RESPONSABILIDADE CIVIL DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL PELA VIOLAÇÃO DE DADOS PESSOAIS SENSÍVEIS:

Debates contemporâneos sobre cidades inteligentes *(smart cities)*

Submetido em: 25-05-2024
Publicado em: 02-12-2024

Cláudio José Franzolin
Doutor em Direito, PUC-SP
cfranzol30@gmail.com

Letícia Pardo Rodrigues do Carmo
Mestre, PUC-Campinas
pardoleticia@outlook.com

RESUMO: O artigo explora a intersecção entre responsabilidade civil, cidades inteligentes e a proteção de dados pessoais sensíveis, com ênfase na proteção da saúde. Trata-se de estudo de objetivo exploratório, que coteja a literatura analisada com previsões legais a partir do diálogo das fontes (Constituição Federal, Lei Geral de Proteção de Dados, Código Civil) e, também, aponta decisões judiciais, merecendo destaque a do Supremo Tribunal Federal (STF). Apresenta-se, inicialmente, a interface da saúde de cidades inteligentes. Após, são abordadas diferentes nuances do dever de proteção dos dados pessoais sensíveis dos cidadãos em matéria de saúde e, em sequência, expõem-se aspectos da responsabilidade civil do Município em caso de violação desses dados, sem excluir uma abordagem acerca das limitações orçamentárias municipais para investimento em tecnologia e segurança da informação. Ao final, ressalta-se a necessidade de preparo da comunidade jurídica e dos órgãos competentes para lidar com proteção de dados pessoais sensíveis de saúde dos indivíduos, incluindo a necessidade de despertar uma cultura de dados dos cidadãos.

Palavras-chave: Cidades inteligentes; Saúde digital; Direito à saúde; Políticas públicas municipais; Proteção de dados sensíveis; Responsabilidade Civil.

CIVIL LIABILITY OF MUNICIPAL PUBLIC ADMINISTRATION FOR VIOLATION OF PERSONALLY SENSITIVE DATA:

contemporary debates on smart cities

ABSTRACT: The article conducts an in-depth examination of the confluence among civil liability, intelligent urban development, and the safeguarding of confidential health-related personal data, under the purview of domestic legal frameworks, with a particular focus on the General Data Protection Law (LGPD). This research, structured as a literature review with an exploratory aim, juxtaposes the scrutinized scholarly works with statutory mandates, such as the Federal Constitution, LGPD and the Civil Code, as well as jurisprudential outcomes,

predominantly from the Supreme Court. The discourse commences with an exposition of the health-related functionalities within intelligent cities. Subsequently, it delves into the multifaceted obligations to preserve the privacy of citizens' health-related sensitive data, succeeded by an analysis of municipal accountability in instances of data infringement. This encompasses an exploration of the interplay between data protection and the municipality's fiscal wherewithal for technological and informational security investments. The treatise culminates by underscoring the imperative for the legal fraternity and authoritative entities to be well-equipped to address the intricacies surrounding the defense of individual health data privacy, advocating for the integration of a data-centric ethos within municipal governance.

Keywords: Smart cities; Digital health; Right to health; Data protection; Civil liability; Municipal public administration.

1 INTRODUÇÃO

Quando se pensa em cidade inteligente, é possível que um cenário como aquele retratado na animação "Os Jetsons" venha à mente. O desenho animado, já na década de 1960, previa cidades equipadas de dispositivos e equipamentos eletrônicos nas casas repletas de tecnologias. No desenho, em certo episódio, um dos personagens realizava consultas *online* (telemedicina); noutro, havia a empregada doméstica que era um robô; noutra circunstância, personagens se comunicavam por videochamadas, inclusive, por meio de relógios digitais; ainda, as personagens que representavam crianças, tinham o assistente tecnológico para auxiliá-las nas suas lições de casa.

Essas situações que pareciam distantes, hoje não é mais. As pessoas podem consultar o médico via teleconsulta. Também há os *smartwatchs* para monitoramento de sinais vitais do paciente. Além disso, hoje também há assistentes virtuais, como *Alexa* e *Siri*.

Em especial, nos centros urbanos, despontam-se as cidades globais ou mundiais[25], as quais passam a receber grandes investimentos em tecnologias por parte de grupos corporativos multinacionais; e nesse contexto, não há como não despertar interesse da administração pública para a gestão mais eficiente pelo administrador público e que, neste estudo, nos concentramos na área da saúde.

Na verdade, à medida que as tecnologias incorporam as telecomunicações, desponta-se, por exemplo, a *internet* das coisas (*IoT*), conforme os objetos conectam-se uns com os outros transmitindo dados, informações. Por meio do aparelho móvel, por exemplo, permite monitorar e controlar equipamentos da casa, como ligar ou desligar o ar-condicionado; e, conforme o caso, aparelhos acoplados aos indivíduos por algum motivo de saúde (como, controle de oxigenação) podem também ser monitorados por outros dispositivos.

Enfim, tecnologias cada vez mais refinadas as quais avançam em intervalos de tempo cada vez menores. Ressalte-se, porém, que dada a limitação do objeto deste estudo, inovações tecnológicas e a interface com a gestão pública e com os serviços públicos vários não serão abordados, mas nos concentraremos, apenas, com relação a saúde, e ainda, assim, apenas sob uma perspectiva, qual seja, sobre os dados pessoais do cidadão. Acrescente-se, também, que não é objeto deste estudo as tecnologias disruptivas na área do agronegócio.

Ou seja, o foco é a dinâmica da vida urbana e a incorporação crescente da tecnologia para atendimento dos mais variados interesses, seja para a administração, seja para a coletividade, despertam os estudos das denominadas cidades inteligentes (*smart cities*).

Segundo a *Carta Brasileira para Cidades Inteligentes*, estas abrangem o ambiente urbano alinhado à transformação digital com vistas à sustentabilidade (econômica, ambiental

[25] O sistema de relações econômicas globais passa a ostentar uma forma mais urbanizada, de maneira que se destaca a "espacialidade dispersa, porém com a organizada interação global de atividades econômicas, sob a forte égide de atuação das grandes empresas com presença mundial. As cidades passaram a influenciar vastas regiões através de diversos recursos, principalmente financeiros, telecomunicações, ciência, desenvolvimento de tecnologia e serviços industriais especializados (...). Portanto, um novo tipo de cidade aparece, essa é a cidade mundial". Ou seja, estes rearranjos que passam a ser denominadas as cidades como globais, tem como características: i. foca o desenvolvimento de uma geografia específica no controle de lugares na ordem econômica internacional; ii. valorizam produções particulares específico para os consumidores locais; iii. produzem serviços materiais e imateriais nestas cidades a permitir que se comande o processo de reprodução do espaço de outras cidades; iv. Despontam-se novos arranjos de habitantes, que detém novos tipos de perceber, conceber e interpretar a sociedade urbana, tendo como foco, o consumismo, a necessidade de o engajamento político e contato com novos tipos de prestações de serviços (Silva, 2005, p. 12).

e sociocultural), a fim de serem enfrentados problemas concretos, como acesso à saúde, à redução das desigualdades e à melhora da qualidade de vida das pessoas (Brasil, 2021, p. 28).

Tecnologias também que possam contribuir na adoção de políticas públicas permitindo que as cidades se preparem para situações de agravamento de saúde pública associadas às contaminações decorrentes de contato dos habitantes com água poluída em virtude de enchentes. Como está ocorrendo com parte da população das cidades do Estado do Rio Grande do Sul[26] ao ser atingida pelas inundações em virtude de chuvas intensas associadas às questões climáticas. Assim, contatado que o cidadão está com *leptospirose*, dita informação passa a ser um dado sensível seu, integrado num sistema de saúde que permite o acompanhamento por várias secretarias e órgãos da rede pública do estado de saúde desse cidadão contaminado e, também, permite levantar e detectar regiões, evitando, assim, o agravamento e expansão das contaminações.

Enfim, as cidades inteligentes podem ser compreendidas como aquelas que se apoiam em três componentes centrais: *o elemento humano, o tecnológico e o institucional,* de modo que a correlação entre eles deve focar o bem-estar da pessoa humana (Nam; Pardo, 2011, p. 286), afinal, todos têm direito à cidade, enquanto expressão de direito humano.

Só que o manejo das ferramentas tecnológicas para a gestão mais eficiente da cidade inteligente, conforme haja falta de segurança para o cuidado na proteção dos dados pessoais, desaguam nos debates na seara da responsabilidade civil.

