgãos governamentais das áreas de Saúde, Segurança Pública e Defesa Civil no planejamento estratégico de ações que visavam à identificação de demandas de logística para possível repasse de ajuda humanitária, por meio da identificação de zonas onde poderiam ocorrer maior disseminação do vírus COVID-19, utilizando-se de matrizes de deslocamento de origem e destino das pessoas. Buscando, por meio de análise estatística, avaliar o comportamento da população quanto ao isolamento social, identificação de formação de pontos de aglomeração, definição das principais vias utilizadas pela população para deslocamento e comportamento do êxodo para outras cidades.

Posteriormente, visando ampliar a quantidade das operadoras de telefonia envolvidas na referida atividade, em 14 de abril de 2020, o IPT firmou Acordo de Cooperação Técnica com as Prestadoras de Serviços de Telecomunicações de Interesse Coletivo (Claro S.A., Oi Móvel S.A., Telefônica Brasil S.A., Tim S.A.). Tendo por escopo o acesso da plataforma *Big Data*, para que lhe permitisse, por meio da atuação de seus pesquisadores especialistas, apoiar tecnicamente os órgãos governamentais legitimados, diante do interesse público geral e irrestrito em conter a disseminação do COVID-19.

Tal sistema de parcerias denominou-se Sistema de Monitoramento Inteligente de São Paulo (SIMI-SP), e, desde que implementado, passou a ser alvo de questionamentos judiciais de legalidade por diversos meios. Em tais ações, questiona-se a legalidade do tratamento de tais dados, considerados pessoais, pelo Poder Público e a finalidade de sua captura, bem como a ausência de consentimento expresso dos usuários de rede de telefonia móvel com a transmissão das informações coletadas. Desse modo, cumpre avaliar a compatibilidade do sistema de monitoramento implantado às disposições da LGPD.

Inicialmente, é necessário esclarecer que, quando da operacionalização inicial do sistema, em abril de 2020, a quase totalidade das disposições contidas na nova legislação encontravam-se em período de *vacatio legis*, posto que entraram em vigor apenas vinte e quatro meses após a publicação, ou seja, em agosto de 2020, nos termos do artigo 65 da LGPD.

Assim, o regramento então vigente encontrava-se disposto no artigo 72, §2º da Lei Geral de Telecomunicações (Lei nº 9.472/97), que estabelece a possibilidade do compartilhamento de informações pelas operadoras, desde que não permitam a identificação do usuário:

Art. 72. Apenas na execução de sua atividade, a prestadora poderá valer-se de relativas à utilização individual do serviço pelo usuário.

§ 1º A divulgação das informações individuais dependerá da anuência expressa e específica do usuário.

§ 2º A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que elas não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade.¹⁶

O Acordo de Cooperação Técnica firmado pelo IPT com as Prestadoras de Serviços de Telecomunicações, por sua vez, apresenta o seguinte objeto:

1. DO OBJETO DO ACORDO

1.1. O presente Acordo estabelece a cooperação entre as Partes para:

16 BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995 (grifo nosso). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 25 mai. 2022.

1.1.1 Permitir acesso do ENTE PÚBLICO aos DADOS disponibilizados na PLATAFORMA BIG DATA, com a finalidade de apoiar os órgãos governamentais legitimados e devidamente motivado, diante do interesse público geral e irrestrito em conter a disseminação do vírus Covid-19, *por meio da identificação de zonas, onde podem ocorrer maior disseminação do vírus, utilizando-se de matrizes de fluxos de deslocamento de origem e destino*, entre outras aplicação que possam ser desenvolvidas com a mesma finalidade.

