Centro Universitário de Brasília

ANA LUÍZA GONÇALVES COSTA DA LUZ

PROTEÇÃO DE DADOS PESSOAIS EM CONTRATOS DE TERCEIRIZAÇÃO DE TI NA SAÚDE PÚBLICA: LACUNAS CONTRATUAIS, RESPONSABILIZAÇÃO ENTRE CONTROLADOR E OPERADOR À LUZ DA LGPD - LIÇÕES DO CASO ZELLO

Brasília
2026

ANA LUÍZA GONÇALVES COSTA DA LUZ

PROTEÇÃO DE DADOS PESSOAIS EM CONTRATOS DE TERCEIRIZAÇÃO DE TI NA SAÚDE PÚBLICA: LACUNAS CONTRATUAIS, RESPONSABILIZAÇÃO ENTRE CONTROLADOR E OPERADOR À LUZ DA LGPD - LIÇÕES DO CASO ZELLO

Trabalho apresentado ao Centro Universitário de Brasília (CEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Direito do Trabalho e Previdenciário.
Orientadora: Prof.ª Dr.ª Tatiana Reinehr de Oliveira

Brasília
2026

ANA LUÍZA GONÇALVES COSTA DA LUZ

PROTEÇÃO DE DADOS PESSOAIS EM CONTRATOS DE TERCEIRIZAÇÃO DE TI NA SAÚDE PÚBLICA: LACUNAS CONTRATUAIS, RESPONSABILIZAÇÃO ENTRE CONTROLADOR E OPERADOR À LUZ DA LGPD - LIÇÕES DO CASO ZELLO

Trabalho apresentado ao Centro Universitário de Brasília (CEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Direito - Trabalho e Previdenciário.

Orientadora: Prof.ª Dr.ª Tatiana Reinehr de Oliveira

Brasília, março de 2026.

Banca Examinadora

_____

Profa. Dra. Tatiana Reinehr de Oliveira

_____

Prof. Dr. Gilson Ciarallo

_____

Prof. Me. Kátia Adriana Cardoso de Oliveira

Àqueles que foram estrelas firmes no meu céu inquieto, permitindo que eu encontrasse direção mesmo quando a noite era densa, livre para existir no ritmo próprio da luz que descobre, ao seu tempo, por onde seguir.

AGRADECIMENTOS

À minha mãe, Verinha, e ao meu pai, Gerson (*in memoriam*), por terem me formado com amor e por continuarem presentes em mim, naquilo que sou e no caminho que construo.

Aos meus irmãos, Amanda, Guilherme, Letícia e Isabella, por serem meu alicerce, minha alegria e exemplos constantes de resiliência.

Aos meus sobrinhos, Calebe e Júlia, por iluminarem a minha rotina com gestos simples, espontâneos e cheios de afeto, lembrando-me da beleza que existe nas pequenas alegrias do cotidiano.

À minha filha canina, Lolita, por estar ao meu lado em todos os momentos, oferecendo companhia silenciosa, lambeijos que enxugam lágrimas e uma alegria pura que torna cada dia mais leve.

Ao meu marido, Lucas, por ser o meu lugar favorito no mundo, por me acolher em todas as versões de mim e por transformar cansaço em calma e medo em coragem, como bem traduz a frase de Taylor Swift: “This love is golden.”.

À minha orientadora, professora Tatiana Reinehr, pela generosidade em compartilhar conhecimento, pela paciência nas dúvidas, pela confiança nas minhas escolhas e por iluminar, com delicadeza e firmeza, o caminho desta monografia.

Sobretudo, a Deus, pelo dom da vida, pela força nos dias em que pensei em desistir e pela graça de poder dividir esta caminhada com quem amo.

“A proteção de dados constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea. Relembrar isto a cada momento não é verbosidade, pois toda mudança que afeta a proteção de dados tem impacto sobre o grau de democracia que nós podemos experimentar.”.

Stefano Rodotà

RESUMO

Este trabalho analisa a conformidade dos contratos de terceirização de tecnologia da informação (TI) firmados pelo Ministério da Saúde com a Lei Geral de Proteção de Dados Pessoais (LGPD). Partindo da premissa de que a crescente externalização de serviços digitais, exemplificada pelo sistema e-SUS Notifica e a empresa Zello, amplia a circulação de dados em infraestruturas privadas, a pesquisa investiga como essa prática potencializa riscos de segurança, evidenciados pelos episódios de vazamento de dados de milhões de brasileiros em 2020. O objetivo principal é verificar se os instrumentos contratuais distribuem de forma clara as obrigações entre o ente público (controlador) e as empresas contratadas (operadoras). A problemática central reside na existência de lacunas contratuais, onde cláusulas de sigilo genéricas substituem previsões específicas de proteção de dados, gestão de incidentes e registros de operações de tratamento. Utilizando pesquisa bibliográfica e documental, com foco em editais, termos aditivos e normas como a IN SGD/ME nº 94/2022 e a Lei nº 14.133/2021, o estudo testa a hipótese de que a definição contratual de obrigações específicas para o operador é essencial para o fortalecimento da segurança. A análise indica que a imprecisão contratual dificulta a atribuição de responsabilidades e fragiliza o controle estatal. Conclui-se que o uso rigoroso de Estudos Técnicos Preliminares e modelos estruturados de governança é indispensável para identificar riscos precocemente e assegurar a efetividade da proteção de dados na Administração Pública federal.

Palavras-chave: Proteção de dados pessoais; Lei Geral de Proteção de Dados; Terceirização de tecnologia da informação; Administração Pública; Contratos administrativos.

ABSTRACT

This study analyzes the compliance of information technology (IT) outsourcing contracts signed by the Ministry of Health with the General Data Protection Law (LGPD). Starting from the premise that the increasing externalization of digital services, exemplified by the e-SUS Notifica system and the company Zello, expands the circulation of personal data within private infrastructures, this research investigates how this practice heightens security risks, as evidenced by the data breach episodes involving millions of Brazilians in 2020. The primary objective is to determine whether contractual instruments clearly distribute obligations between the public entity (the controller) and the contracted companies (the operators). The central problem lies in the existence of contractual gaps, where generic confidentiality clauses replace specific provisions regarding data protection, incident management, and records of processing activities. Using bibliographic and documentary research, focusing on public tenders, addenda, and regulations such as IN SGD/ME No. 94/2022 and Law No. 14.133/2021, the study tests the hypothesis that the contractual definition of specific obligations for the operator is essential for strengthening security. The analysis indicates that contractual ambiguity hinders the allocation of responsibilities and weakens state control. It concludes that the rigorous use of Preliminary Technical Studies and structured governance models is indispensable for identifying risks early and ensuring the effectiveness of data protection in the federal public administration.

Keywords: Personal data protection; General Data Protection Law; Information technology outsourcing; Public Administration; Administrative contracts.

SUMÁRIO

INTRODUÇÃO

A Administração Pública federal, em especial o Ministério da Saúde, depende cada vez mais da contratação de serviços de tecnologia da informação (TI) prestados por empresas terceirizadas. Essa dinâmica institucional faz com que grandes volumes de dados pessoais, inclusive dados sensíveis relacionados à saúde, sejam processados e armazenados em sistemas operados por agentes privados que atuam em nome do poder público, muitas vezes fora da estrutura direta do Estado (Brasil, 2022).

Episódios de vulnerabilidade e vazamentos envolvendo bases do Sistema Único de Saúde (SUS) e sistemas como o e-SUS Notifica demonstraram que falhas técnicas ou fragilidades estruturais podem expor informações de milhões de pessoas, incluindo CPF, endereço e dados médicos. Tais ocorrências geram riscos concretos de violação à privacidade e de uso indevido das informações, além de comprometer a confiança social nas instituições responsáveis pela gestão de bases informacionais de grande escala (Nexo Jornal, 2020; WeLiveSecurity, 2020). Nesse contexto, a proteção de dados pessoais relaciona-se diretamente à legitimidade democrática das instituições públicas, pois, em ambientes de intensa digitalização estatal, a confiança da sociedade na Administração Pública depende não apenas da continuidade e eficiência dos serviços prestados, mas também da capacidade institucional de tratar informações pessoais de forma segura, transparente e conforme os direitos fundamentais.

Nesse cenário, o Ministério da Saúde atua como controlador de extensas bases de dados relacionadas à saúde pública, enquanto empresas contratadas para desenvolvimento e manutenção de sistemas desempenham funções típicas de operadoras no tratamento dessas informações. A forma como as responsabilidades são distribuídas entre Administração Pública e contratadas, portanto, deixa de representar um aspecto meramente burocrático da contratação e assume papel central na proteção dos direitos fundamentais dos titulares de dados.

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabeleceu parâmetros normativos mais rigorosos para as atividades de coleta, armazenamento, compartilhamento e segurança de dados pessoais. O

regime jurídico instituído pela LGPD definiu papéis, deveres e responsabilidades aplicáveis ao tratamento de dados, impondo ao poder público e aos agentes privados que atuam em seu nome a adoção de medidas técnicas e administrativas voltadas à proteção das informações tratadas (Brasil, 2018).

A problemática central desta pesquisa decorre da constatação de que podem existir lacunas normativas nos instrumentos que estruturam contratações públicas de tecnologia da informação no que se refere à delimitação precisa das responsabilidades das empresas responsáveis pelo tratamento de dados. Observa-se que, em diversas contratações, os instrumentos convocatórios e documentos que orientam a contratação apresentam previsões genéricas de sigilo ou confidencialidade, sem estabelecer obrigações específicas relacionadas à proteção de dados pessoais, à gestão de incidentes de segurança, ao registro das operações de tratamento ou à cooperação com o controlador na avaliação de riscos e impactos.

A análise toma como referência o contexto do sistema e-SUS Notifica, desenvolvido para o Ministério da Saúde e associado a episódios de vulnerabilidade divulgados em 2020. Nesse cenário, considera-se a contratação realizada, por intermédio do Departamento de Informática do Sistema Único de Saúde (Datasus), com a empresa Zello Tecnologia da Informação Ltda. (antiga MBA Mobi), não como objeto exclusivo da investigação, mas como exemplo concreto que evidencia os riscos envolvidos na terceirização de serviços de tecnologia da informação (EM, 2020).

A investigação documental concentra-se no edital que estruturou a contratação analisada. A escolha desse documento justifica-se por se tratar do instrumento que estabelece as condições jurídicas e técnicas da contratação, delimitando previamente as obrigações das partes e os parâmetros que orientam a execução contratual. Elaborado em período anterior à edição da Lei Geral de Proteção de Dados Pessoais, o instrumento convocatório não contemplava disposições específicas relacionadas à proteção de dados pessoais. Suas cláusulas refletiam o contexto normativo vigente à época, caracterizado pela predominância de previsões genéricas de sigilo, confidencialidade e segurança da informação institucional (Brasil, 2016).

Com a entrada em vigor da LGPD em setembro de 2020, a Administração Pública federal passou a ter o dever de adequar seus arranjos institucionais e contratuais às novas exigências relacionadas à governança em privacidade, à segurança da informação e à responsabilização no tratamento de dados pessoais

(Brasil, 2018). Nesse contexto, torna-se relevante analisar em que medida os instrumentos que estruturam contratações de tecnologia da informação incorporam parâmetros compatíveis com o novo regime jurídico de proteção de dados.

A partir desse cenário, formula-se a seguinte pergunta de pesquisa: em que medida a imprecisão ou ausência de cláusulas específicas sobre proteção de dados em contratações de tecnologia da informação na Administração Pública pode ampliar a exposição dos titulares de dados a riscos de vazamento, uso indevido ou discriminação, bem como sujeitar o próprio Estado a formas de responsabilização civil, administrativa e reputacional (SERPRO, 2020)?

Busca-se, portanto, investigar se os instrumentos que estruturam contratações públicas de tecnologia da informação delimitam de forma suficiente as obrigações relativas ao tratamento de dados pessoais em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). Avalia-se, nesse contexto, se tais instrumentos estabelecem parâmetros claros de responsabilização entre controlador e operador ou se mantêm ambiguidades capazes de fragilizar a proteção dos titulares.

Para atingir esse objetivo, o estudo adota pesquisa bibliográfica e documental. O referencial normativo e teórico engloba a Lei Geral de Proteção de Dados Pessoais e seus regulamentos, bem como instrumentos institucionais relacionados à governança em privacidade na Administração Pública. Incluem-se, ainda, documentos e guias oficiais sobre proteção de dados nas contratações estatais, além da literatura especializada acerca da terceirização de serviços de tecnologia da informação e da responsabilidade civil do Estado (Brasil, 2018; Brasil, 2022; Bioni, 2020).

A investigação documental recai sobre o edital que orientou a contratação analisada, bem como sobre atos normativos e documentos institucionais relacionados à proteção de dados e à terceirização de TI no Ministério da Saúde, além de registros públicos sobre os incidentes examinados. O marco normativo adotado privilegia a legislação federal, especialmente a Lei nº 13.709/2018, a Lei nº 14.133/2021 e a Instrução Normativa SGD/ME nº 94/2022, aplicável às contratações de TIC no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

Adicionalmente, analisam-se guias orientativos e documentos institucionais elaborados por órgãos da Administração Pública federal. Entre eles, destacam-se o *Guia orientativo sobre segurança da informação para agentes de tratamento de*

pequeno porte e o *Guia orientativo sobre a função do controlador, do operador e do encarregado*, publicados pela Agência Nacional de Proteção de Dados (ANPD)[1], bem como documentos voltados à governança pública e à transformação digital, como o *Referencial básico de governança organizacional para organizações públicas*, do Tribunal de Contas da União, a *Estratégia de Saúde Digital para o Brasil 2020–2028* e a *Política Nacional de Informação e Informática em Saúde*, ambas do Ministério da Saúde.

A relevância do tema decorre das dificuldades que muitos órgãos públicos ainda enfrentam para se adequar integralmente à LGPD, em razão de limitações institucionais, tecnológicas e orçamentárias. Tal contexto gera incertezas quanto aos parâmetros que devem constar dos editais e dos instrumentos contratuais para assegurar, de maneira efetiva e não apenas formal, a segurança da informação e a proteção de dados pessoais (SERPRO, 2020; CRP Computadores, 2025).

A pesquisa parte da hipótese de que a ausência ou insuficiência de cláusulas específicas relativas à governança em privacidade, à segurança da informação e à gestão de incidentes em contratações de tecnologia da informação fragiliza a posição dos titulares de dados. Paralelamente, amplia o risco de responsabilização estatal ao concentrar deveres em normas abstratas, em vez de estabelecer obrigações contratuais concretas dirigidas ao operador responsável pelo tratamento.

Busca-se demonstrar que a inclusão de previsões claras acerca dos papéis das partes, dos limites de utilização dos dados pessoais e dos padrões mínimos de segurança reduz margens para interpretações ambíguas. Igual relevância assume a exigência de registros das operações de tratamento, mecanismos de reporte de incidentes, auditorias e cooperação com autoridades competentes, medidas que contribuem para alinhar a prática administrativa às exigências materiais da LGPD (Brasil, 2018; Brasil, 2022).

Objetiva-se, ademais, contribuir para a formulação de parâmetros objetivos voltados à elaboração e à fiscalização de contratações de tecnologia da informação no setor público. Tal discussão torna-se particularmente relevante diante da rápida informatização do sistema de saúde, fenômeno que convive com vulnerabilidades

[1] A Autoridade Nacional de Proteção de Dados passou a denominar-se **Agência Nacional de Proteção de Dados (ANPD)** após a promulgação da Lei nº 15.352, de 25 de fevereiro de 2026, que alterou sua natureza institucional. Para fins deste trabalho, adota-se essa denominação.

estruturais e com a necessidade de consolidação de uma cultura institucional de proteção de dados na Administração Pública (EPSJV/FIOCRUZ, 2022; Brasil, 2022).