Para fixar limites neste estudo, o foco dentro da responsabilidade, por sua vez, é delimitado diante do dano decorrente do manejo pelo gestor público dos dados pessoais associados à saúde, denominados como sensíveis, ante o não atendimento aos princípios estruturantes da Lei Geral de Proteção de Dados (L. 13.709/2018), como boa-fé, finalidade, prevenção, dentre outros.

---

[26] "Pessoas que tiveram contato com água das cheias e inundações, como as que atingem Porto Alegre nos últimos dias, devem ficar atentas a possíveis sintomas de leptospirose. A recomendação de atenção também é válida para profissionais de saúde, no atendimento a pacientes. O alerta sobre o risco de contaminação é da Secretaria Municipal de Saúde (SMS) e foi emitido neste domingo, dia 5. A leptospirose é uma doença infecciosa causada por uma bactéria chamada leptospira, presente na urina de ratos e de outros animais. É transmitida por água contaminada e pelo contato com a pele, principalmente se houver algum arranhão ou ferimento. "Em situações de enchentes e inundações, a urina dos ratos em esgotos e bueiros mistura-se à enxurrada e à lama, fazendo com que qualquer pessoa que tenha contato com a água das chuvas ou o lodo contaminado possa ser atingida", explica a diretora da Vigilância em Saúde de Porto Alegre, Evelise Tarouco da Rocha". (Prefeitura de Porto Alegre, 2024).

Na verdade, cidades inteligentes abrangem o tratamento de dados pessoais dos cidadãos na *práxis* da *urbe.*

Aliás, na *Carta Brasileira para Cidades Inteligentes* consta como um de seus objetivos a utilização segura e responsável de dados pessoais dos cidadãos e das TICs em geral.

Até porque a utilização desses dados pessoais por meio do manejo das TICs incrementam de forma exponencial a transformação dos serviços públicos, desde que dito manejo pela gestão pública seja com transparência, responsabilidade e eficiência (Bloomberg, 2014, p. V-VI).

Só que há grande abrangência dos serviços públicos que possa envolver tratamento de dados pessoais pela gestão pública local; por isso, dentro dos estudos que envolvem cidades inteligentes (como segurança pública, lazer, educação), o presente estudo – sem a pretensão de esgotar todo o complexo conteúdo que envolve o tema – aborda algumas reflexões das ditas cidades no contexto do acesso à saúde, notadamente, na interface com a problemática da utilização indevida ou em desatenção aos deveres de cuidado, proteção e segurança necessários, dos dados pessoais, relacionados à saúde do cidadão (*i.e.*, em descompasso com as regras e princípios da LGPD, como, por exemplo, uso de um dado de saúde com finalidade diversa que justificou sua coleta) e, a partir daí, a imputação do dever de indenizar do município.

Nesse sentido, esta investigação busca abordar sobre o regime jurídico de responsabilidade civil dos municípios pela violação de dados pessoais sensíveis - associados à saúde - do cidadão, considerando o diálogo das fontes[27] como metodologia de análise, entre Estatuto da Cidade (L. 10.257/2001-EC), Lei Geral de Proteção de Dados Pessoais (L. 13.709/2018-LGPD) e Código Civil (L. 10.406/2002-CCi) e legislação conexa.

Inclui-se, nessa análise, o estudo da jurisprudência do Supremo Tribunal Federal.

---

[27] Diálogo das fontes, enquanto um método, trazido ao Brasil pela Cláudia Lima Marques, mas desenvolvido por Erik Jayme. Método enquanto "face do atual pluralismo pós-moderno de um direto com fontes legislativas plúrimas, ressurge a necessidade de coordenação entre as leis no mesmo ordenamento, como exigência para um sistema jurídica eficiente e justo (...)". Ainda, a expressão diálogo das fontes, conforme a autora, é uma tentativa de expressar a necessidade de uma aplicação coerente das leis coexistentes, contribuindo para que se "dê uma eficiência não hierárquica, mas funcional do sistema plural e complexo de nosso direito contemporâneo, a evitar a antinomia, incompatibilidade ou a não coerência". Ao se sustentar o diálogo "há aplicação conjunta de as duas normas ao mesmo tempo e ao mesmo caso, seja complementarmente, seja subsidiariamente, seja permitindo a opção pela fonte prevalente, ou mesmo permitindo uma opção por uma das leis em conflito abstrato", em suma, permitir uma interpretação mais aberta para se permitir uma "solução mais favorável ao mais fraco na relação (tratamento diferente dos diferentes)" (Marques, 2016, p. 135-153).

Para tanto, será realizada revisão de literatura, de objetivo exploratório, a partir de documentos (leis, decisões judiciais) e de artigos científicos, livros, materiais a serem referenciados no decorrer do trabalho.

Inicialmente, serão abordadas noções sobre cidades inteligentes e sua interface com as questões da saúde. Após, será feito o cotejo dos dados pessoais associados à saúde do cidadão - dados pessoais sensíveis - e o dever de proteção desses dados dos titulares e, por fim, são expostos aspectos da responsabilidade civil do Município em caso de violação desses dados.

2 ACESSO À SAÚDE E CIDADES INTELIGENTES: Desafios à frente

Como anteriormente visto, a proposta de cidades inteligentes que são retratadas em animações como "Os Jetsons", são aquelas que se valem de tecnologia para resolução de problemas urbanos e promoção da qualidade de vida. Ressalvados, por óbvio, os estudos analíticos diversos sobre cidades inteligentes conforme os vários autores e posições que eles defendem.

Apesar de a animação retratar o que seria uma cidade inteligente, na literatura, não há um consenso sobre sua compreensão analítica.

Para alguns autores, cidades inteligentes estão associadas com soluções tecnológicas a partir da utilização das TICs na gestão dos problemas urbanos (Mora; Bolici; Deakin, 2017, p. 16-18). Em suma, nesta acepção, a tecnologia não é o elemento principal, mas alinhada para promoção da qualidade de vida para as pessoas nas cidades inteligentes. Não é a tecnologia implantada que dá o tom para o atributo de inteligente para uma cidade, enquanto um fim em si mesma (Kummitha; Crutzen, 2017, p. 46; Nam; Pardo, 2011, p. 286), mas, a tecnologia à serviço da melhoria de qualidade de vida e ambiente urbano mais sustentável. Ressaltamos que há autores que firmam no propósito de associar cidade inteligente com a tecnologia.

Detendo na abordagem de cidade inteligente e saúde, ganha destaque o assunto: abordando *saúde digital*.

O relatório *World Cities Report* de 2022, da ONU-HABITAT, destaca a problemática da *equidade* e a *importância de ferramentas tecnológicas aplicadas à saúde* para estas contribuírem na busca de soluções voltadas para a universalidade do acesso a serviços de saúde, e de maneira que ditos serviços sejam executados com melhor qualidade.

Saúde digital, aqui entendida de forma ampla e à luz da Organização Mundial da Saúde (OMS, 2021, p. 14), está associada às diversas formas de aplicação das TICs em saúde, tais como *telemedicina*, *telessaúde*, *Internet* das Coisas (*IoT*), inteligência artificial (IA), dentre outros apetrechos e recursos associados ao *e-saúde.*

No dito relatório da ONU-HABITAT (2022, p. 228-229) aponta, por exemplo sobre a possibilidade de a *telemedicina* contribuir para a *equidade* na saúde, considerando que dita tecnologia pode fomentar atendimentos remotos do médico com pacientes (*teleconsulta*), conforme estes não possam se deslocarem, em virtude das mais variadas justificativas. A telemedicina, na sua especificidade de *teleinterconsulta*, também pode ser manejada para que um médico especialista da rede pública, lotado num grande centro, possa, de forma remota, acompanhar o médico generalista, também da rede pública e lotado noutro lugar onde ali, este tem contato direto com o paciente.

Registre-se que a *Associação Brasileira de Normas Técnicas* (ABNT, 2021, p. 33-36) compilou a NBR ISO 37122 - indicadores para cidades inteligentes – onde, nela, detalha o conteúdo material que uma cidade inteligente deve apresentar em áreas como energia, educação, meio ambiente, governança, segurança e, *também na área da saúde*.

Em termos de saúde – que é o foco deste estudo – a NBR aponta que na cidade inteligente deve ser implementado o prontuário eletrônico, unificado e acessível *online* pelos provedores de serviços de saúde; ainda, deve promover a realização de consultas médicas à distância. Também dispõe a NBR sobre a necessidade de sistemas de alertas públicos, em tempo real, sobre condições climáticas e qualidade de água, afinal, também impactam na saúde do cidadão.

Por exemplo, em matéria de *vigilância de saúde*, implica, necessariamente, na coleta de grande número de dados pessoais originários de fontes variadas, como, fichas de notificações de agravos e doenças, as obtidas em unidades de saúde da atenção básica, dados coletados em hospitais para aquelas doenças que necessitem obrigatoriamente de internação (Freitas, Périssé, 2023, p. 35).