1.2. As PARTES declaram que para a execução do presente Acordo *não há o tratamento de qualquer dado pessoal, tendo em vista que todos os DADOS são anonimizados, agregados, estatísticos e volumétricos disponibilizados das bases das PRESTADORAS.*

Além disso, no “Glossário” do Acordo realizado constam os tipos de dados que serão compartilhados entre as partes, bem como a definição da plataforma *Big Data*, utilizada para gerenciamento de tais informações agregadas:

(i) DADOS: consistem nos dados estatísticos e volumétricos *disponibilizados de forma anonimizada*, por meio de mapas de calor, e com vistas ao fortalecimento da política pública de contenção da expansão do coronavírus e de combate ao COVID-19 no território nacional, dentre outras aplicações, portanto sempre relacionados com a finalidade pretendida no Acordo.

[...]

(v) PLATAFORMA BIG DATA: Plataforma gerida pela ABR Telecom, contendo os DADOS, anonimizados e agregados, *sem a possibilidade de identificação do titular do dado e da PRESTADORA* que a disponibilizou[...].¹⁷

Observa-se, desse modo, nos termos do Acordo firmado, que não há compartilhamento de informações acerca da identidade dos usuários conectados à antena de telefonia em determinada região, nem mesmo da operadora de telefonia conectada, mas, tão somente, informações agregadas da quantidade de aparelhos ligados a uma determinada antena de certa região.

Conclui-se, portanto, tratar-se de dados anonimizados, não considerados pessoais para os fins da LGPD, nos termos do disposto em seu artigo 12:

17 BRASIL. Lei nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995 (grifo nosso). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/19472.htm. Acesso em: 25 mai. 2022.

Art. 5º Para os fins desta Lei, considera-se:

III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

XI – anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;”

Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.¹⁸

Importa destacar, por outro lado, que o sistema de monitoramento em estudo foi implementado em um cenário de calamidade pública de saúde causada pela pandemia do Coronavírus. Desse modo, o monitoramento dos dados tratados é instrumento de política de saúde pública com vistas a conter a disseminação do vírus por meio da verificação da adesão populacional à política de isolamento social, o que acaba por refletir na tomada de decisão dos administradores quanto às demais medidas a serem tomadas no combate à doença.

Assim, ainda que se considere que as informações transmitidas se enquadram no conceito de dados pessoais, entende-se que incidiria o disposto no inciso III do artigo 7 da LGPD, que elenca como uma das hipóteses de possibilidade de tratamento de dados pessoais a utilização de dados “pela Administração Pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres”.

Outrossim, considerando a primazia do bem jurídico tutelado pelas políticas de saúde pública, a própria Lei de Proteção de Dados dispõe, no artigo 13, que, na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados, exclusivamente, dentro deles e estritamente para a finalidade de realização de estudos e pesquisas. Além da obrigatoriedade de serem mantidos em ambiente controlado e seguro, conforme

18 BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados (LGPD)**. Brasília, DF: Presidência da República [2020]. Casa Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 19 jul. 2024.

práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Por fim, destaca-se que, justamente por considerar assegurado o anonimato, bem como preservado o sigilo dos dados apurados pelas empresas de telefonia móvel antes da transferência ao IPT, o Tribunal de Justiça de São Paulo, por reiteradas vezes, inclusive por meio de seu órgão especial, julgou válida a implantação do sistema de monitoramento. À título ilustrativo, destaca-se julgado proferido em mandado de segurança:

MANDADO DE SEGURANÇA. Constitucional. Termo de Cooperação Técnica firmado pelo Instituto de Pesquisas Tecnológicas (IPT) com as prestadoras de serviços de telecomunicações e com a Associação Brasileira de Recursos em Telecomunicações (ABR TELECOM). Alegação de ultraje aos princípios da intimidade e privacidade. Inocorrência. Instrumental tecnológico de alcance genérico de movimentação. Informações anonimizadas que não permitem conhecer os titulares dos chips telefônicos e das respectivas companhias. Visualização, tão só, da circulação diária não individualizada. Estrutura legal e opinativa que escoram a medida adotada. Direito líquido e certo absente ante a inexistência de invasão dos direitos de personalidade da autora. Precedentes do Colendo Superior Tribunal de Justiça e deste Emérito Órgão Especial em casos análogos. DENEGAÇÃO DA ORDEM.¹⁹

Do exposto, entende-se que a implantação do sistema de monitoramento se deu em compatibilidade com as previsões constantes e posteriormente vigentes da LGPD, não tendo ocorrido indevido tratamento de dados pessoais pelo poder público.