O presente trabalho foi estruturado em três capítulos, além da conclusão. No primeiro capítulo, apresentam-se os fundamentos teóricos e normativos da proteção de dados pessoais na Administração Pública federal, com destaque para a evolução do direito à privacidade e a consolidação da autodeterminação informativa como vetor da tutela da pessoa na sociedade digital. Examina-se a estrutura da Lei nº 13.709/2018 (LGPD), com ênfase em seus princípios orientadores, nos direitos dos titulares e nos deveres de governança aplicáveis ao Poder Público, bem como na delimitação das figuras do controlador e do operador no contexto da terceirização de serviços de tecnologia da informação. A análise também dialoga criticamente com o modelo europeu de proteção de dados (GDPR), apontando as limitações da chamada "tropicalização" da norma europeia diante das assimetrias institucionais brasileiras.

O segundo capítulo proporciona uma análise dos marcos normativos e conceituais que incidem sobre a terceirização de serviços de TI pela Administração Pública federal, com especial atenção à interação entre a LGPD, o Marco Civil da Internet, a Lei de Acesso à Informação e a Nova Lei de Licitações e Contratos Administrativos (Lei nº 14.133/2021). Investigam-se as obrigações jurídicas imputáveis ao operador, os desafios do regime das contratações públicas de TI e os deveres contratuais específicos aptos a traduzir, em cláusulas concretas, as exigências legais de proteção de dados pessoais. A discussão organiza-se em torno de quatro eixos contratuais estruturantes: descrição do tratamento, segurança da informação e governança em privacidade, cooperação e apoio ao controlador, e responsabilidade, sanções e mitigação de riscos.

No terceiro capítulo, apresenta-se como estudo de caso a contratação da empresa Zello Tecnologia da Informação Ltda. pelo Ministério da Saúde, celebrada para o desenvolvimento de sistemas de notificação epidemiológica utilizados durante a pandemia de Covid-19, em especial o e-SUS Notifica. A partir da análise do edital que estruturou a contratação e dos incidentes de segurança ocorridos em 2020, identificam-se as lacunas contratuais e institucionais que permitiram a exposição massiva de dados pessoais sensíveis de saúde, bem como as dificuldades de responsabilização dos agentes de tratamento. Examina-se, ainda, a reiteração de vulnerabilidades no ataque promovido pelo grupo Lapsus$ em dezembro de 2021,

cujo vetor de entrada reproduziu falhas semelhantes às identificadas no caso Zello. Ao final, propõem-se condições institucionais mínimas para a adequada proteção de dados sensíveis em contratos de terceirização de TI em saúde, com destaque para a necessidade de positivação de padrões uniformes em normas internas estruturantes, a exemplo do modelo adotado por outros órgãos da Administração Pública federal.

Por fim, a conclusão sintetiza os principais achados da pesquisa e retoma a tese de que a efetividade da LGPD no setor público depende não apenas da existência formal da norma, mas da construção de uma cultura institucional de governança em privacidade, do aprimoramento dos instrumentos contratuais e da definição clara de responsabilidades entre controlador e operador, especialmente em contextos de tratamento massivo de dados sensíveis.

1 Fundamentos da proteção de dados pessoais na Administração Pública federal e na terceirização de TI

A Lei nº 13.709, de 14 de agosto de 2018, denominada como Lei Geral de Proteção de Dados Pessoais (LGPD), foi editada para disciplinar o tratamento de dados pessoais, inclusive nos meios digitais, por pessoas naturais e jurídicas de direito público e privado. Seu escopo é proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade (Brasil, 2018).

No âmbito da Administração Pública federal, a proteção de dados assume contornos específicos, uma vez que os órgãos e as entidades estatais tratam diariamente grandes volumes de informações dos cidadãos. Parte expressiva desse acervo possui natureza sensível e é indispensável à formulação, à execução e ao monitoramento de políticas públicas. É o caso do Ministério da Saúde, responsável por gerir os extensos cadastros do Sistema Único de Saúde (SUS) e os sistemas de saúde digital, que concentram informações altamente críticas da população (Brasil, 2022).

A crescente digitalização da máquina pública e a ampliação da terceirização de serviços de tecnologia da informação (TI) intensificam a circulação de dados em infraestruturas privadas. O cenário apresentado exige rigor na definição de responsabilidades e na adoção de mecanismos de segurança. Torna-se indispensável, portanto, a correta delimitação dos papéis de controlador e de operador.

Nessa relação, o órgão público figura como controlador, a quem compete decidir sobre as finalidades e os elementos essenciais do tratamento. A empresa contratada, por sua vez, atua como operadora, executando as atividades técnicas em nome do Estado. Essa clareza jurídica é fundamental para assegurar a efetividade da LGPD e para mitigar os riscos de incidentes, de vazamentos e de responsabilização (ANPD, 2021).

Este capítulo tem o objetivo de apresentar os fundamentos teóricos da proteção de dados, a evolução do direito à privacidade e a estrutura normativa da LGPD. O destaque recai sobre os dispositivos que orientam a atuação do Poder Público. O intuito é fornecer o suporte conceitual necessário para a compreensão das lacunas na aplicação da lei e dos riscos gerados aos titulares e à própria Administração.

A partir desse referencial teórico, estabelecem-se as bases para examinar, nos capítulos seguintes, como tais vulnerabilidades se manifestam concretamente nos contratos de TI celebrados pelo Ministério da Saúde. A análise posterior focará, sobretudo, na eficácia da delimitação de responsabilidades entre o ente público controlador e a empresa privada operadora.

1.1 A evolução da proteção de dados pessoais na garantia da privacidade no tratamento de dados contratuais

A proteção de dados pessoais não surge de forma isolada no ordenamento jurídico. Ela se desenvolve a partir da evolução do direito à privacidade e dos direitos da personalidade, reinterpretados à luz das transformações tecnológicas e da consolidação das tecnologias da informação e comunicação (Doneda, 2006).

Tradicionalmente, a tutela da vida privada esteve vinculada à proteção de uma esfera de reserva individual contra ingerências indevidas. Tal perspectiva manifesta-se nos debates clássicos acerca da intimidade, da honra e da imagem no âmbito do direito civil e constitucional. Todavia, tal modelo mostra-se insuficiente diante da relevância assumida pelos bancos de dados, cadastros informatizados e sistemas digitais na sociedade contemporânea. Esses instrumentos possuem capacidade de registrar, cruzar e analisar informações em larga escala, influenciando comportamentos, oportunidades e formas de participação social (Almeida, 2019).

Sob essa perspectiva, emerge a noção de autodeterminação informativa. Por esse conceito, o titular deve exercer controle sobre a coleta, o uso e a circulação de seus dados pessoais. A proteção de dados passa, assim, a se relacionar diretamente com o livre desenvolvimento da personalidade, uma vez que o tratamento da informação interfere na forma como o indivíduo é percebido, classificado e inserido na sociedade da informação (Doneda, 2006).

No plano europeu, essa releitura da privacidade conduziu à construção de um arcabouço normativo próprio, o qual culminou na elaboração do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), aplicável desde 2018. O GDPR reconhece a proteção de dados pessoais como um direito fundamental autônomo, embora conectado ao direito à vida privada. O documento estabelece princípios,

bases legais e direitos do titular voltados a equilibrar a inovação tecnológica, os interesses econômicos e a salvaguarda da dignidade humana (EDPS; IAPP).

A experiência europeia exerceu influência direta sobre a Lei Geral de Proteção de Dados Pessoais (LGPD). A norma brasileira incorporou categorias centrais do regime estabelecido pelo GDPR, especialmente nos artigos 5º e 6º da Lei nº 13.709/2018 (Brasil, 2018). Tais dispositivos sistematizam definições essenciais relativas ao tratamento, aos agentes envolvidos e aos princípios orientadores da proteção de dados no Brasil.

Nos termos do artigo 5º da LGPD, considera-se dado pessoal toda informação relacionada a pessoa natural identificada ou identificável (inciso I). Os dados sensíveis, por sua vez, abrangem informações sobre origem racial ou étnica, convicção religiosa, opinião política e condição de saúde, entre outras categorias que demandam proteção reforçada (inciso II).

Quanto aos agentes, o controlador é definido como o responsável pelas decisões relativas às finalidades e aos meios do tratamento (inciso VI). O operador é aquele que realiza o tratamento em nome do controlador, conforme instruções e vínculo contratual específico (inciso VII). Além disso, os princípios orientadores, como finalidade, adequação, necessidade, transparência, segurança e responsabilização, estão previstos no artigo 6º. Já os direitos assegurados ao titular, que incluem acesso, correção, anonimização e eliminação de dados, encontram-se elencados no artigo 18 (Brasil, 2018).

O processo de incorporação do modelo europeu ao regime brasileiro é, por vezes, descrito criticamente pela doutrina como uma “tropicalização” do GDPR. A dinâmica evidencia o risco de transposição normativa predominantemente formal, sem adaptação adequada às limitações estruturais da Administração Pública. Entre tais restrições, destacam-se escassez orçamentária, insuficiência de pessoal especializado e dependência tecnológica em relação a operadores privados.

Diferentemente do cenário europeu, marcado por governança digital consolidada e recursos direcionados a programas de conformidade, o Brasil enfrenta profundas assimetrias institucionais (Bioni, 2020). A falta de equipes capacitadas e o subinvestimento crônico em cibersegurança forçam o Poder Público a depender de empresas terceirizadas. Como essas fornecedoras detêm um domínio tecnológico não

acompanhado por mecanismos estatais proporcionais de fiscalização, as estratégias de conformidade do setor público acabam esvaziadas (TCU, 2020; CGU, 2020).

Nesse sentido, a doutrina aponta três críticas principais a essa transposição do modelo europeu: (i) a incorporação mecânica de obrigações contratuais do GDPR para a LGPD, sem parâmetros mínimos compatíveis com a realidade administrativa nacional; (ii) a ausência de programas amplos e estruturados de capacitação voltados aos servidores públicos; e (iii) o tratamento diferenciado conferido ao Poder Público pela LGPD, que tende a enfraquecer as sanções e os incentivos à conformidade efetiva.

A primeira crítica diz respeito à importação do modelo contratual do artigo 28 do GDPR para os artigos 37 a 39 da LGPD. Enquanto a norma europeia exige que o contrato entre controlador e processador especifique detalhadamente as medidas de segurança, os procedimentos de auditoria e os protocolos de exclusão de dados, a legislação brasileira é mais genérica. O artigo 39 da LGPD limita-se a afirmar que o operador deve realizar o tratamento segundo as instruções do controlador, sem exigir formalização contratual rigorosa para esse fim (GETPRIVACY, 2025).

Essa abertura normativa, desprovida de regulamentação infralegal, repercute diretamente no Ministério da Saúde. Os contratos celebrados com as empresas responsáveis pela operação do DataSUS e da Rede Nacional de Dados em Saúde (RNDS) frequentemente carecem de cláusulas sobre gestão de incidentes, padrões de criptografia e direitos de auditoria. Consequentemente, transfere-se ao titular dos dados o ônus de uma proteção que o instrumento contratual não assegurou (Soares, 2022).

A segunda crítica refere-se às limitações estruturais da Administração Pública para implementação da LGPD. Auditoria realizada pelo Tribunal de Contas da União identificou que 76,7% das organizações públicas federais ainda se encontravam em estágio inicial ou pouco expressivo de adequação à legislação. O levantamento apontou deficiências relevantes nos indicadores de preparação institucional, contexto organizacional e capacitação, além de registrar 48 organizações que sequer haviam designado encarregado pelo tratamento de dados pessoais (TCU, 2025).

No Ministério da Saúde, os efeitos dessa fragilidade tornaram-se evidentes em episódios de exposição indevida de dados vinculados a sistemas do SUS durante a

pandemia de COVID-19. Incidentes de segurança envolvendo bases como o e-SUS Notifica e sistemas relacionados ao monitoramento da COVID-19 revelaram falhas na governança da informação e nos controles de acesso a dados sensíveis, expondo informações de milhões de brasileiros (G1, 2020).

A terceira crítica recai sobre o regime diferenciado conferido ao Poder Público pelo artigo 4º e pelo Capítulo IV da LGPD. Na prática, as exceções para atividades de segurança pública e defesa nacional, somadas ao regime sancionatório abrandado, reduzem os incentivos à adequação. As sanções pecuniárias têm aplicabilidade controvertida contra entes públicos, sendo substituídas, em regra, por advertências e medidas corretivas (Doneda et al., 2021; Mendes, 2019).

No âmbito do Ministério da Saúde, essa assimetria sancionatória fragiliza a posição dos titulares. O órgão público, como controlador, beneficia-se de um escudo institucional que limita sua exposição coercitiva. Em contrapartida, a Agência Nacional de Proteção de Dados (ANPD) encontra dificuldades para impor medidas que transformem as práticas de governança, o que inclui a fiscalização das empresas terceirizadas que atuam como operadoras (Bioni, 2020; Doneda et al., 2021).

Cabe ressaltar que, no Brasil, a Constituição Federal de 1988 já assegurava a inviolabilidade da intimidade, da vida privada, da honra e da imagem. Contudo, essa tutela permaneceu fragmentada por longo período, dispersa em diplomas como o Código de Defesa do Consumidor e o Marco Civil da Internet. A sistematização normativa ocorreu apenas com a edição da Lei Geral de Proteção de Dados Pessoais em 2018 (Brasil, 2018).

Os fundamentos expressos no artigo 2º da Lei, como o respeito à privacidade, à autodeterminação informativa e o livre desenvolvimento da personalidade, evidenciam que a LGPD não constitui corpo normativo estranho ao ordenamento jurídico brasileiro. Ao contrário, a Lei aprimora a tutela da pessoa diante das novas dinâmicas da sociedade digital, alinhando-se a parâmetros internacionais de proteção de dados, como os estabelecidos pelo Regulamento Geral de Proteção de Dados da União Europeia (Bessa, 2021).

A centralidade da transparência no regime jurídico da proteção de dados também se relaciona ao dever de informação clara nas relações informacionais contemporâneas. A doutrina do direito do consumidor aponta que, em contextos

marcados por forte assimetria informacional e pela mediação tecnológica, as informações disponibilizadas aos usuários devem ser claras, adequadas e compreensíveis, de modo a permitir o exercício efetivo de seus direitos. A qualidade da informação fornecida ao indivíduo constitui, portanto, elemento essencial para a proteção do consumidor na sociedade da informação (Khouri, 2013).

No contexto da Administração Pública, a proteção de dados pessoais também se relaciona à legitimidade democrática das instituições. A atuação estatal no tratamento de informações em larga escala somente se justifica quando acompanhada de mecanismos capazes de assegurar transparência, controle social e proteção efetiva dos direitos fundamentais. No campo da governança pública digital, destaca-se que o uso de tecnologias e dados pelo poder público deve ocorrer em consonância com formas de participação e de controle social sobre as políticas públicas (Oliveira, 2024).

Nessa perspectiva, a participação social na formulação e no acompanhamento das políticas públicas constitui elemento relevante para a legitimidade das decisões estatais relacionadas ao uso de tecnologias e ao tratamento de dados. Tal compreensão reforça que a gestão pública baseada em dados não pode prescindir de mecanismos institucionais capazes de preservar a confiança social nas instituições responsáveis pela administração dessas informações (Oliveira, 2024).