Em termos de ferramentas de saúde digital devem ser atreladas aos ambientes urbanos inteligentes. No entanto, não se pode afastar os riscos que todas essas potencialidades tecnológicas podem ocasionar para a vida dos cidadãos.

Isto é, partindo da premissa que a saúde digital é complexa, conforme avançam-se sistemas baseados no tratamento de dados pessoais do cidadão, como uso, coleta, dentre

outras atividades, acentuam-se também os deveres de cuidado e proteção para que possam gerenciar riscos inerentes ao uso dos ditos dados. É preciso, sim, considerar a segurança da informação *(accountability),* a fim de evitar impactos deletérios não só em detrimento do cidadão ao ter seus dados violados, mas, acima de tudo, porque o dano sempre será difuso, afetando grande parte da população local (Cavet, 2023, p. 27).

Em suma, não há como negar o risco de danos pelo vazamento de informações relacionadas aos dados pessoais dos cidadãos (Tomasevicius Filho, 2021, p. RB-10.3) à medida que a administração pública passa a utilizar e equipar com novas tecnologias[28] os espaços urbanos, os serviços e os bens públicos, num ambiente, cada vez mais, hiperconectado, captando, coletando, mais e mais, dados pessoais; mas, por outro, podem evidenciar situações danosas em detrimento dos titulares desses dados, conforme eles vivem na *urbe*.

No entanto, em se tratando de dados pessoais associados à saúde – denominado sensíveis – acentua-se, de um lado, a gravidade diante da sua eventual violação; por outro, não há como deixar de reconhecer que a coleta e compartilhamento de certos dados sobre saúde, podem promover melhor a proteção coletiva dos cidadãos. Não há como evitar nem tem sentido, proibir, em matéria de tutela de saúde coletiva, a coleta e compartilhamento de dados pessoais sobre saúde dos cidadãos. Não só! A possibilidade, por exemplo, do acesso aos dados pessoais do cidadão, ou pelos agentes de saúde do hospital público local, ou pelo gestor da secretaria de saúde, dito acesso se mostra relevante, seja para avaliar as causas de uma dada doença naquela região, seja para ali sejam deslocados profissionais mais especializados e assim contribuírem para melhor atendimento e cuidado das pessoas que ali vivem, bem como evitar que uma doença se alastre.

3 DADOS PESSOAIS DE SAÚDE DO TITULAR ENQUANTO DADOS SENSÍVEIS E O DEVER DE PROTEÇÃO PELO PODER PÚBLICO MUNICIPAL

[28] Essas novas tecnologias, de maneira geral, são citadas por Klaus Schwab (2016, p. 135), conforme o autor denomina como Quarta Revolução Industrial, ele destaca que a "conectividade digital possibilitada por tecnologias de software está mudando profundamente a sociedade" e ele aponta vinte e uma mudanças tecnológicas. Por exemplo, i. tecnologias implantáveis; ii. Presença digital na internet; iii. Acomodação de tecnologias em bens de utilidade pessoal, por exemplo, smartphones. Dentre outras, o autor cita as cidades inteligentes, ao afirmar que elas ampliam "sua rede tecnológica de sensores e trabalhos em plataformas de dados, que serão o centro de conexão dos diferentes projetos tecnológicos e de da adição de serviços futuros, com base na ciência da análise de dados e modelagem preditiva".

A preocupação com dados pessoais passou a ganhar relevância nos debates de maneira geral. Com a elevação à dignidade constitucional ao ser reconhecido como direito fundamental, o "direito à proteção dos dados pessoais", inclusive nos meios digitais, consoante Emenda Constitucional, 115, de 2022, passou a ter mais visibilidade referido direito, em que pese a LGPD fosse anterior à dita Emenda.

E esse incremento sobre dados pessoais inaugura, na verdade, a necessidade de se construir uma cultura de dados, que hoje ainda é muito incipiente.

Não é para menos. Numa sociedade que as pessoas têm falta de comida e água potável, obviamente, primeiro, elas se preocupam em se alimentar e, por isso, a preocupação delas com seus dados pessoais acabam se tornando preocupação secundária. Mas, não se pode afastar a relevância que a LGPD inaugura na sociedade.

Nesse sentido, a LGPD é uma norma que

> *visa modificar a cultura no tratamento de dados pessoais para que riscos sejam mitigados desde antes do tratamento, evitando-se ao máximo qualquer hipótese, sempre presente, de violação de dados pessoais*. No decorrer da Lei há uma motivação nítida nesse sentido, impondo que os agentes de tratamento, desde a concepção da iniciativa que visa tratar dados pessoais e durante todo o seu ciclo de vida, que termina com o seu descarte, reflitam, analisem e adotem medidas efetivas para garantir a legalidade dos procedimentos e a proteção desse insumo tão valioso, mas, ao mesmo tempo, tão perigoso, se tratado de forma irregular (Blum; Maldonado; 2019, p. 158, grifos nossos).

No atual contexto histórico, na denominada *sociedade da informação*[29], os dados pessoais dos seus respectivos titulares adquirem valor econômico; e, por outro, ditos dados pessoais mostram-se indispensáveis para o funcionamento de organismos públicos, como na execução de políticas públicas (Pereira; Alvim, 2020, p. RB-45.1).

Consoante art. 1º, da *Lei Geral de Proteção de Dados*, ela consigna, de forma expressa, sua aplicação às pessoas jurídicas de direito público; e no seu *Parágrafo Único* resta claro que as normas da referida LGPD "são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e *Municípios*" (grifos nossos).

Ademais, conforme orientação da Autoridade Nacional de Proteção de Dados (ANPD), é de que o "tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD"

[29] A expressão "sociedade da informação" é utilizada para denominar o paradigma técnico-econômico principalmente visto no século XXI que destaca a utilização da própria informação como matéria-prima da atuação humana, impulsionados pela tecnologia. Essa sociedade promove transformações significativas na vida individual e social, no conhecimento produzido e utilizado, na mudança contínua e aprendizado, na diversidade e em políticas ambientais sustentáveis (Werthein, 2000, p. 71-72).

(Brasil, 2022, p. 6). Esclarece, nesse sentido, que ditos dispositivos devem ser "interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público" (Brasil, 2022, p. 6).

Dentre os *dados pessoais*, há aqueles relacionados à saúde da pessoa humana. É que, quando se aborda as informações relacionadas à saúde da pessoa humana, enquanto uma dimensão da sua vida privada - no caso, do paciente[30] - a proteção desses seus dados pessoais de saúde, conforme sejam manejados pelos profissionais da saúde e pelos agentes públicos, bem como, pelos órgãos e gestores públicos municipais. Incluem-se aqui, as concessionárias de serviços públicos. Assim, pode ocorrer a necessidade de atender algum dever legal pela concessionária de serviço público municipal, quando ela tem de encaminhar algum dado pessoal – de saúde – de algum funcionário seu para um órgão municipal, considerando alguma questão, como infecção, ou alguma informação que reflete na execução do serviço.

Ainda, há que se destacar também os serviços de saúde de natureza digital.

Sobre saúde digital, há outras normas jurídicas que regulam a temática da proteção de informações pessoais dos pacientes. Por exemplo, tem a L. 13.787/2018 (Brasil, 2018), que dispõe, conforme seu art. 1º, sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuários de pacientes. Ainda, sobre a questão digital da saúde, tem a *telemedicina*. É possível destacar que havia, num primeiro momento, a Lei n.º 13.989, de 15 de abril de 2020. Esta lei foi sancionada para viabilizar o uso da telemedicina durante a crise causada pelo coronavírus[31] em território nacional. Depois, a prática da *telessaúde* no Brasil consolidou-se com a Lei nº 14.510, sancionada em 27 de dezembro de 2022.

Só que a telemedicina e suas várias possibilidades envolvem coleta dos dados sensíveis de seus titulares e eles transitam pela rede; e, sem a segurança, coloca em risco a privacidade. Ou seja, embora o Brasil disponha de uma Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD) que regula a proteção de dados pessoais e apresente um rol de

[30] Albuquerque (2022, p. RB-14.5) expõe que "a violação da confidencialidade dos seus dados [do paciente] pode expor a sua vida íntima, eventos dolorosos, doenças estigmatizantes e outras particularidades, o que incrementa a sua fragilidade e tem o condão de acarretar-lhe danos psíquicos graves".