5. CONCLUSÕES

O advento da LGPD tem por objetivo regulamentar o tratamento dos dados pessoais em um contexto de constante inovação tecnológica e utilização das informações transmitidas para fins de mercado, por meio do armazenamento e compartilhamento destas em imensos bancos de dados.

A era informacional mudou a realidade da gestão pública. As informações constantes em prontuários físicos passam a ceder lugar à existência de bancos de dados informacionais integrados em rede. Com a entrada em vigor das disposições

19 SÃO PAULO (Estado). Tribunal de Justiça do Estado de São Paulo. *Cabe Mandado de Segurança Cível nº 2020.0000594814*. Impetrante: Fernanda Maria Schincarol. Impetrado: Governador do Estado de São Paulo [2020]. Relatora: Beretta da Silveira.

da LGPD, faz-se necessária a adaptação da Administração à normativa no que se refere ao tratamento de dados pessoais.

A Administração Pública insere-se nesse contexto à medida em que coleta e trata dados pessoais para realização de seus escopos na implantação de políticas públicas. Daí a essencialidade da advocacia pública no assessoramento da desta Administração durante esse processo, devendo o administrador estar atento às condicionantes jurídicas de sua atuação, evitando declarações de ilegalidade de atos e aplicação de sanções.

A imprescindibilidade da advocacia pública nesse cenário de implantação de novas tecnologias e formas legislativas de regulação pôde ser vista em concreto a partir do Sistema de Monitoramento Inteligente de São Paulo (SIMI-SP). Alvo de inúmeros questionamentos judiciais, a atuação da advocacia pública revelou-se essencial para demonstrar a legalidade do sistema implementado, bem como sua compatibilidade com as determinações da LGPD.

REFERÊNCIAS

AGUDO, Hugo Crivilim; TEIXEIRA, Tarcisio. As limitações da utilização de mecanismos de big data à luz da lei geral de proteção de dados pessoais. *In*: TEIXEIRA, Tarcísio; MAGRO, Américo Ribeiro. (Coord). **Proteção de dados: Fundamentos jurídicos**. 2. ed. Salvador: Editora JusPodivm, 2022, p. 229-265.

ARAGÃO, Alexandre Santos de; SARMENTO, Daniel; BINENBOJM, Gustavo; ÁVILA, Humberto; SCHIER, Paulo Ricardo. **Interesses Públicos versus Interesses Privados: desconstruindo o princípio de supremacia do interesse público**. Rio de Janeiro: Editora Lúmen Júris, 2007.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 25 mai. 2022.

BRASIL. **Lei nº 9.472, de 16 de julho de 1997**. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 25 mai. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em: 25 mai. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Presidência da República [2020]. Casa Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 25 mai. 2022.

CARVALHO, Cláudio Oliveira de. Políticas Públicas e Gestão Urbana Ambiental. *Revista de Direito Ambiental*, São Paulo, 2022, v. 26, n.7, p. 277-289.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. *Revista Brasileira de Direito Civil em Perspectiva*. Belém, 2019, v. 5, n. 2, p. 22-41. Disponível em: <https://www.indexlaw.org/index.php/direitocivil/article/view/5778/pdf>. Acesso em: 20 out. 2020.

DI PIETRO, Maria Sylvia Zanella. *Direito Administrativo*. 19. edição. São Paulo: Editora Atlas, 2006.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral da Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil Conteúdo e Tecnologia Ltda., 2006.