Assentadas essas bases normativas e institucionais da proteção de dados no Brasil, a análise passa a concentrar-se na governança das informações no contexto da terceirização de serviços de tecnologia da informação pela Administração Pública. Trata-se de ambiente no qual a participação de operadoras privadas, muitas vezes dotadas de maior capacidade tecnológica, amplia os riscos e as responsabilidades inerentes ao tratamento de dados pessoais.

1.2 Estrutura normativa da LGPD e governança de dados na terceirização de serviços de TI

A estrutura normativa da Lei Geral de Proteção de Dados Pessoais (LGPD) revela um modelo de tutela que ultrapassa a mera proclamação de direitos. A legislação exige a construção de mecanismos institucionais capazes de assegurar governança, rastreabilidade e responsabilização no tratamento de informações.

No âmbito da Administração Pública federal, essa exigência assume particular relevância. O Estado atua simultaneamente como garantidor de direitos fundamentais e como agente que realiza tratamentos massivos de dados. Essa operação ocorre, muitas vezes, por meio de operadores privados contratados, conforme a distinção estabelecida nos incisos VI e VII do artigo 5º da LGPD.

Diante disso, os dispositivos legais aplicáveis não devem ser compreendidos apenas como comandos formais, eles constituem parâmetros concretos para a organização contratual e administrativa dos serviços terceirizados de tecnologia da informação (TI). O referido conjunto normativo abrange os princípios orientadores do tratamento (art. 6º), as bases legais (artigos 7º e 11), os direitos dos titulares (art. 18) e as regras específicas para o Poder Público (artigos 37 a 39).

No aspecto conceitual, a lei define dado pessoal como qualquer informação relacionada a pessoa natural identificada ou identificável (art. 5º, I). Os dados sensíveis, por sua vez, recebem proteção reforçada e abrangem informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, genética, biometria, saúde ou vida sexual (art. 5º, II). O tratamento dessas informações é admitido apenas nas hipóteses restritas do artigo 11, o que inclui consentimento específico, cumprimento de obrigação legal, proteção da vida, tutela da saúde, proteção ao crédito ou execução de políticas públicas (Brasil,, 2018).

Outro pilar fundamental corresponde aos princípios do tratamento, previstos no artigo 6º. Vetores como finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização orientam toda a aplicação da LGPD. Eles permitem avaliar se as práticas adotadas por controladores e operadores estão em conformidade com os objetivos protetivos da legislação (ANPD, 2021).

Em relação às bases legais que legitimam o tratamento, a LGPD estabelece regras próprias para a Administração Pública. O artigo 7º, inciso III, autoriza o uso de dados pessoais quando necessário ao cumprimento de obrigação legal ou regulatória, bem como à execução de políticas públicas.

A legislação também assegura ao titular um amplo conjunto de direitos. Destacam-se o acesso, a correção, a exclusão, a portabilidade e o direito à informação sobre as operações realizadas. A observância dessas garantias é fiscalizada pela Agência Nacional de Proteção de Dados (ANPD), conforme os artigos 17 a 22 e 55-J da LGPD.

Adicionalmente, a lei estabelece diretrizes específicas para o setor público. O destaque recai sobre a obrigatoriedade de adotar estruturas de governança em privacidade, de manter registros das operações e, quando cabível, de elaborar relatórios de impacto à proteção de dados (artigos 37 e 38 da LGPD).

Nesse contexto, o artigo 37 desponta como o pilar central da integridade. O dispositivo impõe a adoção de estruturas de governança tanto pelos agentes públicos quanto pelos operadores a eles vinculados, a exemplo das empresas terceirizadas de TI (Maldonado; Blum; Borelli, 2020).

A imposição normativa exige que controlador e operador documentem todo o ciclo de vida dos dados pessoais. Devem ser detalhados a natureza do tratamento, a finalidade perseguida, o período de retenção das informações e as medidas de segurança adotadas, especialmente nas hipóteses que envolvem tratamento de alto risco.

A documentação sistemática torna-se particularmente relevante nas terceirizações do serviço público. O registro das operações permite rastrear os fluxos informacionais e identificar, com maior celeridade, eventuais falhas na cadeia de tratamento de dados.

A ausência de mecanismos adequados de rastreabilidade pode gerar consequências relevantes na gestão de dados públicos. Episódios ocorridos durante a pandemia de Covid-19, envolvendo sistemas do Ministério da Saúde e empresas terceirizadas responsáveis pelo desenvolvimento de aplicações digitais, evidenciaram fragilidades na governança de dados e na gestão de contratos de tecnologia da informação.

O caso relacionado à empresa Zello Tecnologia ilustra de forma concreta os riscos decorrentes da falta de controles técnicos e de registros estruturados das operações de tratamento. A análise detalhada do episódio será desenvolvida adiante, quando se examinarão as implicações práticas da terceirização de serviços de TI no tratamento de dados sensíveis de saúde.

Os registros de tratamento devem documentar etapas como coleta, armazenamento e compartilhamento de dados pessoais. Funcionam como instrumento de comprovação de conformidade perante a Agência Nacional de Proteção de Dados e o Tribunal de Contas da União (Brasil, 2018; Tribunal de Contas da União, 2022). Quando o tratamento é realizado por terceirizadas, a obrigação assume contornos contratuais. Na prática, materializa-se em cláusulas que imponham

à prestadora o fornecimento de trilhas de auditoria e a documentação das decisões arquiteturais do sistema.

O episódio envolvendo a empresa Zello ilustra as consequências da ausência desses registros. A vulnerabilidade permaneceu ativa por período indeterminado e acabou descoberta por agente externo. A divergência pública sobre a autoria da decisão técnica evidenciou a inexistência de documentação capaz de esclarecer responsabilidades (EM, 2020). A obrigação de registrar as operações promove a prevenção e alinha-se ao princípio da responsabilização, previsto no artigo 6º, inciso X, da LGPD.

De forma complementar, o artigo 38 da lei permite que a ANPD exija o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) em hipóteses de tratamento de alto risco. O documento descreve os processos envolvidos, os riscos identificados e as salvaguardas adotadas. Nas terceirizações de TI, o RIPD constitui instrumento relevante para identificar vulnerabilidades ainda na fase pré-contratual. A exigência fortalece a diligência prévia (*due diligence*[2]) do órgão contratante e contribui para a proteção preventiva dos titulares (Vainzof, 2021).

O cumprimento de tais deveres demonstra que a conformidade com a LGPD ultrapassa a observância meramente formal da lei. A efetividade da proteção depende da incorporação das diretrizes legais em práticas administrativas e instrumentos contratuais adequados.

As práticas de governança devem ser proativas e mensuráveis. Fundamentam-se na designação de encarregado pelo tratamento de dados, na realização de treinamentos contínuos e em auditorias periódicas junto às terceirizadas. O monitoramento constante é essencial para prevenir incidentes e assegurar alinhamento com os princípios da LGPD.

Ademais, os instrumentos contratuais precisam estabelecer responsabilidades claras para a operadora. Isso inclui a obrigatoriedade de elaborar o RIPD, a manutenção de registros compartilhados e a previsão de penalidades objetivas para casos de vazamento. Dessa forma, assegura-se ao Poder Público o pleno direito de fiscalização sobre a atuação da empresa contratada.

---

[2] *Due diligence* (diligência prévia, em português): procedimento investigativo realizado previamente à celebração de um contrato com terceiro, com o objetivo de verificar, avaliar e analisar riscos nas dimensões financeira, jurídica, tecnológica e de conformidade regulatória. No contexto da LGPD, consiste na avaliação prévia da maturidade do fornecedor em proteção de dados e segurança da informação, subsidiando a tomada de decisão quanto à contratação e à definição de cláusulas de responsabilização.

A efetividade dessas medidas de governança e das cláusulas contratuais depende da correta definição dos papéis desempenhados pelos agentes envolvidos no tratamento de dados pessoais.

No contexto da Administração Pública federal, essa distinção assume especial relevância, uma vez que a atuação conjunta entre órgãos públicos e empresas terceirizadas de tecnologia da informação exige delimitação precisa de competências, responsabilidades e deveres de conformidade. Torna-se, portanto, necessário examinar as categorias jurídicas de controlador e operador previstas na Lei Geral de Proteção de Dados, bem como os desafios práticos relacionados à aplicação desses conceitos no âmbito da gestão pública e das contratações administrativas.

1.3 Controlador e Operador no Âmbito da Administração Pública federal: conceitos, responsabilidades e desafios de conformidade

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece uma divisão funcional clara entre os agentes de tratamento. O controlador decide sobre as finalidades e os meios do tratamento dos dados, enquanto o operador realiza essas atividades em nome do controlador e de acordo com suas instruções, conforme dispõe o artigo 5º, incisos VI e VII.

No contexto da Administração Pública federal, o papel de controlador é exercido, em regra, pelo órgão ou pela entidade responsável pela política pública que demanda a utilização dos dados. O operador, por sua vez, costuma ser a empresa privada contratada para prestar serviços técnicos, como desenvolvimento, manutenção e hospedagem de sistemas de tecnologia da informação (TI).

Essa divisão de papéis, embora conceitualmente definida, apresenta desafios práticos relevantes. O primeiro deles diz respeito à necessidade de clareza contratual. A ausência de uma definição precisa das obrigações de cada parte pode gerar conflitos sobre a responsabilização em casos de incidentes de segurança, vazamentos de dados ou violações de direitos dos titulares.

Na prática, a clareza na definição de responsabilidades é alcançada por meio da inclusão de cláusulas específicas nos instrumentos contratuais. As disposições contratuais devem delimitar expressamente as atividades autorizadas ao operador, os dados aos quais terá acesso, os protocolos de resposta a incidentes sob seu encargo e as penalidades aplicáveis em caso de descumprimento. A formalização das

obrigações confere maior segurança jurídica às partes envolvidas (SERPRO, 2020).

O segundo desafio decorre da assimetria de informação e de capacidade técnica entre o ente público e o parceiro privado. Empresas de tecnologia frequentemente possuem maior domínio sobre riscos, padrões de segurança e soluções operacionais. Tal desnível pode resultar em contratos que não asseguram ao Estado mecanismos suficientes de controle e fiscalização.

Para mitigar essa assimetria, destacam-se instrumentos preventivos e de monitoramento. Entre eles, figuram a exigência de certificações de segurança da informação como condição de habilitação nos editais e a previsão de auditorias periódicas, a serem realizadas pelo órgão contratante ou por entidade independente.

Acrescenta-se, ainda, a garantia de acesso irrestrito aos registros de operação do sistema (*logs*) e a obrigatoriedade de notificação imediata ao controlador em caso de incidentes de segurança. Tal medida é essencial para viabilizar o cumprimento do prazo, estabelecido pela Resolução CD/ANPD nº 15/2024, para comunicação de incidentes de segurança à Agência Nacional de Proteção de Dados (ANPD, 2024).

O terceiro desafio relaciona-se à cooperação contínua exigida pela LGPD. Essa atuação conjunta é fundamental na prevenção e na resposta a incidentes, na realização de auditorias e na interlocução institucional.

Conforme a referida Resolução CD/ANPD nº 15/2024, o controlador tem três dias úteis para comunicar à ANPD e aos titulares qualquer incidente de segurança que possa acarretar risco ou dano relevante. A norma permite a complementação das informações em até vinte dias úteis subsequentes (ANPD, 2024).

Quando essas obrigações não são detalhadas desde a fase de contratação, a relação entre o controlador e o operador tende a se tornar conflituosa e ineficiente. Exemplo disso foi o caso Zello, citado anteriormente, em que a falta de registros adequados impediu ambas as partes de demonstrarem documentalmente a origem da falha sistêmica e o cumprimento de seus respectivos deveres legais.

Dessa forma, a delimitação inadequada de papéis nos contratos de terceirização de TI cria zonas de incerteza que fragilizam a proteção de dados pessoais. A lacuna normativa resultante expõe os titulares a acessos indevidos e sujeita a Administração Pública a graves consequências jurídicas e institucionais, com impactos ainda maiores em setores sensíveis como o da saúde.

Verifica-se, portanto, que a conformidade com a LGPD no setor público não se esgota na proclamação abstrata de direitos. Ela demanda a implementação de

mecanismos efetivos de governança em privacidade e o detalhamento das responsabilidades contratuais dos agentes de tratamento. A partir dessa constatação, o capítulo subsequente examina os instrumentos normativos e contratuais aplicáveis à terceirização de TI, com o objetivo de identificar deveres específicos capazes de mitigar riscos nessas parcerias.

2. Marcos normativos e conceituais da proteção de dados na terceirização de serviços de TI

A prestação de serviços de tecnologia da informação (TI) pode ser compreendida como o conjunto de atividades voltadas ao desenvolvimento, à manutenção e ao suporte de sistemas. Engloba também a gestão de infraestrutura, de redes e de bases de dados, bem como a computação em nuvem e a segurança da informação. Tais atividades são consideradas essenciais ao funcionamento das organizações públicas e privadas (Fernandes; Abreu, 2014).

Quando essas operações são executadas por uma empresa contratada, configura-se a terceirização (*outsourcing*[3]) de serviços de TI. Nessa modalidade, o ente público transfere a execução de determinadas funções a uma pessoa jurídica especializada, mas permanece responsável pela definição das políticas, das diretrizes e dos objetivos a serem alcançados (Fortini; Vieira, 2021).

No âmbito da Administração Pública federal, esse modelo encontra fundamento no Decreto-Lei nº 200/1967. A norma prevê a possibilidade de o Estado desobrigar-se da realização material de atividades executivas, recorrendo à execução indireta mediante contrato precedido de licitação (Brasil, 1967). Embora a terceirização seja adotada para suprir déficits técnicos internos, a prática implica riscos de assimetria informacional e de controle caso não seja acompanhada de mecanismos contratuais adequados de governança e fiscalização (Fortini; Vieira, 2021; TCU, 2017).

Diante do exposto, a proteção dos dados pessoais tratados por terceirizadas na Administração Pública federal é estruturada por um conjunto de marcos normativos complementares.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabelece os princípios, os direitos dos titulares e os deveres de controladores e operadores. A norma define as bases legais, os requisitos de segurança e os mecanismos de

[3] *Outsourcing* (terceirização, em português): processo de gestão por meio do qual uma organização transfere a terceiros a execução de atividades que originalmente seriam realizadas internamente, buscando eficiência operacional, redução de custos e acesso a conhecimento técnico especializado. No âmbito da Administração Pública, o instituto encontra fundamento no Decreto-Lei nº 200/1967, que prevê a possibilidade de o Estado desobrigar-se da realização material de atividades executivas, recorrendo à execução indireta mediante contrato precedido de licitação pública. No contexto de TI, o *outsourcing* é adotado para suprir déficits técnicos internos, mas implica riscos de assimetria informacional e de controle quando não acompanhado de mecanismos contratuais adequados de governança e fiscalização.

responsabilização aplicáveis a toda a cadeia de tratamento, inclusive nos contratos de terceirização de TI (Brasil, 2018).

O Marco Civil da Internet (Lei nº 12.965/2014), por sua vez, fixa princípios e garantias relacionados ao uso da rede no Brasil. O destaque recai sobre a proteção da privacidade, a inviolabilidade das comunicações e a guarda adequada de registros de acesso e de aplicações. As exigências descritas incidem diretamente sobre os provedores de infraestrutura e as empresas de TI que operam sistemas públicos conectados em rede (Brasil, 2014).