[31] A pandemia decorrente do COVID-19 foi reconhecida pela OMS. Tratou-se de um vírus transmitido facilmente de uma para outra pessoa; assim, no intuito de se conter e combater a contaminação, os países adotaram variadas medidas, como quarentena, distanciamento e isolamento social, interrupção de atividades (WHO – World Health Organization).

deveres de proteção, segurança e cuidado, não significa que a execução desses deveres está sendo adimplida.

Esclareça-se que a LGPD, logo no artigo primeiro, dispõe que ela regula o tratamento de dados pessoais para proteção da privacidade e da liberdade da pessoa humana, além de assegurar o livre desenvolvimento de sua personalidade.

Diante do escopo da LGPD, é preciso esclarecer, primeiramente, o que é tratamento do dado pessoal e qual o seu conteúdo; e a partir daí, como ditos conceitos relacionam com a saúde na perspectiva digital. No artigo art. 5º, da LGPD, ela aponta duas espécies de dados pessoais: dado pessoal e dado pessoal sensível[32].

Dado pessoal, consoante previsto na LGPD, é compreendido em sentido amplo; é aquele que diz respeito à informação relacionada à pessoa identificada ou identificável, especificamente pessoa natural[33]; isto é, o dado é pessoal se ele, por si só, identifica seu titular ou, então, a partir da combinação e integração com outras informações que se referem ao dito titular (Konder, 2023, p. RB-16.3).

Lado outro, há, segundo Konder (2023, p. RB-16.1), alguns dados que são considerados sensíveis em decorrência do princípio da dignidade da pessoa humana, notadamente de suas facetas de privacidade, identidade pessoal e vedação de discriminação.

A LGPD define dado pessoal sensível como aquele de "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" (art. 5º, II). Assim, por expressa previsão legal, os dados relativos à saúde do indivíduo são considerados sensíveis.

Compreender a diferença entre ambos é fundamental, eis que há normativas específicas para a utilização (tratamento) desses dados, de acordo com sua natureza (Vainzof, 2022, p. RL-1.2). O presente trabalho foca no estudo de dados de saúde, denominados pela LGPD como sensíveis.

Contudo, antes de aprofundar em tais possibilidades, é importante esclarecer o que é o tratamento de dados pessoais que a LGPD traz, no art. 5º, X. É

---

[32] "Art. 5º Para os fins desta Lei, considera-se: 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;"

[33] "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;"

> toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A previsão legal traz um rol exemplificativo. Nota-se que existe um "ciclo de vida" do dado pessoal, ou seja, dito ciclo vai desde sua coleta, passa pelo manejo deles nos variados modos, até, finalmente, eles serem eliminados pelo controlador (Tamer, 2022, p. 87-88). Ademais, a LGPD aponta seus princípios orientativos e aplicáveis a quaisquer operações de tratamento de dados, sejam sensíveis ou não.

Tomasevicius Filho (2021, p. RB-10.3) compreende que todos os princípios elencados no art. 6º da LGPD se subsumem aos deveres anexos ou colaterais à boa-fé: coerência, informação e cooperação. Especialmente para o caso dos dados sensíveis, dois princípios são destacados: o da finalidade e o da não discriminação (Mulholland, 2018, p. 164).

Segundo o princípio da finalidade, os dados devem ser tratados para um objetivo específico, o qual deve ser informado, previamente e de forma explícita, ao titular dos dados, vedando-se a utilização posterior para outra finalidade (Mulholland, 2018, p. 164). Assim, esse princípio reflete a importância da proteção dos dados pessoais, eis que, ao se exigir um fim específico para cada operação com o dado, determina que dito dado não mais seja tratado à revelia do titular, sem objetivo definido, a fim de coibir a lógica de "coletar e armazenar tudo" (Tamer, 2022, p. 102).

Por sua vez, o princípio da não discriminação é de grande importância na área da saúde, uma vez que os dados de saúde trazem características personalíssimas do titular (Mulholland, 2018, p. 165). Por esse princípio, veda-se o tratamento de dados com fins discriminatórios, ilícitos ou abusivos.

Percebe-se que a vedação à discriminação é qualificada pelos adjetivos "ilícito" e "abusivo". Assim, a LGPD só autoriza o tratamento de dados de forma diferenciada, se estiver em consonância com objetivos lícitos e no exercício regular de direito do agente de tratamento. Essa verificação passa também pelas lentes do intérprete, à medida que ele deve preencher o conteúdo das normas de calibração com alta vagueza semântica, como é o princípio da boa-fé; ou seja, permite ao intérprete seja analisada a coleta e tratamento de dados sensíveis conforme os pressupostos fáticos que abrangem a situação concreta que pretende o acesso a esse tipo de dado do cidadão (Mulholland, 2018, p. 165; Tamer, 2022, p. 115).

Além dos princípios apresentados pelo legislador que orientam o intérprete para analisar a conduta do agente de tratamento, quando envolve dados pessoais sensíveis, há dispositivo expresso na LGPD, qual seja, o Art. 11 da LGPD.

Segundo Tamer (2022, p. 167), as bases legais são os motivos expressos na LGPD que legitimam a realização do tratamento de dados pessoais do titular. E, no caso do tratamento de dados sensíveis, como os de saúde, a LGPD enumera um rol taxativo de bases legais, haja vista que o potencial lesivo ao ser manejado indevidamente envolve maior risco ao titular.

Conforme art. 11, há previsão de tratamento de dados "com" e "sem" consentimento do titular. Na primeira hipótese, estabelece a LGPD que o consentimento deve ocorrer de forma específica e destacada para finalidades singulares (art. 11, I, LGPD). Nota-se, pois, exigência de solenidade na forma e no conteúdo da manifestação de vontade do titular, ou seja, imperioso o termo de consentimento do titular.

Importante esclarecer que o consentimento a ser prestado pelo paciente no âmbito da saúde não deve ser genérico, tampouco em forma de simples formulário de ciência.

Tratando-se de dados sobre saúde, designe-se, neste estudo, o titular como paciente ou não. Sendo paciente, ele é titular da informação, porém ostenta uma vulnerabilidade agravada. Primeiramente porque a preocupação dele não será sobre seus dados pessoais. Segundo, porque a linguagem técnica do médico e os dados não são assimilados na sua integralidade pelo paciente que está preocupado com a situação de sua moléstia. Ademais, não é possível deixar de reconhecer sobre a incerteza acerca da efetividade de o consentimento ser livre e espontâneo (Scaff, 2022, p. RB-10.4-10.5; Albuquerque, 2022, RB-14.2). Livre até pode ser, mas numa questão que a saúde pública exige movimentação rápida de pessoas e dados, me parece que fica a dúvida da efetividade do consentimento, quando abrange questões associadas aos dados pessoais sensíveis.

Deve o titular, antes de consentir, receber informações por meio de linguagem acessível e com lealdade (Scaff, 2022, p. RB-10.4-10.5). E aqui estão alguns desafios. O paciente realmente conseguiu compreender a moléstia que lhe acomete? O profissional da saúde conseguiu esclarecer as alternativas, os riscos, e quais os efeitos posteriores aos tratamentos disponíveis e oferecidos? E se o paciente é analfabeto?

No mais, o tratamento de dados pessoais sensíveis sem consentimento do titular é autorizado em sete hipóteses elencadas no art. 11, inciso II: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) pela Administração Pública, para o tratamento e uso

compartilhado de dados necessários à execução de políticas públicas conforme previsão em lei ou regulamento; c) para realização de estudos por órgãos de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) para o exercício regular de direitos, inclusive em contrato e em processo administrativo, judicial ou arbitral; e) para proteção da vida ou da incolumidade física do titular ou de terceiros; f) para tutela da saúde, em procedimento realizado por profissionais da área de saúde ou autoridade sanitária; g) para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Além disso, há a hipótese prevista no *caput* do artigo 13, que se refere a estudos em saúde pública, quando órgãos de pesquisa podem tratar dados pessoais, exclusivamente, para a finalidade do estudo; devendo, portanto, restringir o tratamento ao próprio órgão de pesquisa e à manutenção de sua segurança, priorizando, sempre que possível, a anonimização[34], ou, no mínimo, pseudoanonimização[35] dos dados.

Ressalta Mulholland (2018, p. 168) que as bases legais para o tratamento de dados sensíveis se referem, em grande parte, às hipóteses de interesse público, as quais prevalecem em detrimento do interesse particular do titular.

Contudo, conforme adverte Albuquerque (2022, p. RB-14.2-14.5), a dispensa do consentimento do paciente não significa que a lei estaria retirando o dever de proteção de dados que cabe ao agente de tratamento; ao revés, a primazia é pelo consentimento do paciente e, nas hipóteses que a lei o dispensa, é igualmente necessário que o agente de tratamento assegure os direitos dos titulares, o que se desdobra nas obrigações de garantir a

[34] Segundo o artigo 5º, III e XI, da LGPD, o dado anonimizado é aquele que perde sua característica de dado pessoal, assim, a anonimização do dado se refere a emprego de mecanismos disponíveis na época do tratamento com o escopo de retirar do dado sua qualidade de pessoal, desassociando-o do indivíduo a que se refere.