LAEBER, Márcio Rafael Silva. Proteção de dados pessoais: o direito à autodeterminação informativa. *Revista de Direito Bancário e do Mercado de Capitais*, São Paulo, 2007, v. 37.

MAGRO, Américo Ribeiro. A (in)eficácia do direito à anonimização de dados pessoais em face da análise de BIG DATA dos metadados produzidos no âmbito da internet das coisas. *In*: TEIXEIRA, Tarcisio; MAGRO, Américo Ribeiro. (Coord). *Proteção de dados: Fundamentos jurídicos*. 2. ed. Salvador: Editora JusPoivm, 2022, p. 13-51.

MAYER-SCHÖNBERGER, Viktor. 1997. apud MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti. (Coord.). *Direito Digital: Direito Privado e Internet*. 4. ed. Indaiatuba: Editora Foco, 2021, p. 42. 2021.

PEREIRA, Ana Paula Martins Regiolli Pereira. O tratamento de dados pessoais pelo Poder Público a partir da perspectiva da LGPD. *In*: TEIXEIRA, Tarcisio; MAGRO, Américo Ribeiro. (Coord). *Proteção de dados: Fundamentos jurídicos*. 2. ed. Salvador: Editora JusPodivm, 2022, p. 115-137.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O direito à proteção de dados pessoais e a privacidade. *Revista da Faculdade de Direito da UFPR*, Curitiba, n. 47, 2008, p. 29-64.

SÃO PAULO (Estado). Tribunal de Justiça do Estado de São Paulo. **Cabe Mandado de Segurança Cível nº 2020.0000594814**. Impetrante: Fernanda Maria Schincarol. Impetrado: Governador do Estado de São Paulo [2020]. Relatora: Beretta da Silveira.

SÃO PAULO (Estado). Assembleia Legislativa do Estado de São Paulo. Acordo de Cooperação Técnica entre Instituto de Pesquisas Tecnológicas do Estado de São Paulo (IPT) e Claro S.A, Oi Móvel S.A, Telefonica Brasil S.A, Tim S.A e Associação Brasileira de Recursos em Telecomunicações - ABR Telecom. Disponível em https://www.al.sp.gov.br/spl/2020/10/Acessorio/1000337521_1000394583_Acessorio.pdf. Acesso em 22 jul. 2024.

SOUZA, Thiago Vieira de. *A proteção de dados pessoais como direito fundamental e a [in]civildade do uso de cookies*. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Direito, Universidade Federal de Uberlândia, Uberlândia, 2018.

TESSER, André Luiz Bäuml. Premissas fundamentais de um adequado e efetivo programa de privacidade e proteção de dados pessoais na administração pública: uma análise das necessidades e possibilidade a partir da LGPD. *In*: PIRONTI, Rodrigo. (Coord.). *Lei Geral de Proteção de dados no Setor Público*. Belo Horizonte: Fórum, 2022.

WONTOBA, Bruno; ÁBILA, Paola. Lei Geral de Proteção de Dados: Os Direitos do Titular dos Dados Pessoais. **Justen, Pereira, Oliveira e Talamini advogados**, 2020. Disponível em: <https://justen.com.br/pdfs/IE163/IE163-BrunoePGADtosTitDadosPessoaisLGPD.pdf>. Acesso em: 26 mai. 2022. Disponível em: <https://justen.com.br/pdfs/IE163/IE163-BrunoePGA-DtosTitDadosPessoaisLGPD.pdf>. Acesso em: 2 jun. 2022.

XU, Shunqing; LI, Yuanyuan. Beware of the second wave of COVID-19. **The Lancet**, 2020, v. 395, p. 1321-1322. Disponível em: [https://www.thelancet.com/pdfs/journals/lancet/PIIS0140-6736\(20\)30845-X.pdf](https://www.thelancet.com/pdfs/journals/lancet/PIIS0140-6736(20)30845-X.pdf). Acesso em: 2 jun. 2022.