Somam-se a esses diplomas outras normativas relevantes para o setor público. A Lei de Acesso à Informação (Lei nº 12.527/2011) disciplina a transparência ativa e passiva, impondo limites ao acesso a informações de caráter pessoal (Brasil, 2011). Adicionalmente, a legislação de contratações públicas exige a previsão de cláusulas contratuais aptas a assegurar a adequada execução do objeto e a responsabilidade das partes, nos termos da Lei nº 14.133/2021, sendo comum a inclusão de disposições relativas à segurança da informação e à proteção de dados pessoais em conformidade com a Lei nº 13.709/2018 (LGPD).

A articulação desses marcos normativos é fundamental para reduzir a assimetria entre o órgão controlador e a empresa operadora. A integração entre os instrumentos jurídicos exige que os contratos de terceirização incorporem obrigações específicas em matéria de segurança, governança em privacidade e responsabilização. O objetivo consiste em efetivar a tutela dos titulares de dados pessoais em um ambiente tecnicamente complexo e fortemente dependente de prestadores externos (Bioni, 2020).

2.1 A Lei Geral de Proteção de Dados e as Obrigações do Controlador e do Operador

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece uma divisão funcional clara entre os agentes de tratamento. O controlador decide sobre as finalidades e os meios do tratamento, enquanto o operador executa a atividade em nome e segundo as orientações daquele, conforme o artigo 5º, incisos VI e VII.

Cabe ao controlador, portanto, determinar a base legal aplicável, verificar a compatibilidade da operação com os direitos fundamentais do titular e definir o escopo do tratamento. O operador, por sua vez, responde pela execução técnica e deve atuar

em estrita conformidade com as instruções documentadas do controlador. Apesar das funções distintas, ambos respondem juridicamente pela coleta, pelo tratamento e pelo armazenamento dos dados. Logo, a posição de operador não se confunde com a de um mero executor neutro.

A divisão funcional não isenta o contratado de responsabilidades. O artigo 42 da LGPD prevê que ambos os agentes podem ser responsabilizados por danos decorrentes de tratamento ilícito ou irregular, admitindo-se a responsabilidade solidária em determinadas hipóteses. A previsão legal afasta a premissa de que o operador atue como simples prestador técnico e impõe o dever de adotar condutas diligentes para garantir a qualidade e a segurança das operações sob sua guarda.

Embora a legislação não apresente um rol exaustivo de deveres específicos do operador, a interpretação sistemática revela obrigações inerentes a essa função. Os artigos 5º, inciso VII, 39 e 46 a 49, combinados com os princípios do artigo 6º, permitem delinear um conjunto mínimo de exigências jurídicas.

Em primeiro lugar, infere-se o dever de atuar exclusivamente conforme as instruções do controlador, com a abstenção de uso dos dados para finalidades próprias ou não autorizadas (artigos 5º, inciso VII, e 39). Na prática, essa premissa exige que o contrato administrativo delimite expressamente o escopo do tratamento. O instrumento deve especificar quais informações podem ser acessadas, por quais colaboradores, em que circunstâncias e para quais objetivos.

A ausência de delimitações contratuais permite que o operador acesse ou utilize dados além do estritamente necessário, sem que o ente público disponha de mecanismos para coibir eventuais desvios. Caso o contratado descumpra as diretrizes lícitas do controlador ou atue com negligência, a legislação prevê sua equiparação ao ente público. A circunstância atrai responsabilidade solidária pelos danos causados aos titulares, nos termos do artigo 42, § 1º, inciso I da LGPD (Brasil, 2018).

Em segundo lugar, impõe-se a obrigação de adotar medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração ou difusão. Trata-se do dever de segurança, fundamentado nos artigos 46 a 49 (Brasil, 2018).

As medidas técnicas compreendem a criptografia de dados em trânsito e em repouso, o controle de acesso com autenticação multifator e a segregação de funções.

Incluem também o uso de *firewalls*[4], sistemas de detecção de intrusão, anonimização ou pseudonimização de dados sensíveis e a manutenção de trilhas de auditoria (*logs*). Tais práticas estão em conformidade com os controles de segurança previstos no Anexo A da norma ABNT NBR ISO/IEC 27001:2022, padrão internacional voltado à gestão da segurança da informação (ABNT, 2022).

Já as medidas administrativas abrangem a elaboração de políticas internas de privacidade e de segurança da informação. Envolvem o treinamento periódico dos colaboradores, a condução de auditorias regulares e a gestão documentada de riscos, com o devido registro das decisões e das ações corretivas (ANPD, 2021).

Nas terceirizações de tecnologia da informação no serviço público, a exigência contratual dessas medidas é indispensável para viabilizar a fiscalização e a eventual responsabilização da operadora. Por essa razão, o edital de licitação já deve especificar os padrões mínimos de segurança exigidos da futura contratada.

Por fim, emerge o dever de cooperação institucional. O operador deve atuar em conjunto com o controlador na prevenção e na mitigação de incidentes, bem como na viabilização do exercício dos direitos dos titulares. A atuação conjunta alinha-se aos princípios da prevenção, da responsabilização e da prestação de contas previstos no artigo 6º da LGPD (Brasil, 2018).

O dever de ambos agentes de tratamento se concretiza em obrigações operacionais objetivas. O operador deve comunicar imediatamente qualquer incidente de segurança ocorrido em seus sistemas, permitindo que o controlador notifique a Agência Nacional de Proteção de Dados (ANPD) e os titulares no prazo legal de três dias úteis (Resolução CD/ANPD nº 15/2024). Ademais, cabe à contratada fornecer os dados necessários para o atendimento de solicitações de acesso, correção, portabilidade ou exclusão, além de disponibilizar registros e *logs* para auditorias (ANPD, 2021).

A ausência de cooperação institucional estruturada tornou-se evidente no episódio envolvendo a empresa Zello, no âmbito do Ministério da Saúde. A disputa pública sobre a origem da falha sistêmica revelou a inexistência de fluxos de comunicação previamente definidos para situações de crise. O cenário retardou a

[4] *Firewall*: mecanismo de segurança que monitora e controla o tráfego de dados entre redes ou sistemas, permitindo ou bloqueando comunicações de acordo com regras previamente definidas, com o objetivo de proteger sistemas contra acessos não autorizados.

resposta ao incidente e comprometeu a prestação de informações adequadas aos titulares afetados (EM, 2020).

As obrigações operacionais, contudo, não são detalhadas de forma minuciosa na LGPD. A disciplina brasileira adota abordagem mais principiológica, deixando maior espaço para definição contratual das responsabilidades do operador. O modelo diverge do Regulamento Geral de Proteção de Dados da União Europeia (RGPD), que estabelece comandos contratuais expressos dirigidos ao operador.

O artigo 28 do regulamento europeu determina que o contrato deve especificar o objeto, a duração e a finalidade do tratamento, o tipo de dados pessoais envolvidos e as categorias de titulares. O dispositivo prevê ainda deveres específicos relativos à confidencialidade, à segurança da informação, à subcontratação e à eliminação ou devolução dos dados ao término do serviço (União Europeia, 2016; Mendes, 2019; Bioni, 2019).

A densidade normativa europeia contrasta com a disciplina brasileira, que carece de um rol equivalente de requisitos contratuais obrigatórios. Essa lacuna reforça a necessidade de concretizar tais deveres por meio de cláusulas específicas, especialmente nos contratos de terceirização celebrados pela Administração Pública federal.

Para materializar essas obrigações, o contrato administrativo deve descrever o alcance das responsabilidades do operador de maneira precisa. Ao contratar uma empresa de TI, o Poder Público precisa estabelecer padrões mínimos de segurança, procedimentos de resposta a incidentes e mecanismos de cooperação em fiscalizações. Deve prever também as consequências jurídicas aplicáveis em caso de descumprimento (ANPD, 2022). Tais disposições funcionam como instrumento de internalização da LGPD na relação contratual, reduzindo a assimetria técnica e informacional entre as partes.

Nesse contexto, as cláusulas relativas à comunicação de incidentes assumem especial relevância. Um incidente é compreendido como qualquer evento adverso, confirmado ou sob suspeita fundada, que resulte em acesso não autorizado, destruição, perda, alteração, divulgação ou tratamento incompatível com as normas de proteção de dados (ANPD, 2021).

Embora a LGPD atribua ao controlador o dever de comunicar incidentes que possam acarretar risco ou dano relevante (art. 48), é imprescindível que o operador

seja contratualmente obrigado a reportar qualquer evento de segurança em sua infraestrutura de forma tempestiva e detalhada.

A comunicação tempestiva é aquela realizada em tempo hábil para que o controlador cumpra o limite de três dias úteis, contados do conhecimento do fato, conforme estabelecido no artigo 6º da Resolução CD/ANPD nº 15/2024. Já a notificação detalhada deve conter a descrição da natureza e da categoria dos dados afetados, bem como o número de titulares impactados. Precisa apontar as medidas técnicas adotadas antes e após o evento, a causa principal identificável e o operador responsável (ANPD, 2024).

O fluxo de informação é essencial para que o controlador cumpra seus deveres de avaliação de risco, de registro interno e de notificação institucional. Na ausência de cláusula clara sobre o dever de reporte, a operadora pode postergar a comunicação de falhas por receio de sanções contratuais, desgastes reputacionais ou custos de remediação. O desalinhamento de incentivos aumenta a probabilidade de que vulnerabilidades permaneçam ativas, o que amplia a superfície de dano aos titulares e agrava a responsabilidade do controlador público (Brasil, 2018; ANPD, 2021).

Torna-se, portanto, indispensável adotar critérios rigorosos para a escolha do operador, fundados não apenas no menor preço, mas sobretudo na melhor técnica. A maturidade em segurança da informação e a capacidade comprovada de conformidade com a LGPD configuram requisitos essenciais para a contratação de prestadores responsáveis pelo tratamento de dados pessoais.

A constatação evidencia que a proteção efetiva dos titulares depende também da forma como o Poder Público estrutura e conduz suas contratações de tecnologia da informação. Nesse sentido, impõe-se analisar o regime jurídico das contratações públicas de TI e os instrumentos disponíveis para mitigação de riscos relacionados ao tratamento de dados pessoais.

2.2 O regime das contratações de TI e os desafios da proteção de dados pessoais

A contratação pública no Brasil submete-se a um regime jurídico próprio, estruturado em âmbito federal pela Lei nº 14.133/2021, a Nova Lei de Licitações e Contratos Administrativos. O diploma unificou e modernizou regras que estavam dispersas em diferentes normativas e tornou-se de observância obrigatória a partir de

1º de abril de 2023, consolidando a revogação da Lei nº 8.666/1993 no final daquele mesmo ano (Brasil, 2021).

A nova lei disciplina de forma integrada a contratação de obras, serviços, compras e alienações. No âmbito dos serviços, engloba expressamente aqueles voltados à tecnologia da informação (TI). O processo orienta-se por princípios delineados no artigo 5º, entre os quais legalidade, impessoalidade, moralidade, publicidade, eficiência, desenvolvimento nacional sustentável e segregação de funções. O intuito é assegurar a seleção da proposta mais vantajosa para a Administração Pública (Brasil, 2021; Di Pietro, 2023).

No rito licitatório, cada princípio desempenha função específica. A legalidade exige o cumprimento estrito dos procedimentos e das cláusulas previstas em lei e no edital. A impessoalidade assegura o tratamento isonômico entre os licitantes. A moralidade pauta a atuação administrativa pela boa-fé e pela probidade, enquanto a publicidade confere transparência aos atos. A eficiência, por sua vez, determina que a escolha do contratado produza o melhor resultado possível para o interesse público, distanciando-se do critério exclusivo de menor preço formal (Di Pietro, 2023).

Historicamente, a legislação enfatizou a seleção da proposta mais vantajosa sob a ótica econômico-financeira, como estratégia para reduzir custos e prevenir o favorecimento e a corrupção. A Lei nº 8.666/1993 consolidou esse modelo a partir da centralidade do critério de menor preço. Contudo, apesar de eficaz na contenção de gastos, a sistemática mostrou-se insuficiente para garantir a qualidade técnica das contratações, especialmente em setores de alta complexidade como o de TI (Di Pietro, 2023; TCU, 2020).

A proteção de dados pessoais como direito fundamental (Emenda Constitucional nº 115/2022) e a vigência da Lei Geral de Proteção de Dados (LGPD) adicionaram uma nova dimensão a essa análise. Não basta contratar a solução mais barata. Exige-se do prestador a comprovação de capacidade técnica, organizacional e de governança para proteger as informações sob sua guarda.

A obrigação de demonstrar conformidade assume relevância especial nos contratos de TI que envolvem o Sistema Único de Saúde (SUS) e as plataformas de saúde digital. As bases cadastrais desses sistemas concentram dados sensíveis. Em ambientes dessa natureza, falhas de segurança podem expor milhões de pessoas a riscos de discriminação, estigmatização, fraudes e danos correlatos (SERPRO, 2020; Brasil, 2018).

Para compatibilizar tais exigências, a Lei nº 14.133/2021 oferece instrumentos técnicos. O artigo 33, incisos III e IV, da Lei nº 14.133/2021 autoriza a utilização dos critérios de julgamento “melhor técnica” ou “técnica e preço”, especialmente em contratações de bens e serviços especiais de tecnologia da informação e comunicação (Brasil, 2021).

Dessa forma, os editais podem prever a exigência de experiência prévia em segurança da informação e a adoção de medidas organizacionais compatíveis com os artigos 46 a 51 da LGPD. Além disso, torna-se possível estipular cláusulas contratuais rigorosas de proteção de dados, acompanhadas de sanções proporcionais em caso de descumprimento (Vale; Oliveira, 2025). Tais requisitos operam como filtro essencial para selecionar empresas aptas a implementar as salvaguardas exigidas pela legislação.

Apesar dos avanços, muitos órgãos ainda encontram obstáculos para incorporar essas diretrizes em seus instrumentos convocatórios. Limitações orçamentárias e carência de equipes especializadas em segurança da informação dificultam a formulação de editais precisos. Adiciona-se a isso o desconhecimento das melhores práticas contratuais sobre governança e proteção de dados por parte dos gestores públicos (SERPRO, 2020).

Na prática, grande parte dos contratos de terceirização de TI permanece estruturada com foco no preço e nos prazos de entrega. Cláusulas essenciais sobre governança em privacidade, comunicação de incidentes, padrões de segurança e deveres do operador são deixadas em segundo plano. O cenário ora apresentado eleva o risco de seleção de empresas com baixa maturidade em proteção de dados, que vencem certames apenas por ofertarem os valores mais baixos, mas sem garantir mecanismos robustos de prevenção e resposta a falhas.

Nos contratos que processam dados sensíveis de saúde, como os geridos pelo Ministério da Saúde, a omissão de critérios técnicos e de cláusulas densas sobre a LGPD enfraquece a posição do ente público. A fragilidade institucional resultante amplia as chances de vazamentos em larga escala, além de tornar mais complexa a apuração de responsabilidades e a reparação de danos aos titulares.

Nesse sentido, surge a necessidade de identificar os deveres contratuais específicos que devem ser exigidos das terceirizadas de TI. Apenas com a inclusão de parâmetros objetivos a proteção de dados deixará de constituir previsão abstrata e passará a assumir contornos concretos nos instrumentos de contratação. A

abordagem fundamenta a análise desenvolvida no subitem a seguir (Moura; Oliveira, 2023).