[35] Acerca da pseudoanonimização dos dados pessoais, dispõe o art. 13, da LGPD, de 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 do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme 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". (...). § 4º. "Para os efeitos deste artigo, a *pseudonimização* é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro". *(grifos nossos*). (Brasil. L. 13.709/2018). Ou seja, conforme Bruno Bioni (2020, p. 195), diferentemente da anonimização, em se tratando de pseudoanonimização, "Na pseudoanonimização, as informações adicionais que permitiriam a identificação do titular são mantidas em separado pelos agentes de tratamento, que podem, assim, reidentificar os dados se fizerem uso dessa informação. Contudo, caso excluam essas informações adicionais, os agentes não mais poderão efetuar a reidentificação "por meios próprios", caracterizando, assim, uma técnica de anonimização. É nesse sentido que a pseudoanonimização seria "o meio do caminho" para a anonimização".

segurança dos dados coletados (seja em meio físico ou eletrônico), assim como a revelação do dado, quando necessária, com segurança.

Portanto, a legislação de proteção de dados pessoais estabelece critérios para o tratamento de dados sensíveis, com destaque, aqui, neste estudo, para os dados pessoais de saúde. Nota-se que a lei busca equilibrar o interesse dos titulares com o interesse público no tratamento dos dados.

Contudo, para além do dever de tratamento de dados pessoais sensíveis, de acordo com a base legal, é necessário, também, assegurar a integridade e segurança deles; e, portanto, não cumprindo esse dever, exsurge o dever de reparação. Só ressaltando que a responsabilidade civil não é a única consequência da ilicitude, à medida que se verifica, por exemplo, como no art. 187, do Código Civil, uma espécie de ilicitude desvinculada do dano, ou seja, o tratamento de dados pode ocorrer de forma abusiva, contrária aos ditames da boa-fé.

No entanto, ressalta-se que o que realmente se busca é que sejam evitados o tratamento de dados de maneira irregular; é importante um agir do poder público de maneira cuidadosa, com segurança, por meio de deveres de conduta de natureza preventiva evitando danos em detrimento da integridade física do cidadão.

E tal prevenção deve ser mais e mais preponderante quando envolvem a utilização de dados pessoais no âmbito de cidades que passam a ser reconhecidas como *inteligentes*; *inteligentes*, à medida que incorporam grande volume de informações para o planejamento e a consecução de políticas públicas. Tendo em mira que o acesso aos bens, serviços e equipamentos públicos devem ser reconhecidos como direito de todos os cidadãos que vivem na *urbe*.

4 ASPECTOS DA RESPONSABILIDADE CIVIL DO MUNICÍPIO EM CASOS DE VIOLAÇÃO À LGPD

Na cidade inteligente, considerando a maior conexão entre tecnologia, digitalização de serviços públicos, e a necessidade de cidades mais inclusiva, todos esses aspectos inspiram uma arquitetura mais desmaterializada fundada no acesso e, portanto, a proteção de dados ganha destaque, eis que, ela demanda coleta e tratamento de dados pessoais. E que, neste estudo, referem-se à dados de saúde, enquanto sensíveis.

Assim, é necessário considerar a responsabilidade civil do município em relação ao ilícito – que é pressuposto do dever de indenizar porque ele significa contrariedade ao direito – envolvendo os danos associados ao tratamento indevido de dados pessoais sensíveis no âmbito da saúde pública, enquanto controlador; e neste sentido, pode abranger questões envolvendo todo o ciclo de vida dos dados pessoais, desde a coleta até a sua eliminação indevida no âmbito da prestação de serviço em saúde

Acrescente-se que o hospital público municipal também assume a posição de controlador, à medida que ele coleta dados sensíveis dos munícipes que por ali transitam e buscam atendimento. Como bem destaca Patrícia Peck (2019, n.p.), sobre dados pessoais associados à saúde (sensíveis),

> devemos lembrar que há todo um ecossistema interligado, que vai da clínica médica ao hospital, perpassa o laboratório, a farmácia, o próprio paciente e os agentes de saúde, bem como toda a esfera pública - como o Sistema Único de Saúde (SUS). Ou seja, alcança desde o registro de um simples cadastro em um consultório até a entrada em um PS de um hospital (público ou privado).

Assim, este tópico não tem a pretensão de exaurir a matéria, até porque, como a LGPD é relativamente recente no ordenamento jurídico brasileiro, a doutrina, os novos interesses e os valores podem inspirar novos rumos na interpretação.

Há, outrossim, uma crítica acerca da responsabilização envolvendo proteção de dados, conforme o estágio da segurança deles.

Isto é, apesar da adoção pelo agente de tratamento de dados de melhores práticas no assunto, não há como eliminar todos os riscos de tratamento irregular e/ou vazamentos; porém, estas situações não excluem as responsabilidades da Administração Pública municipal.

Registre-se que há, sim, o dever de mitigar riscos a um nível aceitável pela gestão pública municipal, conforme a doutrina se fortaleça para destacar mais e mais a função preventiva da responsabilidade civil, pela qual, diante dos riscos e incertezas da sociedade hodierna, busca-se a adoção de uma conduta orientada a evitar que os danos ocorram ou continuem a ocorrer (Rosenvald; Braga Netto, 2024).

A LGPD tem um papel central em matéria de proteção de dados pessoais[36], mas ela não inaugura um novo regime de responsabilização.

[36] Não vamos aqui abordar a análise crítica, sobre sua eficácia e nem os desafios a frente para que ela seja cada vez mais exigida.

Nessa rota, há de se pontuar que a LGPD não prevê a natureza da responsabilidade civil na questão de tratamento de dados, *i.e.*, se objetiva ou subjetiva (Tomasevicius Filho, 2021, p. RB-10.4; Tepedino; Terra; Guedes, 2023, p. 297). O regime pressupõe uma interpretação dialógica entre Código Civil e LGPD, buscando, também, considerar as circunstâncias no caso concreto (Tomasevicius Filho, 2021, p. RB-10.4) e, para tanto, é importante ter em mira o direito à cidade e a tutela dos que nela vivem em todas as dimensões.

No caso do município, enquanto controlador de dados pessoais, por se tratar de um ente da Federação, atrai, inexoravelmente, a incidência da Constituição Federal, notadamente a disposição do art. 37, §6º[37], que prevê a responsabilidade da pessoa jurídica de direito público pela reparação de danos a terceiros, assegurado o direito de regresso contra o responsável.

Sobre a natureza dessa responsabilidade no âmbito da LGPD, Tomasevicius Filho (2021, p. RB-10.4) entende que se trata de objetiva, ou seja, não é necessária a discussão do elemento culpa *lato sensu*, sendo, bastante, a prova dos demais pressupostos da responsabilidade civil, quais sejam: a conduta, o dano e o nexo de causalidade.

Mas, ainda, há um desdobramento a ser analisado para identificação com clareza da natureza da responsabilidade civil do poder público municipal.

Necessária a averiguação da espécie de conduta que origina o dano: se é por ação ou se é por omissão. Quando se tratar de conduta comissiva, ou seja, de uma ação, a responsabilidade é a objetiva, por força do texto constitucional, não parecendo haver profícua discussão doutrinária nesse ponto (Carvalho Filho, 2022, p. 515).

Contudo, quando a conduta em discussão é na modalidade omissiva, a natureza da responsabilidade civil pode ser subjetiva ou objetiva, de modo que a identificação demanda análise se a omissão estatal é de cunho *genérico* ou *específico* (Carvalho Filho, 2022, p. 515-516). Explica-se.

A omissão considerada como *genérica* é aquela que o Estado deixa de atuar em vários de seus deveres (como na educação, saúde, segurança, meio ambiente, *etc.*). Contudo, o Estado não assume a figura de garantidor universal, não possui responsabilidade integral e há limitações a efetivação de direitos, como a ausência de recursos financeiros ou mal

[37] Art. 37, §6º, CF: "As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa".

investimento, de modo que a exigência de ações perenes em todas as áreas de responsabilidade estatal não se mostraria razoável[38]. Nesse cenário, a responsabilização se dá na forma subjetiva, devendo-se verificar a culpa *lato sensu* da Administração (Carvalho Filho, 2022, p. 516; Pereira; Alvim, 2020, p. RB-45.3).