2.3 Deveres contratuais de proteção de dados nas terceirizações de serviços de TI

Diante do quadro normativo traçado pela Lei Geral de Proteção de Dados Pessoais (LGPD) e pelo regime de contratações públicas, a proteção de informações na terceirização de tecnologia da informação (TI) depende de como as obrigações legais são convertidas em cláusulas contratuais concretas (Moura; Oliveira, 2023). A efetividade da tutela conferida aos titulares, em especial quanto a dados sensíveis de saúde, relaciona-se diretamente à precisão com que o contrato administrativo disciplina o tratamento realizado pelo operador privado, sob a coordenação do controlador público (Brasil, 2018).

Conceitualmente, identificam-se quatro grupos centrais de deveres inerentes à proteção de dados em terceirizações de TI. São eles: cláusulas de descrição do tratamento; cláusulas de segurança da informação e governança em privacidade; cláusulas de cooperação e apoio ao controlador; e cláusulas de responsabilidade, sanções e mitigação de riscos (Moura; Oliveira, 2023; Soares, 2022).

O primeiro grupo compreende a descrição detalhada das operações. O instrumento deve delimitar expressamente as categorias de dados abrangidas, identificando aquelas de natureza sensível, bem como as finalidades e as bases legais aplicáveis. No setor de saúde, os objetivos mais comuns envolvem a gestão de prontuários eletrônicos, o agendamento de procedimentos clínicos e o monitoramento da saúde pública.

As bases legais frequentemente invocadas são o cumprimento de obrigação legal ou regulatória (artigos 7º, inciso II, e 11, inciso II, alínea "a", da LGPD) e a execução de políticas públicas (artigos 7º, inciso III, e 11, inciso II, alínea "b"). Nos casos de prestação direta de serviços, aplica-se também a tutela da saúde por autoridade sanitária (artigo 11, inciso II, alínea "f") (Brasil, 2018).

Quanto à duração do tratamento, a LGPD não fixa um prazo uniforme. A lei estabelece apenas que as informações devem ser eliminadas após o término da atividade, ressalvadas as hipóteses de conservação previstas no artigo 16 (Brasil, 2018).

Sendo assim, é prática recomendável vincular a vigência do tratamento ao prazo do contrato, acrescido do período de retenção legalmente exigível para cada categoria de dado, admitida a prorrogação contratual nos termos do art. 107 da Lei nº 14.133/2021 (ANPD, 2024).

O contrato também deve especificar os sistemas, os ambientes e os módulos tecnológicos utilizados no tratamento. Exemplos dessa infraestrutura no âmbito federal incluem o Prontuário Eletrônico do Cidadão (e-SUS PEC), o Sistema Nacional de Regulação (SISREG) e a Rede Nacional de Dados em Saúde (RNDS). Torna-se necessário detalhar os módulos aos quais o operador terá acesso, como a gestão de leitos, o agendamento eletrônico e os instrumentos de faturamento ambulatorial, que integram a infraestrutura digital do Sistema Único de Saúde (Brasil, 2023).

A minúcia na definição contratual delimita com precisão o escopo de atuação do parceiro privado e o vincula juridicamente às finalidades definidas pelo controlador, o que coíbe o uso indevido das informações. Ademais, fornece parâmetros objetivos para auditorias, relatórios de impacto e avaliações de conformidade em bases cadastrais extensas (Moura; Oliveira, 2023).

O segundo grupo abrange as cláusulas de segurança da informação e de governança. A LGPD impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados, destruição, perda, alteração ou tratamento ilícito (artigos 46 a 49).

No contexto contratual, isso se traduz na obrigação de o operador implementar controles de acesso, trilhas de auditoria, criptografia e segmentação de ambientes. Exigem-se também testes periódicos de vulnerabilidade, planos de continuidade e rotinas de cópias de segurança (*backup*[5]) destinadas à restauração das informações em caso de incidentes (ANPD, 2025).

De forma complementar, os instrumentos de governança sugerem que o contrato incorpore a privacidade em todo o ciclo de vida das soluções tecnológicas. Isso ocorre por meio de avaliações de risco em novos desenvolvimentos, em alinhamento aos princípios da privacidade desde a concepção (*privacy by design*[6]) e

[5] *Backup* compreende "a cópia das informações armazenadas nos equipamentos e servidores utilizados para prover os serviços tecnológicos", destinada à eventual restauração dos dados em caso de falha, incidente ou desastre.
[6] O *privacy by design* (privacidade desde a concepção) determina que a proteção de dados seja considerada desde o início do desenvolvimento de qualquer produto, sistema ou processo, de forma proativa e preventiva, e não como medida corretiva posterior.

da privacidade por padrão (*privacy by default*[7]), implícitos no artigo 46, § 2º, da LGPD (Brasil, 2018; ENAP, 2023).

Na prática, a privacidade desde a concepção obriga o operador a estruturar a proteção de dados nas fases de especificação e de desenvolvimento dos sistemas. Já a privacidade por padrão vincula o contratado a entregar as configurações no nível máximo de restrição, assegurando a blindagem desde o primeiro uso, sem depender de ajustes posteriores por parte da Administração Pública (ENAP, 2023; Brasil, 2023).

O terceiro eixo de cláusulas regula a cooperação e o apoio ao controlador. A LGPD determina que o operador atue de acordo com as instruções do ente público e o auxilie no cumprimento das exigências legais. A atuação conjunta inclui responder a requisições da Agência Nacional de Proteção de Dados (ANPD), colaborar na elaboração de relatórios de impacto e viabilizar o pleno exercício dos direitos dos titulares.

Nas contratações voltadas à saúde, esse dever materializa-se quando a operadora fornece mecanismos técnicos para o atendimento aos cidadãos. A contratada deve permitir que a Administração processe solicitações de acesso, correção ou eliminação de registros, confirme a existência de tratamento e informe eventuais compartilhamentos com terceiros, em observância aos artigos 18 e 19 da LGPD (Brasil, 2018; Moura; Oliveira, 2023).

A doutrina aponta que, em terceirizações de alto risco voltadas ao processamento de dados sensíveis em larga escala, a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) pode ser atribuída à própria empresa contratada. A exigência busca alinhar a especialização técnica do fornecedor às demandas de conformidade impostas ao Poder Público (Moura; Oliveira, 2023). Ao mapear fluxos informacionais, identificar vulnerabilidades e propor medidas de mitigação, o RIPD fornece o substrato necessário para que o controlador responda aos titulares com agilidade e precisão (Brasil, 2018).

Ainda no escopo da cooperação, a disciplina contratual dos incidentes de segurança assume papel essencial. Como compete ao controlador comunicar eventos que acarretem risco ou dano relevante, o contrato deve estipular prazos, canais e o

[7] O *privacy by default* (privacidade por padrão) exige que, desde o primeiro uso, o produto ou serviço já esteja configurado com o nível mais restritivo de privacidade possível, dispensando qualquer ajuste posterior pelo titular.

conteúdo mínimo da notificação que o operador enviará ao constatar violações em sua infraestrutura.

A Resolução CD/ANPD nº 15/2024 fixa em três dias úteis o prazo para que o controlador reporte o incidente à Agência e aos afetados. Consequentemente, o contrato administrativo deve estabelecer um lapso temporal ainda mais exíguo para o alerta interno por parte do operador, garantindo ao ente estatal tempo hábil para o cumprimento do dever legal (ANPD, 2024). A norma determina, no art. 6º, § 4º, o uso exclusivo de formulário eletrônico para as comunicações à ANPD, lógica que deve ser replicada no ambiente interno por meio de canais rastreáveis e documentados.

Quanto aos canais, a Resolução estabelece que a comunicação à ANPD se dê exclusivamente por formulário eletrônico disponibilizado pela Agência cabendo ao contrato replicar essa lógica internamente, com a previsão de canal formal, documentado e rastreável para a notificação do controlador pelo operador (ANPD, 2024).

Quanto ao conteúdo mínimo, o art. 6º, § 2º, da Resolução define que a comunicação contenha: a descrição da natureza e da categoria dos dados pessoais afetados; o número de titulares impactados; as medidas técnicas e de segurança adotadas antes e após o incidente; os riscos identificados e os possíveis impactos aos titulares; as medidas adotadas ou a adotar para reverter ou mitigar os efeitos; a data da ocorrência e do conhecimento do incidente; a identificação do operador; e a descrição do incidente com sua causa principal, quando identificável (ANPD, 2024).

A efetividade dessas obrigações, contudo, depende de que o contrato as reproduza de forma expressa e vinculante para o operador, sob pena de o arcabouço normativo tornar-se insuficiente para garantir a resposta tempestiva ao incidente.

O quarto grupo reúne as cláusulas de responsabilidade, sanções e mitigação de riscos. A LGPD admite a responsabilização conjunta de controlador e operador pelos danos decorrentes de tratamento ilícito ou em desacordo com a lei (art. 42, LGPD).

Nesse sentido, o contrato deve explicitar as consequências de violações em matéria de proteção de dados, como multas contratuais, obrigação de indenizar, rescisão por descumprimento grave e eventual exigência de garantias financeiras ou seguros específicos (Brasil, 2020).

Além disso, a previsão de auditorias periódicas, planos de correção e mecanismos de acompanhamento de não conformidades contribui para demonstrar,

perante a ANPD e órgãos de controle, que o controlador público adotou um programa de governança em privacidade compatível com o nível de risco da terceirização (ENAP, 2023).

Nos termos do art. 50, § 2º, I, da LGPD, esse programa deve, no mínimo: demonstrar o comprometimento do controlador com normas e boas práticas de proteção de dados; ser adaptado à escala e ao volume das operações e à sensibilidade dos dados tratados; estabelecer políticas e salvaguardas baseadas em avaliação sistemática de impactos e riscos à privacidade; contar com planos de resposta a incidentes e remediação; e ser atualizado continuamente com base em monitoramento e avaliações periódicas (Brasil, 2018).

Em cenários críticos de saúde pública, essas exigências adquirem maior rigor. O contexto impõe o emprego de técnicas de anonimização ou pseudonimização, a adoção de criptografia de alto nível e a manutenção de políticas de confidencialidade alinhadas aos padrões internacionais (Brasil, 2018; Brasil, 2024).

A inobservância dessas diretrizes no plano contratual extrapola o mero descumprimento formal da lei, pois compromete a proteção efetiva dos cidadãos e a integridade sistêmica. Na terceirização tecnológica no SUS, falhas na definição do tratamento, na segurança ou na gestão de incidentes provocam vazamentos estruturais e dificultam a responsabilização das operadoras privadas.

Nesse sentido, a análise do edital que guiou a contratação com a empresa Zello durante a pandemia de Covid-19 permite avaliar como os deveres de proteção de dados foram internalizados no instrumento pactuado. O exame de suas disposições é imprescindível para verificar a adequação dos mecanismos adotados frente aos vazamentos ocorridos.

O estudo de caso aproxima as exigências da LGPD da realidade operacional das contratações públicas de TI. Ao confrontar o texto normativo com a execução contratual, extraem-se lições relevantes sobre lacunas técnicas e sobre a eficácia da governança de dados em cenários de crise sanitária de grandes proporções.

3 Terceirização de tecnologia da informação, saúde pública e proteção de dados: a necessidade de padrões mínimos de proteção a partir da análise do edital que estruturou a contratação da empresa Zello Tecnologia da Informação Ltda.

A digitalização progressiva das políticas públicas de saúde no Brasil, especialmente no âmbito do Sistema Único de Saúde (SUS), vem ampliando, há anos, a dependência do Ministério da Saúde em relação a soluções de tecnologia da informação contratadas junto à iniciativa privada, como plataformas de saúde digital, serviços de hospedagem em nuvem e desenvolvimento de sistemas sob demanda (Brasil, 2020; Brasil, 2024).

Sistemas de prontuário eletrônico, ferramentas de vigilância epidemiológica, bases integradas de dados e painéis de monitoramento utilizam, de forma contínua, grandes volumes de dados pessoais e sensíveis de cidadãos, profissionais e gestores, de modo que a governança desse ecossistema digital se torna elemento estrutural da atuação estatal em saúde (Brasil, 2020; Haddad; Lima, 2024).

A pandemia de Covid-19 não inaugurou esse cenário, mas o tornou mais visível e crítico. A necessidade de expansão acelerada de sistemas de notificação, de emissão de certificados digitais e de monitoramento de leitos reforçou o uso de soluções de TI terceirizadas, a exemplo do e-SUS Notifica e do Conecte SUS, e evidenciou vulnerabilidades na segurança da informação, na definição de responsabilidades entre o controlador público e operadores privados e na densidade das cláusulas contratuais em matéria de proteção de dados (Brasil, 2022; Brasil, 2024).

Entre 2020 e 2021, episódios de exposição de credenciais de acesso e de bases de dados do Ministério da Saúde ilustraram como fragilidades acumuladas em arquitetura de sistemas, gestão de identidades e desenho contratual podem produzir efeitos de grande escala em contextos de alta pressão e uso intensivo.

Em novembro de 2020, o vazamento de logins e senhas de acesso a sistemas de vigilância epidemiológica expôs dados pessoais e informações de saúde de pelo menos 16 milhões de pacientes testados para Covid-19, incluindo CPF, endereço, telefone e doenças pré-existentes (G1, 2020).

Pouco depois, uma falha na configuração de aplicações do e-SUS Notifica, decorrente da inclusão de credenciais no código-fonte de um site do Ministério, deixou acessíveis dados de cerca de 243 milhões de pessoas, vivas e falecidas, com

informações identificadoras e médico-assistenciais (G1, 2020; We Live Security, 2020).

Os efeitos concretos desses incidentes ultrapassam o momento emergencial da pandemia. As bases e plataformas envolvidas continuam sendo empregadas em rotinas correntes de cuidado, gestão e monitoramento em saúde, por exemplo na consulta a históricos de atendimento via Meu SUS Digital, na consolidação de dados de vigilância em âmbito nacional e na interlocução com outros sistemas estaduais e municipais (Brasil, 2020; Brasil, 2022; Brasil, 2024).

Em um cenário em que a Lei Geral de Proteção de Dados Pessoais se encontra plenamente vigente e em processo de aplicação mais efetiva pela Agência Nacional de Proteção de Dados, a expectativa de conformidade em relação ao tratamento de dados sensíveis de saúde no SUS se eleva tanto na perspectiva regulatória quanto na percepção social (ANPD, 2021; ANPD, 2025).

Isso significa que escolhas contratuais e tecnológicas realizadas em contratos de terceirização de TI na área da saúde, inclusive aqueles celebrados antes ou durante a pandemia, seguem produzindo impactos concretos sobre a proteção de dados pessoais, tais como ampliação da superfície de exposição de informações sensíveis, dependência de controles de segurança implementados por terceiros, maior dificuldade de rastrear responsabilidades em incidentes e desafios na realização de auditorias técnicas e jurídicas sobre cadeias de subcontratação (Haddad; Lima, 2024; Brasil, 2022; Brasil, 2024).

A análise retrospectiva e prospectiva das práticas adotadas pelo Ministério da Saúde, a partir de incidentes já registrados e de contratos específicos, torna-se, assim, instrumento central para identificar padrões mínimos de proteção de dados a serem exigidos nos arranjos de terceirização.

À luz desse contexto, importa delimitar o ambiente específico da terceirização de serviços de tecnologia da informação em saúde, marcado pela combinação entre digitalização crescente, forte dependência de fornecedores privados e aplicação da LGPD como premissa da transformação digital do SUS, reconhecida pelo próprio Ministério da Saúde no âmbito do Programa SUS Digital e em atos recentes que definem o conceito de dado pessoal sensível de saúde e reforçam a centralidade da proteção de dados na agenda institucional (Brasil, 2024).

A configuração institucional produz um campo de tensão permanente entre, de um lado, a busca por eficiência administrativa, escalabilidade e inovação tecnológica

e, de outro, a necessidade de assegurar padrões adequados de segurança, governança de dados e responsabilização na relação entre o Ministério, seus operadores e eventuais suboperadores (Haddad; Lima, 2024; Peck, 2021; Brasil, 2020; Doneda et al., 2021).

À luz desse contexto, importa delimitar o ambiente da terceirização de serviços de tecnologia da informação em saúde, demonstrando como a combinação entre digitalização crescente, dependência de fornecedores privados e aplicação da LGPD, reconhecida pelo Ministério da Saúde como premissa da transformação digital do SUS (Brasil, 2024), produz um campo de tensão permanente entre eficiência administrativa e proteção de dados pessoais.

3.1 O ecossistema digital do SUS, a dependência estrutural de TI terceirizada e os riscos à proteção de dados sensíveis de saúde diante de lacunas normativas

O Departamento de Informática do SUS (DATASUS), criado em 1991, consolidou ao longo de três décadas um portfólio expressivo de sistemas de informação voltados à gestão, à vigilância epidemiológica e à regulação da atenção à saúde em todo o território nacional. O conjunto de sistemas abrange plataformas como o Sistema de Informações Hospitalares (SIH), o Sistema de Informação sobre Mortalidade (SIM), o Cadastro Nacional de Estabelecimentos de Saúde (CNES) e o e-SUS PEC (Prontuário Eletrônico do Cidadão), cujo funcionamento contínuo depende do tratamento diário de vastos volumes de dados pessoais e sensíveis de cidadãos, profissionais e gestores de saúde (DATASUS, 2019; Brasil, 2022).

A grandeza desse acervo informacional distingue o ecossistema digital do SUS de outros ambientes de terceirização de TI na Administração Pública federal. Trata-se de dados que, por sua natureza clínica e epidemiológica, são simultaneamente indispensáveis à execução de políticas públicas de saúde e extremamente vulneráveis a usos indevidos, discriminatórios ou lesivos quando acessados por agentes não autorizados (Haddad; Lima, 2024).

A centralização de informações sobre internações, óbitos, cobertura vacinal e prontuários clínicos em poucos sistemas nacionais torna qualquer falha de segurança um evento potencialmente massivo e de difícil contenção. Dada a complexidade desse portfólio, sua manutenção e desenvolvimento não são realizados exclusivamente por servidores públicos. O Plano Diretor de Tecnologia da Informação e Comunicação

(PDTIC) do DATASUS para o período 2019-2021 reconhece expressamente a insuficiência do quadro técnico próprio e a necessidade de complementação permanente por meio de contratações externas, tanto para desenvolvimento quanto para sustentação de sistemas críticos (DATASUS, 2019).

A própria estratégia de saúde digital do Ministério da Saúde parte do pressuposto de que a consecução de suas metas depende de parcerias tecnológicas com fornecedores privados em larga escala (Brasil, 2022). O modelo predominante nessas avenças é o pagamento por Unidade de Serviço Técnico (UST), mecanismo difundido pelo Tribunal de Contas da União como forma de vincular a remuneração à entrega de resultados mensuráveis em substituição à locação de mão de obra (TCU, 2017).

O regime, embora juridicamente adequado quando submetido a fiscalização efetiva, pode transferir ao fornecedor privado influência relevante sobre decisões técnicas de alto impacto, como a arquitetura dos sistemas, a gestão de credenciais de acesso e os padrões de segurança da informação adotados no desenvolvimento e na manutenção das plataformas, sobretudo quando o órgão contratante não dispõe de equipe interna capaz de auditar tais escolhas em profundidade (DATASUS, 2019; TCU, 2017).

A dependência técnica gerada por esse modelo assume natureza estrutural. Ao longo de anos de execução contratual, a empresa operadora acumula conhecimento sobre a infraestrutura, os fluxos de dados e as vulnerabilidades do sistema em nível muito superior ao que o órgão contratante consegue monitorar com a equipe interna disponível (TCU, 2017).

Na prática, isso significa que o controlador público passa a depender não apenas da prestação do serviço, mas também da capacidade da contratada de definir e implementar salvaguardas de segurança adequadas, o que fragiliza a posição do Estado para impor exigências técnicas mais rigorosas em matéria de proteção de dados e para substituir o fornecedor em caso de desempenho insatisfatório

A assimetria técnica e informacional não passou despercebida pelos órgãos de controle. Em auditoria concluída em 2017, o Tribunal de Contas da União avaliou contrato de TI do Ministério da Saúde, com valor aproximado de 60 milhões de reais anuais, e identificou irregularidades que revelam a profundidade do problema: ausência de rastreamento formal dos serviços prestados, inexistência de memória de cálculo do volume contratado e classificação unilateral das requisições de tarefas pela

própria contratada, sem mecanismos de validação independente pelo órgão contratante (TCU, 2017).

Os achados da auditoria indicam que, muito antes da emergência sanitária de 2020, a maturidade institucional do Ministério da Saúde na gestão de contratos de TI era insuficiente para a dimensão e a criticidade das plataformas envolvidas. A limitação institucional tornava improvável a definição e o monitoramento de requisitos de proteção de dados com o nível de detalhamento exigido pelo tratamento de dados sensíveis de saúde (TCU, 2017).

A combinação entre baixa maturidade institucional e elevada complexidade tecnológica acabou por produzir uma assimetria decisória nas relações contratuais.

A dependência estrutural de operadores privados, associada às fragilidades da governança contratual, criou um ambiente em que decisões técnicas de grande impacto sobre a proteção de dados eram, em larga medida, tomadas pelas contratadas sem supervisão efetiva pelo controlador público (TCU, 2017; BRASIL, 2020).

Nessas condições, a responsabilidade formal atribuída ao Ministério da Saúde pela LGPD convive com uma distribuição fática de poder decisório que favorece o fornecedor privado, ampliando o risco de que padrões de segurança, práticas de desenvolvimento e rotinas de gestão de credenciais sejam definidos prioritariamente por critérios de custo e conveniência operacional, e não por critérios de proteção de dados pessoais.

A gravidade do problema torna-se ainda mais evidente quando se considera a natureza das informações envolvidas. A qualificação jurídica dos dados de saúde como dados pessoais sensíveis, nos termos do artigo 5º, inciso II, da LGPD, reflete o reconhecimento de que informações sobre condições clínicas, diagnósticos, tratamentos, histórico de vacinação e doenças preexistentes possuem potencial de gerar danos específicos e de difícil reversão quando acessadas ou divulgadas sem autorização (Brasil, 2018).

Tais danos extrapolam a dimensão patrimonial e abrangem discriminação em processos seletivos de emprego, restrições no acesso à saúde suplementar, estigmatização social de pessoas com determinadas condições médicas e, em situações extremas, a utilização dessas informações para chantagem ou fraude (ANPD, 2022; Peck, 2021; Brasil, 2020; Doneda et al., 2021).

No âmbito do SUS, os riscos são amplificados pela escala dos sistemas envolvidos. Plataformas como o e-SUS Notifica, o Sistema de Informações do Programa Nacional de Imunizações e o Conecte SUS concentram dados clínicos de dezenas de milhões de titulares, de modo que uma única vulnerabilidade pode produzir impactos simultâneos sobre parcela expressiva da população brasileira, considerando que aproximadamente 76% dos brasileiros dependem diretamente do Sistema Único de Saúde (Brasil, 2022; Haddad; Lima, 2024; Brasil, 2025).

A conjugação entre grande escala, elevada sensibilidade das informações e dependência de infraestrutura terceirizada transforma o ecossistema digital do SUS em ambiente de risco acentuado para a proteção de dados pessoais, sobretudo na ausência de parâmetros normativos uniformes para contratação e supervisão de operadores de tecnologia da informação no setor público.

Durante a pandemia de Covid-19, o cenário foi tensionado pela necessidade de expansão acelerada da infraestrutura tecnológica do Ministério da Saúde, em prazo reduzido e sob intensa pressão institucional para assegurar a continuidade de serviços essenciais e a produção de informações em tempo real (Brasil, 2022).

O caráter emergencial das contratações realizadas nesse período tende a comprimir ou suprimir etapas fundamentais da gestão do risco, como a verificação da maturidade do fornecedor em segurança da informação, a pactuação de cláusulas específicas de proteção de dados e a elaboração prévia de Relatório de Impacto à Proteção de Dados Pessoais (ANPD, 2021; TCU, 2025).

O salto mais representativo desse processo foi a implantação da Rede Nacional de Dados em Saúde (RNDS), infraestrutura central de interoperabilidade desenvolvida pelo DATASUS e lançada em caráter piloto em 2020 para apoiar o enfrentamento da pandemia, integrando dados de testagem, vacinação e vigilância epidemiológica provenientes de diferentes sistemas e pontos de atenção, públicos e privados (Brasil, 2022).

A integração das bases informacionais permitiu ganhos relevantes de operacionalização, como a consolidação em tempo quase real de indicadores nacionais de vacinação e a possibilidade de emissão de comprovantes digitais acessíveis pelo cidadão em múltiplos canais. Ao mesmo tempo, o modelo ampliou substancialmente o perímetro de dados pessoais sensíveis em circulação e multiplicou o número de agentes com acesso a essas informações (Brasil, 2022; Haddad; Lima, 2024).

A RNDS (Rede Nacional de Dados em Saúde) passou a interligar sistemas de esferas federal, estaduais, municipais e privadas, o que aumentou a complexidade das cadeias de responsabilidade e fiscalização, sem que os instrumentos contratuais e normativos disponíveis acompanhassem essa expansão com exigências proporcionais de segurança, transparência e prestação de contas (Brasil, 2022). Assim, ganhos de eficiência operacional e de coordenação da resposta sanitária conviveram com um incremento significativo do risco de exposição indevida de dados sensíveis de saúde, em um ambiente que já apresentava fragilidades prévias de governança e fiscalização dos contratos de TI.

Em avaliação recente sobre a implementação da LGPD na administração pública, o Tribunal de Contas da União constatou que a maioria das organizações federais ainda se encontrava em estágios iniciais de adequação, com deficiências relevantes em indicadores de preparação, contexto organizacional e capacitação de equipes, e identificou que parte expressiva das entidades sequer havia designado encarregado pelo tratamento de dados pessoais (TCU, 2025).

No caso do Ministério da Saúde, a fragilidade estrutural revelou-se de forma particularmente intensa, pois o órgão atuava, durante e após a pandemia, simultaneamente como responsável pela resposta à maior crise sanitária do século e como controlador de um dos maiores acervos de dados sensíveis de saúde do país (Brasil, 2022; ANPD, 2022). A sobreposição dessas atribuições contribuiu para que a dimensão de proteção de dados fosse subordinada à dimensão operacional da resposta à crise, justamente no período em que o tratamento de informações sensíveis atingia seu maior volume e em que os riscos de incidentes se mostravam mais elevados.

A dependência tecnológica, a limitada capacidade de fiscalização, a ausência de parâmetros normativos uniformes para contratação de serviços de tecnologia da informação na administração pública e a expansão acelerada sob pressão emergencial compõem o contexto estrutural no qual se desenvolveu o incidente de 2020 no Ministério da Saúde (TCU, 2017; TCU, 2025). Longe de representar episódio isolado de negligência individual, o vazamento massivo de dados sensíveis de saúde deve ser compreendido como manifestação concreta de um problema sistêmico de governança e de regulação da terceirização de TI em ambientes de alta criticidade.

O problema delineado constitui o objeto do tópico seguinte, que se desenvolve a partir da análise do edital que estruturou a contratação da empresa Zello Tecnologia

da Informação Ltda., instrumento responsável por estabelecer as condições jurídicas e técnicas da contratação. Busca-se identificar as vulnerabilidades verificadas em sua execução e as implicações jurídicas delas decorrentes, especialmente no que se refere à responsabilização do controlador público e da operadora privada.

3.2 O edital que estruturou a contratação da empresa Zello Tecnologia da Informação Ltda.: lacunas na proteção de dados, o incidente de 2020 e as implicações para a responsabilização

A Zello Tecnologia é empresa privada de desenvolvimento de software que, a partir de 2015, firmou contratos com ao menos quinze órgãos da Administração Pública federal. Dentre eles, o Ministério da Saúde consolidou-se como seu maior contratante individual, com repasses estimados em R$ 43 milhões de um total de aproximadamente R$ 151 milhões recebidos do erário até dezembro de 2020 (EM.COM.BR, 2020).

No âmbito do Ministério, a empresa atuava no desenvolvimento da camada de apresentação dos sistemas de notificação epidemiológica, o *front-end*[8], com destaque para o e-SUS Notifica, plataforma criada durante a pandemia para o registro em tempo real de casos suspeitos e confirmados de Covid-19 por profissionais e estabelecimentos de saúde de todo o país.

Operando como repositório de dados pessoais e sensíveis de saúde em escala nacional, o e-SUS Notifica concentrava informações como nome, CPF, endereço, telefone, condições clínicas preexistentes, resultados de exames e evolução do quadro de saúde de milhões de cidadãos, o que o tornava um dos ativos informacionais mais críticos do ecossistema digital do SUS (Brasil, 2020).

O primeiro incidente de segurança tornou-se público em novembro de 2020, quando pesquisadores identificaram que um cientista de dados do Hospital Israelita Albert Einstein, colaborador do Ministério da Saúde em projeto conjunto, havia publicado inadvertidamente, em repositório público da plataforma GitHub, planilha contendo credenciais de acesso aos sistemas e-SUS Notifica e Sivep-Gripe (G1, 2020). Tal exposição tornava tecnicamente possível o acesso a dados pessoais e médicos de ao menos 16 milhões de pacientes, incluindo nome, CPF, endereço,

[8] *Front-end* é a parte de um sistema ou site com a qual o usuário interage diretamente, como telas, botões, formulários e elementos visuais da interface.

telefone, doenças preexistentes, como diabetes, cardiopatias e HIV, além de resultados de testagem para Covid-19.

As investigações jornalísticas que noticiaram o caso evidenciaram a inexistência de mecanismos técnicos capazes de impedir que colaboradores externos, ainda que com acesso temporário, exportassem credenciais para ambientes abertos. Também foi constatada a ausência de rotinas de monitoramento interno aptas a identificar a exposição antes de sua descoberta por terceiros (G1, 2020).

As consequências da dupla omissão são severas, pois materializaram o vazamento massivo de dados sensíveis de saúde de milhões de cidadãos. A divulgação indevida dessas informações expõe os titulares a riscos concretos de discriminação, estigmatização social e fraudes identitárias.

Entre as práticas ilícitas mais recorrentes está a abertura fraudulenta de contas ou contratação de crédito mediante o uso combinado de dados pessoais e informações cadastrais obtidas em vazamentos. Registros médicos possuem alto valor no mercado ilícito por permitirem a criação de identidades falsas ou a realização de crimes financeiros complexos (ENISA, 2023).

Outro risco frequente é a fraude em serviços de saúde, na qual criminosos utilizam dados clínicos e identificadores pessoais para obter medicamentos, procedimentos ou reembolsos indevidos em nome da vítima (IESS, 2024). Também são comuns golpes de engenharia social, como mensagens ou ligações em que criminosos se passam por instituições de saúde, hospitais ou organizações internacionais para induzir vítimas a fornecer novas informações ou efetuar pagamentos fraudulentos (CNCS, 2020).