Diversa é a situação de omissão da Administração quando ela se revela como *específica*.

Este atributo de *específica* é caracterizada quando o Estado tinha o dever específico de evitar a ocorrência do dano, hipótese na qual sua responsabilização se dá de forma objetiva (Carvalho Filho, 2022, p. 516; Pereira; Alvim, 2020, p. RB-45.3).

Tratando de proteção de dados pessoais, a omissão da Administração em adotar procedimentos de segurança na operação com dados pessoais será omissão *específica*; notadamente, pela expressa previsão de princípios da segurança e da prevenção, assim, o regime de responsabilização cível é o objetivo (Pereira; Alvim, 2020, p. RB-45.4).

Outrossim, há parte da doutrina que compreende que a LGPD impôs o regime da responsabilidade subjetiva como regra geral. A esse respeito, Tepedino, Terra e Guedes (2023, p. 298) compreendem que a LGPD estabelece a responsabilidade civil subjetiva como regra, eis que toda a estrutura dessa lei foi pautada na criação de deveres de cuidado a serem seguidos pelo agente de tratamento de dados, o que atrai a análise do elemento culpa, sob pena de se se entender o contrário (responsabilidade objetiva), o que significaria ser prescindível a enumeração de tantos deveres, eis que, na aferição da responsabilidade, não há de se perquirir sobre a ilicitude da conduta do agente de tratamento.

Todavia, considerar a responsabilidade trazida pela LGPD como subjetiva exige reflexão sobre eventual inconstitucionalidade dessa lei ordinária diante da previsão do artigo 37, §6º, da Constituição Federal[39], que, como visto anteriormente, traz hipótese de responsabilidade objetiva da Administração.

---

[38] Carvalho Filho (2022, p. 516) ensina que "Não há dúvida de que o Estado é omisso no cumprimento de vários de seus deveres genéricos: há carências nos setores da educação, saúde, segurança, habitação, emprego, meio ambiente, proteção à maternidade e à infância, previdência social, enfim em todos os direitos sociais (previstos, aliás, no art. 6º da CF). Mas o atendimento dessas demandas reclama a implementação de políticas públicas para as quais o Estado nem sempre conta com recursos financeiros suficientes (ou conta, mas investe mal). Tais omissões, por genéricas que são, não rendem ensejo à responsabilidade civil do Estado, mas sim à eventual responsabilização política de seus dirigentes".

[39] Art. 37, §6º, CF: "As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa".

Registre-se, porém, que a jurisprudência poderá se firmar, quiçá em caráter vinculante, em um ou outro sentido no futuro, sedimentando um posicionamento a ser aplicado na resolução de casos concretos.

No atual contexto, consoante pesquisa realizada, tomando como parâmetros. <responsabilidade civil> , <LGPD> e <Administração Pública>, não se vislumbram julgados vinculantes da Corte Suprema brasileira.

A ADI 6649, julgada em 15 de setembro de 2022 pelo Tribunal Pleno e relatada pelo Min. Gilmar Mendes, discutiu a matéria de forma incidental. O voto do Ministro Relator menciona que a responsabilidade civil pelos danos a particulares oriundos de tratamento de dados pelo Poder Público em descompasso ao disposto na LGPD deverá ocorrer na forma dos artigos 42 e seguintes da LGPD, ou seja, apenas mencionando a cláusula geral de responsabilidade trazida nesse diploma legal[40].

Pontua-se, que a responsabilização na forma objetiva é aquela estabelecida na relação entre o titular do dado pessoal que teve a violação a proteção em face do município. Diversa é a figura da responsabilidade entre a Administração e o agente público que tenha sido responsável pela violação ao dado pessoal, que, por expressa previsão constitucional, responde, em ação de regresso, de maneira subjetiva, ou seja, é necessária a verificação de dolo ou culpa em sua conduta.

Embora não defina a natureza da responsabilidade civil, a LGPD traz algumas previsões a respeito dessa matéria, dispostas na Seção III do Capítulo VI, a saber: a) responsabilidade do agente em razão do tratamento irregular de dados (art. 44, LGPD)[41] e b) responsabilidade pela violação de regras de segurança no tratamento de dados pessoais (art. 44, parágrafo único, LGPD)[42].

---

[40]"o tratamento de dados pessoais promovido por órgãos públicos ao arrepio dos parâmetros legais e constitucionais (ingerência) importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, na forma dos arts. 42 e seguintes da Lei 13.709/2018, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa" (Brasil, 2023, p. 91).

[41] Art. 42 da LGPD: "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo".

[42] Art. 44 da LGPD: "o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
I - o modo pelo qual é realizado;
II - o resultado e os riscos que razoavelmente dele se esperam;
III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado".

No primeiro caso, a própria lei traz como parâmetros de avaliação da (ir) regularidade relacionado ao modo pelo qual o tratamento é feito (inciso I, art. 44, LGPD), e o resultado e os riscos que razoavelmente se espera desse tratamento (inciso II, art. 44, LGPD) e as técnicas de tratamento disponíveis à época dos fatos (inciso III, art. 44, LGPD).

Ditas balizas revelam que a avaliação da conformidade do tratamento do dado pessoal à LGPD deve ser casuística e de forma proporcional ao estado das técnicas de segurança da informação, que não conseguem eliminar complementarmente o risco de tratamento irregular do dado, mas sim reduzem-no a um patamar minimamente aceitável (Tamer, 2022, p. 296).

Ressalta-se a posição deste trabalho segundo a qual a análise da responsabilidade civil na LGPD deve ocorrer sob perspectiva objetiva, retomando-se a Teoria do Risco Administrativo enquanto fundamento da responsabilidade objetiva estatal na promoção de justiça social: como o Estado tem mais poderes jurídicos, políticos e econômicos do que o administrado, é necessário que também tenha um risco naturalmente maior no desempenho de suas atividades (Carvalho Filho, 2022, p. 465).

Seja então tanto por uma conduta comissiva da Administração Pública, a teor da previsão constitucional do art. 37, §6º, seja quanto pelo entendimento de, em se tratando de conduta omissiva que culmine em violação à proteção de dados, há omissão específica do Poder Público, o que atrai também a responsabilidade objetiva à matéria.

Nessa última hipótese, a ausência da atuação do Estado é que cria a situação propícia para a produção do dano relativo à proteção de dados pessoais, quando, em verdade, tinha o Estado o dever de impedir sua ocorrência, sendo úteis a essa avaliação, inclusive, as diretrizes previstas no art. 44 da LGPD, as quais permitem contextualizar a (ir) regularidade do tratamento do dado naquela época específica.

Some-se a isso a necessidade de observância pelo Poder Público aos princípios da proteção e garantia à segurança e privacidade do titular de danos que se amolda de forma mais escorreita à responsabilidade objetiva. Ainda mais em um futuro no qual decisões automatizadas por tecnologias de inteligência artificial tendem a ser mais frequentes, muitas vezes com algoritmos complexos que exigem conhecimento muito aprofundado e específico, que demandam maior proteção ao titular do dado, assim como maior responsabilidade do agente de tratamento em ações de tratamento de dados.

Para além da responsabilização cível, a LGPD também discorre sobre condutas que objetivam prevenir a ocorrência do tratamento irregular, tal qual o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

O RIPD é uma forma de estudo preventivo das atividades de tratamentos de dados pelo agente buscando prevenir a violação ao dado: é o documento do controlador que descreve os riscos às liberdades civis e aos direitos fundamentais ocasionados pelo tratamento de dados pessoais a ser realizado, assim como apresenta medidas para mitigação de risco a esses direitos[43].

Quanto à obrigatoriedade de sua realização, não há na lei dispositivo que expressamente obrigue. Conforme divulgado pela própria ANPD em seu *site*, ainda não existe um regulamento definitivo sobre o RIPD. Contudo, a Autoridade elenca como critério de elaboração do RIPD o alto risco à garantia dos princípios da LGPD, assim como os direitos e liberdades dos titulares (Brasil, 2023, n.p.).

Igualmente não se tem conceito definitivo do que caracterize esse nível de risco alto, orientando a ANPD que, a análise seja casuística, quando verificado ao menos um critério geral: a) tratamento em larga escala e/ou b) afetar significativamente interesses e direitos fundamentais dos titulares; e um critério específico: a) uso de tecnologias emergentes ou inovadoras; b) vigilância ou controle de zonas acessíveis ao público; c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais e d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, adolescentes e de idosos (Brasil, 2023, n.p.).

Especificamente ao Poder Público, o artigo 32 da LGPD prevê que a ANPD poderá *solicitar* a publicação do RIPD pelos órgãos públicos, assim como poderá *sugerir* a adoção de boas práticas. Aliás, a preocupação com o tratamento de dados sensíveis associados à construção de políticas públicas, perpassa, necessariamente pelo crescente diálogo entre direito e políticas públicas[44].