Para a Administração Pública, o dano projeta-se na perda de credibilidade do sistema de saúde digital e na atração de responsabilização civil e administrativa, o que corrói a confiança da sociedade na capacidade protetiva do Estado (Brasil, 2018), colocando em xeque a legitimidade democrática institucional.

Nesse contexto, a análise do edital que orientou a contratação demonstra que a governança de dados prevista no instrumento convocatório se limitava a previsões genéricas de confidencialidade e segurança da informação, sem estabelecer obrigações específicas relacionadas ao tratamento de dados pessoais.

Não foram identificadas cláusulas que disciplinassem, de forma clara, a definição dos papéis de controlador e operador, a adoção de padrões mínimos de segurança da informação ou a implementação de mecanismos de auditoria e

monitoramento das atividades desempenhadas pela contratada. Também inexistia previsão detalhada de procedimentos para gestão e comunicação de incidentes de segurança envolvendo dados pessoais, mesmo após a obrigatoriedade de observância da Lei Geral de Proteção de Dados Pessoais.

Essas lacunas indicam que a proteção de dados não foi incorporada de forma estruturada ao arranjo contratual. Quando o controlador público transfere a operação de bases de dados sensíveis sem impor controles estritos de acesso, trilhas de auditoria e mecanismos efetivos de monitoramento, a fiscalização torna-se limitada e o risco de falha sistêmica é transferido de forma desproporcional ao titular das informações (Moura; Oliveira, 2023). Com efeito, observa-se que a proteção de dados não foi incorporada de maneira estruturada ao arranjo contratual, mas tão somente baseou-se em referências genéricas incapazes de assegurar a efetiva governança do tratamento de informações sensíveis.

No caso analisado, as lacunas contratuais descritas produzem um cenário típico de fragilidade na governança de dados. Quando o controlador público transfere a operação de bases de dados sensíveis sem impor controles estritos de acesso, baseados no princípio do menor privilégio, e sem exigir trilhas de auditoria contínuas, ele abdica de seu dever prático de fiscalização. Nesse arranjo, o risco de falha sistêmica é transferido de forma desproporcional para o titular da informação, que permanece vulnerável diante da incapacidade estatal de aliar a modernização tecnológica a garantias jurídicas e operacionais concretas (Moura; Oliveira, 2023).

Entre os mecanismos que poderiam reduzir esse risco destacam-se a definição expressa dos papéis de controlador e operador, a exigência de controles de acesso baseados no princípio do menor privilégio, a manutenção de trilhas de auditoria contínuas e a previsão de procedimentos formais para detecção e comunicação de incidentes de segurança (Brasil, 2018; ANPD, 2023).

A ausência desses mecanismos contribuiu para a ampliação do risco sistêmico associado ao tratamento das informações. Semanas após a fraude envolvendo a Zello vir à tona, o cenário de vulnerabilidade tornou-se ainda mais evidente com a revelação de um segundo incidente de proporções significativamente maiores. Apurações indicaram que a interface visual do sistema e-SUS Notifica, também desenvolvida pela mesma empresa, continha credenciais de acesso expostas diretamente no código da aplicação, o que permitia que qualquer pessoa com acesso ao código obtivesse acesso indevido ao banco de dados do sistema.

Como consequência, a base cadastral associada ao Sistema Único de Saúde ficou exposta, atingindo dados de mais de 200 milhões de brasileiros, inclusive registros de pessoas falecidas. Estima-se que a vulnerabilidade tenha permanecido ativa por aproximadamente seis meses até ser identificada (G1, 2020; EM, 2020).

Diferentemente do primeiro incidente, a natureza dessa falha não decorre de erro humano isolado, mas de decisão tecnicamente inadequada de desenvolvimento. A inserção de credenciais diretamente no código da aplicação viola princípios elementares de segurança no desenvolvimento de *software* e contraria o conceito de segurança desde a concepção, segundo o qual controles de proteção devem ser incorporados desde as etapas iniciais do desenvolvimento dos sistemas (OSTEC, 2022).

Entre as diretrizes ignoradas no episódio destaca-se o gerenciamento seguro de credenciais. Boas práticas de segurança determinam que senhas e chaves de acesso sejam armazenadas em mecanismos especializados de proteção, jamais incluídas em texto claro no código-fonte (IBSEC, 2024). A prática também amplia a superfície de ataque do sistema, aumentando as oportunidades de exploração por agentes mal-intencionados (ANPD, 2025).

Do ponto de vista contratual, a questão central consiste em verificar se o instrumento convocatório estabelecia padrões mínimos de desenvolvimento seguro. A análise da minuta do edital indica que não havia previsão explícita de práticas específicas de segurança de *software*, como a proibição de inserção de credenciais no código-fonte ou a exigência de auditorias técnicas durante o desenvolvimento.

Essa lacuna pode ser parcialmente explicada pelo contexto normativo da época, uma vez que o edital foi elaborado em 2016, período anterior à promulgação da Lei Geral de Proteção de Dados Pessoais (Doneda, 2019). Entretanto, a entrada em vigor da LGPD durante a execução contratual passou a impor à Administração Pública o dever de adotar medidas técnicas e administrativas adequadas para proteção de dados pessoais (Brasil, 2018).

No caso analisado, contudo, os termos aditivos celebrados limitaram-se à prorrogação da vigência contratual, sem atualização das cláusulas relativas à segurança da informação ou à proteção de dados pessoais. A ausência de adequação contratual evidencia fragilidade na governança do tratamento de dados, uma vez que contratos administrativos que envolvem tratamento de dados pessoais devem refletir

as obrigações legais impostas ao controlador e aos operadores que atuam em seu nome (Bioni, 2020; Mendes; Doneda, 2021).

A repercussão do caso revelou divergência pública quanto à atribuição de responsabilidades. A Zello afirmou que sua atuação teria se limitado ao desenvolvimento da camada *front-end*, a qual não apresentaria erro de codificação, sustentando que eventuais vulnerabilidades decorreriam da arquitetura de serviços definida pelo próprio Ministério da Saúde (E.M., 2020). O Ministério, por sua vez, informou que permanecia apurando as causas do incidente e que havia solicitado auditoria dos demais serviços desenvolvidos no âmbito dos contratos vigentes.

A análise do episódio indica que a divergência entre as partes não afasta a existência de falhas estruturais no arranjo contratual e técnico da solução desenvolvida. Ainda que a empresa tenha afirmado atuar apenas na camada de interface do sistema, a exposição de credenciais diretamente no código da aplicação evidencia fragilidade nas práticas de desenvolvimento adotadas, pois a inclusão de informações sensíveis no código-fonte amplia significativamente o risco de acesso indevido ao sistema.

Por outro lado, o Ministério da Saúde, na condição de controlador dos dados e responsável pela governança da contratação, não estabeleceu requisitos técnicos claros de segurança nem mecanismos efetivos de fiscalização durante a execução do contrato, o que reduziu sua capacidade de prevenir ou identificar vulnerabilidades dessa natureza. O incidente parece decorrer, assim, da combinação entre deficiências técnicas na implementação da aplicação e lacunas institucionais na supervisão da contratação, a revelar que a fragilidade do sistema não pode ser atribuída exclusivamente à atuação de uma das partes, mas ao desenho institucional da contratação e à ausência de mecanismos efetivos de controle sobre a segurança da solução desenvolvida.

Do ponto de vista normativo, parâmetros amplamente adotados de governança em segurança da informação permitiriam compreender com maior clareza essas lacunas. Arranjos alinhados a um Sistema de Gestão de Segurança da Informação, como o previsto na ABNT NBR ISO/IEC 27001, exigem que a organização identifique riscos, estabeleça medidas para preveni-los e documente os controles adotados, inclusive quando há contratação de fornecedores. Em linhas gerais, a norma determina que a segurança da informação não pode depender de decisões pontuais,

mas integrar um processo contínuo de gestão, com definição clara de responsabilidades, registros verificáveis e monitoramento permanente.

No caso da contratação analisada, contudo, não se verificam elementos típicos desse modelo. O instrumento convocatório e os termos contratuais não estabelecem procedimentos estruturados de identificação e tratamento de riscos, tampouco exigem controles específicos relacionados ao desenvolvimento seguro de software ou à gestão de credenciais e acessos. Também não há previsão clara de auditorias contínuas ou de monitoramento técnico das atividades executadas pela contratada. A governança de segurança da informação associada ao contrato aproxima-se, portanto, mais de uma lógica reativa e pontual do que de um sistema estruturado de gestão de riscos, como preconizado pela referida norma técnica.

No plano técnico, boas práticas de desenvolvimento de sistemas recomendam que a programação incorpore critérios de segurança desde o início do ciclo, com testes específicos voltados à identificação de vulnerabilidades antes da entrada em operação (ISMS.Online, 2025a; ISO27001.com, 2026). Tais medidas costumam ser formalizadas como exigências documentadas e verificáveis, especialmente quando há participação de empresas terceirizadas no desenvolvimento. Entre os riscos amplamente reconhecidos nesse contexto está a inclusão de credenciais de acesso diretamente no código-fonte, prática desaconselhada por facilitar sua descoberta e possibilitar acessos não autorizados (Mitre, s.d.).

Nada indica, entretanto, que o edital tenha estabelecido exigências específicas de testes de segurança, revisão de código ou validação técnica independente antes da disponibilização das aplicações. A ocorrência do incidente, caracterizada justamente pela exposição de credenciais no código da aplicação, demonstra que controles técnicos dessa natureza não foram capazes de identificar a vulnerabilidade em tempo hábil.

Diante disso, a previsão de cláusulas contratuais específicas sobre segurança da informação, como a proibição de inserir credenciais diretamente no código, a exigência de boas práticas de gestão de acessos, a realização de revisões e testes de segurança e a entrega de registros que comprovem essas medidas, reduziria significativamente a margem de controvérsia posterior. Com obrigações técnicas claras e verificáveis, a atribuição de responsabilidade tenderia a ser mais objetiva.

A controvérsia pública revela um ponto juridicamente relevante. Caso o contrato tivesse atribuído de forma expressa à Zello a obrigação de adotar padrões

específicos de segurança no desenvolvimento, como aqueles previstos na ABNT NBR ISO/IEC 27001, com proibição clara de inserir credenciais no código-fonte, e caso existissem registros auditáveis das decisões técnicas adotadas durante a execução, a definição de responsabilidade seria mais objetiva e imediata.

No entanto, a ausência desses elementos transformou o incidente em um conflito de versões argumentativas, dificultando a efetivação da responsabilização prevista nos arts. 42 e 48 da Lei Geral de Proteção de Dados Pessoais (Brasil, 2018). Isso porque o edital que orientou a contratação não estabelecia parâmetros contratuais e técnicos claros relacionados à segurança da informação e à proteção de dados, como exigências de desenvolvimento seguro de software, gestão adequada de credenciais ou realização de testes de segurança antes da entrada em operação das aplicações.

O cenário evidencia um vácuo de *accountability*[9], precisamente o tipo de lacuna que instrumentos de governança e mecanismos de supervisão buscam evitar, conforme orientações da Agência Nacional de Proteção de Dados acerca da gestão de incidentes e da responsabilização de agentes de tratamento (ANPD, 2021).

À luz desse contexto, torna-se necessário examinar o caso a partir dos deveres jurídicos que regem o tratamento de dados pessoais na Administração Pública. Nessa perspectiva, identificam-se três lacunas estruturais no arranjo contratual analisado: descrição do tratamento, segurança da informação e cooperação entre as partes.

No que se refere à descrição do tratamento, os elementos tornados públicos indicam ausência de delimitação contratual suficientemente precisa acerca dos sistemas, ambientes e bases de dados que poderiam ser acessados pela contratada, bem como das categorias de dados efetivamente tratadas e dos perfis autorizados a manipulá-las. Essa indefinição contrasta com o princípio da necessidade consagrado pela Lei Geral de Proteção de Dados Pessoais, segundo o qual o tratamento deve se restringir ao mínimo indispensável para a finalidade pretendida (Brasil, 2018).

Em se tratando de dados pessoais sensíveis, como informações de saúde, essa exigência se torna ainda mais rigorosa. No caso, a inexistência de segregação clara entre ambientes de desenvolvimento e produção e a falta de definição estrita de perfis de acesso contribuem para ampliar o risco de exposição indevida. Portanto, a

[9] *Accountability*: princípio relacionado ao dever de prestação de contas, transparência e responsabilização pelos atos praticados, exigindo que agentes públicos ou privados expliquem e justifiquem suas decisões e assumam eventuais consequências decorrentes delas.

possibilidade de exportação de credenciais associadas a sistemas com dados de milhões de pacientes evidencia falha na delimitação e no controle do escopo de acesso. A consequência prática é a dificuldade de comprovação de que o controlador implementou medidas técnicas e organizacionais adequadas e proporcionais ao risco, o que fragiliza sua defesa em eventual responsabilização.

Já no que tange ao eixo da segurança da informação, a controvérsia envolvendo a inserção de credenciais diretamente no código-fonte sugere a inexistência de cláusulas contratuais expressas impondo padrões mínimos de desenvolvimento seguro. A prática conhecida como *hardcoding*[10] de credenciais é amplamente reconhecida como vulnerabilidade grave, pois facilita a descoberta de senhas e possibilita acessos não autorizados (OWASP, 2023; Mitre, s.d.).

Trata-se de conduta que denota desrespeito direto à norma NBR ISO/IEC 27001 da Associação Brasileira de Normas Técnicas (ABNT), que estabelece o dever de as organizações adotarem abordagem sistemática de gestão de riscos e implementar controles formais de segurança da informação, inclusive na relação com fornecedores (ISO, 2022). No entanto, a ausência de previsão contratual de revisão obrigatória de código, testes de segurança prévios à implantação em produção e manutenção de registros auditáveis dessas etapas indica falha na internalização desses controles. Na prática, isso desloca a gestão de riscos do campo preventivo para o campo reativo, permitindo que vulnerabilidades conhecidas evoluam para incidentes com impacto massivo.

Quanto à cooperação entre as partes, a divergência pública de versões acerca da origem da falha e a ausência de comunicação coordenada e tempestiva aos titulares afetados revelam a inexistência de fluxos formais previamente definidos para reporte e resposta a incidentes. Tal conduta fere o dever de comunicar à Agência Nacional de Proteção de Dados (ANPD) e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante (Brasil, 2018) previsto no art. 48 da LGPD.

Ademais, a própria ANPD orienta, por meio do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador e do Regulamento de Comunicação de Incidente de Segurança, que os agentes de tratamento mantenham

[10] *Hardcoding*: prática de programação que consiste em inserir valores ou parâmetros fixos diretamente no código de um sistema, em vez de obtê-los por meio de configurações externas ou entradas dinâmicas, o que pode reduzir a flexibilidade e a segurança do software.

procedimentos estruturados de resposta a incidentes, com registros capazes de documentar os eventos ocorridos e permitir a delimitação de responsabilidades (ANPD, 2021; ANPD, 2024).

A consequência prática dessa lacuna consiste na ampliação da insegurança jurídica, no retardamento da mitigação dos danos e na maior dificuldade de delimitação objetiva da responsabilidade entre controlador e operador, sobretudo quando o edital que estruturou a contratação não estabelece mecanismos claros de cooperação, reporte de incidentes e produção de evidências técnicas.