---

[43] Art. 5º, XVII da LGPD: "relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;"

[44] Sobre políticas públicas e Direito, "busca-se entender as novas configurações do Estado, seus papeis e modos de ação, não mais redutíveis à estrutura monolítica tradicional que ocupava o centro único da esfera política e atuava como fonte exclusiva do Direito. Documentar, analisar e compreender de forma sistemática esses novos padrões de ação estatal, em sua dimensão jurídica, constitui razão de ser da abordagem Direito e Políticas Públicas. Seu objeto é a ação governamental coordenada e em escala ampla, para atuar sobre problemas complexos, em estratégias juridicamente informadas, para estender as conquistas civilizatórias a todas as pessoas" (Bucci, 2019, p. 809).

Veja-se que as terminologias utilizadas nesse dispositivo legal se diferem da possibilidade de fazer *requisição* do RIPD e *exigência* de boas práticas ao Poder Público pela ANDP (Tamer, 2022, p. 247-248), o que, no mínimo, permite discussões sobre as consequências jurídicas de eventual descumprimento de um comando da ANPD.

Noutro giro, o artigo 38 da LGPD[45] prevê que a ANPD poderá *determinar* ao controlador que elabore o RIPD para suas operações de tratamento de dados pessoais, sensíveis ou não, resguardando-se os segredos comercial e industrial. Obviamente aqui, questões comerciais e industriais, referem-se à iniciativa privada. Contudo, há, no artigo, a condicionante de que essa determinação deve ser regulamentada pela ANPD.

De qualquer modo, apesar de incertezas sobre a necessidade de elaboração do RIPD e em quais hipóteses, é necessário chamar a atenção para a potencialidade dessa ferramenta como forma de buscar prevenir a violação aos direitos dos titulares por um tratamento irregular de seus dados pessoais, principalmente quando se trata na saúde, cujos dados são características e atributos personalíssimos e essenciais do indivíduo.

Ao elaborar o mapeamento de todo o ciclo de vida do dado pessoal, o agente de tratamento consegue compreender o processo de tratamento de dados pessoais como um todo e cada uma de suas etapas singulares, possibilitando a análise de falhas, gargalos e pontos que podem ser melhorados a fim de se promover uma atividade de tratamento orientada aos preceitos da LGPD e que busque proteger os direitos dos titulares.

Por fim, ressalta-se que a responsabilização cível prevista na LGPD concorre com outras espécies, como administrativa e penal, notadamente em função da independência entre elas (Carvalho Filho, 2022, p. 499). Aliás, a própria LGPD dispõe, no seu art. 52, sobre a responsabilização na esfera administrativa.

Por derradeiro, o artigo 42, da LGPD também reconhece a possibilidade da tutela coletiva (como ação civil pública, por exemplo), por exemplo, grande vazamento de dados de saúde constantes em um banco de dados de uma secretaria de saúde municipal ou hospital público municipal.

5 CONSIDERAÇÕES FINAIS

[45] Art. 38, *caput*, da LGPD: "A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial".

Este trabalho pretendeu estudar o panorama da responsabilidade civil em caso de violação a direito dos titulares de dados pessoais no escopo da LGPD com direcionamento ao panorama das cidades inteligentes, notadamente a área da saúde desses ambientes urbanos.

Como visto, apesar de inexistir consenso sobre o que se trata cidade inteligente, um núcleo comum versa sobre o emprego das TICs nos mais diversos setores da urbe, tais como a saúde, a fim de potencializar a resolução de problemas, voltando-se para a melhoria do serviço de saúde.

Outrossim, à medida que inovações tecnológicas vêm com o escopo de melhorar a vida dos indivíduos, há o surgimento de novas preocupações, que são de interesse do Direito, sobremaneira a questão da proteção de dados pessoais, que dizem respeito a características da *persona*, ainda mais na saúde, revelando informações muito caras a sua própria personalidade.

Assim, adquire relevância instrumentos jurídicos de proteção de dados e os mecanismos de responsabilização cível por ele trazidos, a fim de se coibir o tratamento irregular desses dados pessoais, assim como de se prezar por técnicas de segurança da informação. Nesse sentido, em solo brasileiro, a LGPD é figura central na matéria, eis que se trata de diploma jurídico especializado no assunto de proteção de dados pessoais.

Viu-se que, por expressa previsão legal, os dados de saúde das pessoas naturais são considerados como sensíveis, demandando proteção mais acurada, haja vista o potencial lesivo majorado em virtude de vazamentos e/ou tratamento irregular. Assim, uma das bases legais na qual se deva fundar o tratamento dos dados de saúde da pessoa é o consentimento do titular, que deve ser informado e espontâneo. Mas, para além dessa base, há outras formas de tratamento que dispensam o consentimento, muitas das quais prestigiam a supremacia do interesse público sobre o particular, como nos casos de execução de políticas públicas e tutela da saúde daquele indivíduo.

É de se anotar que, mesmo nos casos de dispensa de consentimento, isso não significa que não incidirá a LPGD. Ao revés, a lei traz uma estrutura principiológica aplicável a quaisquer hipóteses de tratamento, adquirindo especial importância no campo da saúde os princípios da finalidade daquele tratamento de dado e da não discriminação ilícita e abusiva.

Por fim, em caso de violação aos preceitos da LGPD, há possibilidade de responsabilização municipal no âmbito do Direito Civil. Para tanto, viu-se a controvérsia existente acerca da natureza da responsabilidade desse ente público: se subjetiva ou objetiva, notadamente por inexistir previsão legal expressa na LGPD. Compreendeu-se que, ao se fazer

uma leitura à luz da Constituição Federal, o regime de responsabilização é o objetivo, ou seja, aquele que dispensa a análise do elemento culpa em sentido largo.

Registre-se também que a LGPD se preocupa em equacionar a matéria de responsabilidade civil ao atual estágio tecnológico da segurança da informação, que não consegue eliminar por completo os riscos afetos a esse novo mundo de dados pessoais, mas sim de que sejam exigidas medidas visando minimizá-los, conforme despontam-se deveres de conduta. A matéria ainda se encontra incipiente no ordenamento jurídico brasileiro, sendo que novas reflexões doutrinárias surgirão e, eventualmente, a jurisprudência se posicionará sobre o assunto.

Por fim, há de se ressaltar que a responsabilização civil não é a única possível, notadamente porque a própria LGPD prevê uma estrutura de responsabilização administrativa, com base em um processo administrativo que busque assegurar o contraditório e a ampla defesa.

Acerca da responsabilidade civil municipal, em matéria de tratamento de dados pessoais sensíveis, não tem como desconsiderar que há muitos municípios que tem déficit orçamentário, e assim, não tem como eles investirem em tecnologia e infraestrutura para implantarem os níveis de segurança exigidos para proteção de dados pessoais.

Imaginemos a situação hipotética: um indivíduo que trabalha numa concessionária de serviço público da cidade, não dispondo de hospital público, a secretaria de saúde local decide então, transferi-lo para o hospital municipal de outra cidade – totalmente inteligente – e nela realizam-se vários exames médicos e depois os resultados são enviados para a secretaria de saúde daquela cidade originária. A secretaria local, ao receber os resultados dos exames do dito cidadão, não dispõe de infraestrutura necessária para atender e cumprir os níveis de segurança dos dados pessoais do indivíduo, simplesmente porque a cidade tem déficit orçamentário. Denota-se, portanto, que não podemos adotar, simplesmente, uma responsabilidade objetiva, por si só, sem uma perspectiva mais global de toda a situação que envolve o ecossistema de tráfego de dados pessoais sensíveis na esfera pública.

Enfim, à medida que se avança neste novo paradigma da era dos dados pessoais, é inevitável que surjam novos desafios e questões jurídicas. Portanto, é fundamental que a comunidade jurídica e os órgãos competentes estejam atentos às mudanças e passem a incluir nas suas prioridades, uma cultura de dados, inclusive, no âmbito da gestão pública municipal.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). *NBR ISO 37122:* cidades e comunidades sustentáveis: indicadores para cidades inteligentes. Rio de Janeiro, 2021. p. 33-36.

ALBUQUERQUE, Aline. Saúde digital e a LGPD sob o enfoque do direito do paciente e da sua vulnerabilidade acrescida. *In:* DALLARI, Analluza Bolivar; AITH, Fernando (coord.). *LGPD na saúde digital*. São Paulo: Thomson Reuters, 2022. p. RB-14.1 – RB-14.7. *E-book*.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *Cadernos Jurídicos*, São Paulo, ano 21, nº 53, p. 191-201, jan./mar. 2020.

BLOOMBERG, Michael. Foreword. *In:* GOLDSMITH, Stephen; CRAWFORD, Susan. *The Responsive City:* Engaging Communities Through Data-Smart Governance. Nova York: Jossey Bass, 2014.

BLUM, Renato Opice. MALDONADO, Viviane Nóbrega. *LGPD – Lei Geral de Proteção de Dados Comentada.* 2ª edição. São Paulo: Revista dos Tribunais, 2019.

BRASIL. ANPD. *Tratamento de dados pessoais pelo poder público*. Brasília, jan. 2022.

BRASIL. ANPD. *Relatório de Impacto à Proteção de Dados Pessoais (RIPD).* 06 abr. 2023. n.p. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd#p3. Acesso em: 18 mai. 2024.

BRASIL. Carta Brasileira para Cidades Inteligentes. 2021. Disponível em: https://www.gov.br/cidades/pt-br/acesso-a-informacao/acoes-e-programas/desenvolvimento-urbano-e-metropolitano/projeto-andus/carta-brasileira-para-cidades-inteligentes/CartaBrasileiraparaCidadesInteligentes2.pdf. Acesso em: 13 mai. 2024.

BRASIL. Supremo Tribunal Federal. ADI nº 6649. Relator: Ministro Gilmar Mendes. Tribunal Pleno. Brasília, 15 set. 2022. *Diário Oficial da União.* Brasília, 19 jun. 2023. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768683585. Acesso em: 18 mai. 2024.

BRASIL. L. 13.787/2018. Dispõe sobre digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 18 mai. 2024.

BUCCI, Maria Paula Dallari. Método e aplicações da abordagem direito e políticas públicas (DPP). *Revista Estudos Institucionais*, v. 5, n. 3, p. 791-832, set./dez. 2019.

CARVALHO FILHO, José dos Santos. Manual de direito administrativo. 36 ed. Barueri: Atlas, 2022. *E-book*.

CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 16 ed. Barueri: Atlas, 2023. *E-book.*

CAVET, Caroline Amadori. Saúde digital: entre os dados e o consentimento. *Lex Medicinae*, ano 20, n. 40, p. 21-35, 2023.

FREITAS, Márcia Araújo Sabino de; PÉRISSÉ, André Reynaldo Santos. Controle de epidemias, rastreamento de contatos e privacidade nas favelas: a vigilância em saúde em meio a potencialidades, desafios e equívocos do brasil na pandemia de covid-19. *In:* SILVA, Angélica Baptista; CUNHA, Francisco José Aragão Pedroza [Organizadores]. *Lei geral de proteção de dados e controle social da saúde*. Porto Alegre, Editora Rede Unida, 2023, p. 32-58.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In:* FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. 3 ed. São Paulo: Thomson Reuters, 2023. p. RB-16.1 - RB-16.7. *E-book.*

KUMMITHA, Rama Krishna Reddy; CRUTZEN, Nathalie. How do we understand smart cities? An evolutionary perspective. *Cities*, v. 67, p. 43-52, 2017.

MARQUES, Cláudia Lima. Diálogo das fontes. *In:* BENJAMIN, Antonio Herman V.; MARQUES, Cláudia Lima; BESSA, Leonardo Roscoe. *Manual de direito do consumidor.* 7 ed. São Paulo: Revista dos Tribunais, 2016.

MORA, Luca; BOLICI, Roberto; DEAKIN, Mark. The first two decades of smart-city research: A bibliometric analysis. *Journal of Urban Technology*, v. 24, n. 1, p. 1-25, 2017.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). *R. Dir. Gar. Fund.*, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

NAM, Taewoo; PARDO, Theresa A. Conceptualizing Smart City with Dimensions of Technology, People, and Institutions. *In:* The 12th Annual International Digital Government Research Conference, College Park, Maryland. *Proceedings [...].* Maryland: ACM Press, 2011, p. 282- 291.

ONU-HABITAT. *World Cities Report 2022:* envisaging the future of cities. Nairobi: United Nations Human Settlements Programme (UN-Habitat), 2022. Disponível em: https://unhabitat.org/sites/default/files/2022/06/wcr_2022.pdf. Acesso em: 05 mai. 2024.

ORGANIZAÇÃO MUNDIAL DA SAÚDE (OMS). *Estrategia mundial sobre salud digital 2020–2025*. Genebra: Organização Mundial da Saúde. 2021. Disponível em: https://apps.who.int/iris/handle/10665/344251. Acesso em: 06 mai. 2024.

PECK, Patrícia. LGPD e saúde: os fins justificam os meios? *In:* BRASIL. *SERPRO e LGPD:* segurança e inovação. 23 set. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude. Acesso em: 10 mai. 2024.

PEREIRA, Flávio Henrique Unes; ALVIM, Rafael da Silva. A responsabilidade civil do Estado por danos decorrentes do tratamento de dados pessoais: um estudo de caso. *In:* DAL POZZO, Augusto Neves; MARTINS, Ricado Marcondes (coord.). *LGPD e administração pública:* uma análise ampla dos impactos. São Paulo: Thomson Reuters, 2020. p. RB-45.1 – RB. 45.7. *E-book*.

PREFEITURA PORTO ALEGRE. Saúde alerta para risco de contaminação por leptospirose (06/5/2024). Disponível em: https://prefeitura.poa.br/sms/noticias/saude-alerta-para-risco-de-contaminacao-por-leptospirose-0. Acesso em: 8 mai. 2024.

ROSENVALD, Nelson; BRAGA NETTO, Felipe. *Responsabilidade civil:* teoria geral. Indaiatuba: Foco, 2024. *E-book*.

SCAFF, Fernando Campos. O ato médico, os direitos do paciente e a LGPD. *In:* DALLARI, Analluza Bolivar; AITH, Fernando (coord.). *LGPD na saúde digital*. São Paulo: Thomson Reuters, 2022. p. RB-10.1 – RB-10.8. *E-book*.

SCHWAB, Klaus. *A quarta revolução industrial.* [Trad. Daniel Moreira Miranda]. São Paulo, Edipro, 2016.

SILVA, Carlos Henrique Costa da. Cidades mundiais na contemporaneidade. *Revista Geosul*, Florianópolis, v. 20, n. 39, p 7-27, jan./jun. 2005.

TAMER, Maurício. *LGPD:* comentada artigo por artigo: interpretação e aplicação da lei. 2 ed. São Paulo: Rideel, 2022. *E-book*.

TEPEDINO, Gustavo. TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. *Fundamentos do direito civil:* responsabilidade civil. 4 ed. Rio de Janeiro, Forense, 2023. v. 4. *E-book*.

TOMASEVICIUS FILHO, Eduardo. Responsabilidade civil na LGPD na área da saúde. *In:* DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz de Campos (coord.). *LGPD na saúde*. São Paulo: Thomson Reuters, 2021. p. RB-10.1 – RB. 10.7. *E-book*.

VAINZOF, Rony. Capítulo I: disposições preliminares. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD:* Lei Geral de Proteção de dados comentada. 4 ed. São Paulo: Thomson Reuters, 2022. p. RL-1.2. *E-book.*

WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ci. Inf.*, Brasília, v. 29, n. 2, p. 71-77, mai./ago. 2000.

WHO – WORLD HEALTH ORGANIZATION. WHO Director-General's opening remarksat the media briefing on COVID-19 (11/3/2020). Disponível em: https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. Acesso: 8 mai. 2024.

BIOGRAFIA

Cláudio José Franzolin

Doutor e Mestre em Direito pela Pontifícia Universidade Católica de São Paulo. Professor doutor pesquisador e titular no Programa de Mestrado em Direito da Pontifícia Universidade Católica de Campinas, onde também é professor de direito civil, consumidor e ambiental, nos cursos de graduação de Direito e de Engenharia Ambiental. Autor de capítulos de livros e de artigos científicos. Advogado.

CONTATOS

http://lattes.cnpq.br/0120973253492591
https://orcid.org/0000-0002-9594-1238
cfranzol30@gmail.com

Letícia Pardo Rodrigues do Carmo

CONTATOS

http://lattes.cnpq.br/9288277560276032
https://orcid.org/0000-0003-1885-2669
pardoleticia@outlook.com

Mestra em Direito pela Pontifícia Universidade Católica de Campinas (PUC-Campinas). Pós-graduada em Direito Médico e Bioética (EBRADI). Graduada em Direito pela PUC-Campinas com ênfase em Direito Privado pela mesma instituição, Campinas, São Paulo, Brasil.