No caso do e-SUS Notifica, a vulnerabilidade decorrente da inserção de credenciais diretamente no código da interface da aplicação permaneceu ativa por cerca de seis meses antes de ser descoberta por agente externo. Segundo reportagens que noticiaram o episódio, após a constatação da falha foram adotadas medidas como a alteração das chaves de acesso e a correção pontual do código do sistema (G1, 2020; EM, 2020). Não há registro público, contudo, de comunicação formal do incidente à Agência Nacional de Proteção de Dados ou aos titulares potencialmente afetados, circunstância que pode caracterizar descumprimento do dever previsto no art. 48 da Lei Geral de Proteção de Dados Pessoais (Brasil, 2018).

A ausência de penalidades efetivas no caso evidencia a assimetria sancionatória que fragiliza o regime de responsabilização da LGPD em relação aos entes públicos controladores, comprometendo sua função preventiva e dissuasória (Brasil, 2018; ANPD, 2024). Revela ainda a necessidade de avaliar se, após 2020, os marcos normativos e as condições institucionais evoluíram o suficiente para assegurar proteção efetiva aos dados sensíveis de saúde em contratos de terceirização de TI.

3.3 Terceirização de TI, vulnerabilidades reiteradas e o déficit de densidade normativa na proteção de dados em Saúde

A análise das estratégias de compliance digital adotadas pela Administração Pública revela que ainda há sérias lacunas na proteção de dados dos usuários, sobretudo no que se refere à governança de segurança da informação e à gestão de incidentes envolvendo dados pessoais.

Especificamente no âmbito do Ministério da Saúde, observa-se que o caso Zello não encerrou o ciclo de vulnerabilidades do ecossistema digital da instituição.

Ao contrário, em dezembro de 2021, pouco mais de um ano após os primeiros incidentes terem sido detectados, o grupo criminoso Lapsus$ realizou ataque cibernético que comprometeu sistemas críticos como o e-SUS Notifica, o SI-PNI e o ConecteSUS, tornando indisponíveis dados de vacinação de milhões de brasileiros por período prolongado (Telesíntese, 2021).

Em dezembro de 2021, nova vulnerabilidade do ecossistema digital do Ministério da Saúde tornou-se evidente quando o grupo criminoso Lapsus$ realizou ataque cibernético que comprometeu sistemas como o e-SUS Notifica, o SI-PNI e o ConecteSUS. O ataque foi identificado na madrugada de 10 de dezembro de 2021, quando os portais do Ministério da Saúde e do ConecteSUS foram retirados do ar e substituídos por mensagem deixada pelos invasores (Poder360, 2021; IstoÉ Dinheiro, 2021). Embora rapidamente percebido, o incidente deixou a plataforma indisponível por cerca de treze dias (Jota, 2022), sem que haja dados públicos consolidados sobre eventuais prejuízos individuais sofridos pelos titulares.

Constatou-se que o vetor de entrada utilizado pelo grupo foi precisamente o mesmo tipo de vulnerabilidade identificado no caso Zello. Isto é, credenciais de acesso desprotegidas permitiram o comprometimento da infraestrutura em nuvem do Ministério sem que houvesse mecanismos de detecção e resposta tempestiva (POLI USP, 2022; Telesíntese, 2021).

A recorrência do mesmo vetor de ataque em intervalo inferior a doze meses é a evidência mais contundente de que as fragilidades reveladas em 2020 não foram efetivamente sanadas: a correção pontual do código do e-SUS Notifica e a substituição das credenciais expostas foram medidas de caráter reativo e localizado, insuficientes para resolver o problema estrutural de gestão de credenciais e de supervisão técnica da cadeia de operadores.

A reiteração do incidente poderia ter sido evitada pela implantação de um programa abrangente de segurança da informação, estruturado em gestão de identidades e credenciais, autenticação forte, arquitetura segura em nuvem e capacidades maduras de monitoramento e resposta, em vez de intervenções meramente pontuais sobre o código-fonte e sobre as senhas expostas (Brasil, 2016; Brasil, 2025)

Em termos de gestão de credenciais, a adoção de um modelo centralizado de gestão de acessos, com segregação rigorosa de contas privilegiadas, rotatividade periódica e automatizada de senhas, armazenamento de segredos em cofres

específicos e trilhas de auditoria completas, está alinhada às boas práticas preconizadas para a Administração Pública e teria reduzido sensivelmente a probabilidade de reutilização ou comprometimento prolongado de chaves de acesso a ambientes críticos em nuvem (Brasil, 2016).

Paralelamente, a substituição do modelo de autenticação baseado apenas em usuário e senha por mecanismos de autenticação multifator robusta para contas administrativas (incluindo uso de chaves físicas, aplicativos autenticadores e códigos de verificação), é reiteradamente apontada por guias técnicos e cartilhas especializadas como medida essencial para mitigar ataques baseados em credenciais vazadas, uma vez que impede o uso isolado da senha como vetor de entrada (CERT.BR, 2022; NIC.BR, 2022).

No plano arquitetural, a observância das diretrizes específicas para computação em nuvem no setor público, com segmentação de ambientes (desenvolvimento, homologação e produção), aplicação do princípio do menor privilégio, isolamento de redes e definição de zonas de segurança para sistemas que tratam dados sensíveis de saúde, teria limitado o movimento lateral de invasores e reduzido o escopo do comprometimento, ainda que uma credencial viesse a ser explorada com sucesso (Brasil, 2016; Brasil, 2025).

Finalmente, constitui requisito básico de uma política de segurança madura a implementação de processos permanentes de monitoramento, correlação de logs[11], detecção de anomalias e resposta a incidentes, tal como recomendado pelo Programa de Privacidade e Segurança da Informação (PPSI 2.0) e por normas de cibersegurança da Administração Pública. Isso porque, mecanismos dessa natureza permitiriam: identificar, em tempo quase real, o uso anômalo de credenciais privilegiadas, ativar planos de contenção e reduzir drasticamente a janela de indisponibilidade de serviços essenciais, como o e-SUS Notifica, o SI-PNI e o ConecteSUS, em atendimento ao dever de segurança previsto no artigo 49 da LGPD (Brasil, 2025; ANPD, 2025).

A persistência dessas vulnerabilidades no contexto atual das contratações de terceirizadas pela Administração Pública coloca em xeque a eficácia da LGPD como instrumento de proteção de dados sensíveis de saúde em contratos relacionados à TI. Isso porque, a Lei entrou em plena vigência em setembro de 2020, ao passo que sua

[11] Correlação de *logs* é o processo de analisar e relacionar diferentes registros (*logs*) de sistemas distintos para entender o que realmente aconteceu em um evento ou incidente.

aplicação sancionatória ocorreu em agosto de 2021, ou seja, no intervalo entre os dois ciclos de incidentes descritos envolvendo contratações pelo Ministério da Saúde. Isso significa que o ataque do Lapsus$ ocorreu já sob o pleno regime sancionatório da LGPD, no contexto de total operacionalização da ANPD e, portanto, sob a incidência da obrigação de comunicação de incidentes, a qual imprimia um dever plenamente vigente e exigível.

A ausência de responsabilização pública formal e de mudanças institucionais documentadas no Ministério da Saúde após o episódio de 2021 sugere que a LGPD, por si só, não tem sido suficiente para produzir os efeitos preventivos e dissuasórios esperados no âmbito da terceirização de TI em saúde. Isso remete ao debate sobre os limites normativos identificados no presente trabalho (Brasil, 2018), justificando a análise de novos marcos normativos com potencial de suprir as deficiências protetivas remanescentes.

Nesse sentido, três normas posteriores ao caso Zello merecem exame: a Lei nº 14.133, de 1º de abril de 2021, a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, e a Resolução CD/ANPD nº 15/2024. A Lei nº 14.133, conhecida como a Nova Lei de Licitações e Contratos Administrativos, estabelece, nos arts. 18 e 19, a obrigatoriedade de planejamento estruturado das contratações públicas, com identificação prévia de riscos e definição de requisitos técnicos para as soluções a serem contratadas (Brasil, 2021).

No âmbito das contratações de tecnologia da informação do Poder Executivo Federal, tais diretrizes foram detalhadas pela Instrução Normativa SGD/ME nº 94/2022, que disciplinou o processo de contratação de soluções de TIC pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

Observa-se que o contrato celebrado entre o Ministério da Saúde e a Zello foi firmado em contexto anterior à vigência da Lei nº 14.133/2021 e da regulamentação posterior das contratações de tecnologia da informação no âmbito do Poder Executivo Federal. A nova legislação passou a exigir que os órgãos públicos identifiquem riscos tecnológicos desde a fase de planejamento da contratação e estabeleçam mecanismos estruturados de gestão e fiscalização contratual (Brasil, 2021; Brasil, 2022).

No âmbito dessa regulamentação, a Instrução Normativa SGD/ME nº 94/2022 passou a exigir, entre outros aspectos, a elaboração de Estudo Técnico Preliminar

com identificação de riscos, a adoção de Modelo de Gestão do Contrato com mecanismos estruturados de fiscalização técnica e a assinatura, por todos os colaboradores da contratada diretamente envolvidos na execução, de Termo de Ciência de manutenção de sigilo e das normas de segurança vigentes no órgão contratante (Brasil, 2022).

A análise dessas exigências normativas permite compreender de forma mais clara as fragilidades evidenciadas no caso Zello. A exigência de identificação prévia de riscos tecnológicos no Estudo Técnico Preliminar, por exemplo, poderia ter levado à avaliação de vulnerabilidades associadas ao desenvolvimento e à operação dos sistemas envolvidos. Do mesmo modo, a previsão de modelo estruturado de gestão e fiscalização técnica do contrato ampliaria a capacidade do órgão contratante de acompanhar práticas de desenvolvimento seguro, gestão de credenciais e controle de acesso aos sistemas.

Sob essa perspectiva, a Nova Lei de Licitações e a regulamentação posterior das contratações de TIC reforçam uma mudança relevante de paradigma: a segurança da informação deixa de ser tratada como aspecto meramente acessório da execução contratual e passa a integrar a própria fase de planejamento da contratação. No contexto do caso Zello, a ausência de requisitos técnicos claros e de mecanismos estruturados de gestão de riscos evidencia precisamente o tipo de lacuna institucional que as novas regras procuram evitar.

O segundo marco é a Resolução CD/ANPD nº 15/2024, que operacionalizou o dever de comunicação de incidentes previsto no art. 48 da LGPD, estabelecendo prazos, conteúdo mínimo da comunicação e procedimentos de notificação à ANPD e aos titulares afetados (ANPD, 2024). Tais instrumentos, se efetivamente aplicados, teriam alterado de forma substancial o desfecho do caso Zello: a Lei nº 14.133/2021 e a IN SGD/ME nº 94/2022 teriam exigido a especificação contratual das obrigações que estavam ausentes, e a Resolução nº 15/2024 teria conferido ao dever de comunicação a especificidade operacional necessária para sua exigibilidade.

Entretanto, a efetividade desses marcos normativos depende de condições institucionais que os textos legais por si sós não criam. A Lei nº 14.133/2021 e a IN SGD/ME nº 94/2022 avançam ao exigir a especificação de requisitos de segurança desde a fase de planejamento, mas não fixam o conteúdo mínimo das cláusulas de proteção de dados para contratos de TI que envolvam o tratamento de dados sensíveis de saúde em larga escala. A escassez de densidade normativa aqui

verificada reproduz, em escala reduzida, o hiato identificado no primeiro capítulo deste estudo ao comparar o Regulamento Europeu (art. 28 do GDPR) à Lei Brasileira (art. 39 da LGPD): no Brasil, a existência da obrigação não é acompanhada de critérios suficientes para viabilizar sua aplicação prática.

O GDPR exige que o contrato entre controlador e operador especifique o objeto e a duração do tratamento, a natureza e a finalidade das operações, o tipo de dados e as categorias de titulares, as obrigações e os direitos do responsável, bem como deveres quanto à subcontratação, à segurança e à eliminação ou devolução dos dados. No entanto, o ordenamento brasileiro ainda não conta com regulamentação infralegal equivalente que traduza essas exigências para o contexto específico dos contratos públicos de TI em saúde (FADI, 2022; Brasil, 2021).

O caso Zello demonstra que a proteção efetiva de dados pessoais sensíveis de saúde em contratos de terceirização de tecnologia da informação exige mais do que a simples vigência da LGPD ou a inserção formal de cláusulas genéricas nos instrumentos contratuais. Para que tal regime alcance efetividade, é imperativo o preenchimento de ao menos quatro condições institucionais, as quais ainda não se verificam de forma integral no âmbito do Ministério da Saúde. São elas: capacidade técnica interna do órgão contratante; padrões mínimos verificáveis de segurança no desenvolvimento de software; obrigatoriedade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais, e protocolos de resposta a incidentes.

A primeira condição consiste na capacidade técnica interna do órgão contratante para fiscalizar a conformidade da contratada em matéria de segurança da informação, o que envolve a formação de equipes especializadas e a designação de responsáveis com atribuições efetivas de supervisão. Na prática, tais equipes deveriam realizar a análise técnica das soluções desenvolvidas pela contratada, acompanhar a implementação de controles de segurança da informação, verificar a adoção de práticas de desenvolvimento seguro de *software* e monitorar o cumprimento das obrigações contratuais relacionadas à proteção de dados.

A segunda condição refere-se à exigência, desde a fase de licitação, de padrões mínimos verificáveis de segurança no desenvolvimento de software, como os controles previstos na ABNT NBR ISO/IEC 27001 e as diretrizes da *OWASP*[12] para

[12] A OWASP (*Open Worldwide Application Security Project*) é uma fundação internacional sem fins lucrativos dedicada à segurança de aplicações. Suas diretrizes mais utilizadas em contratos de desenvolvimento seguro são o *Top 10*, que elenca as dez vulnerabilidades mais críticas em aplicações web, entre as quais figuram as falhas de autenticação e o armazenamento inadequado de credenciais, exatamente o vetor verificado no caso Zello, e

desenvolvimento seguro. Concretamente, tais padrões implicariam a obrigatoriedade de adoção de práticas formais de desenvolvimento seguro.

Essas incluem: a proibição de inserção de credenciais diretamente no código-fonte; a utilização de mecanismos seguros de gestão de chaves e segredos; a realização de revisões de código por pares; a execução periódica de testes de segurança e análise de vulnerabilidades antes da entrada em produção das aplicações; bem como a manutenção de registros técnicos capazes de comprovar a adoção dessas medidas ao longo do ciclo de desenvolvimento do software. A verificação desses controles permitiria ao órgão contratante avaliar de forma objetiva se a solução tecnológica atende a requisitos mínimos de segurança da informação, reduzindo a probabilidade de vulnerabilidades estruturais como aquelas observadas no caso analisado.

A terceira condição diz respeito à obrigatoriedade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais nos contratos que envolvam tratamento de dados sensíveis de saúde em larga escala, independentemente do caráter ordinário ou emergencial da contratação. Isso implicaria na identificação prévia das operações de tratamento de dados realizadas pelo sistema contratado, na avaliação dos riscos que tais operações podem representar aos direitos e liberdades dos titulares e na definição de medidas técnicas e administrativas destinadas a mitigar esses riscos.

Na prática, o relatório deveria descrever os fluxos de dados envolvidos, as bases legais aplicáveis, os perfis de acesso aos sistemas, os mecanismos de proteção adotados e os procedimentos previstos para prevenção e resposta a incidentes de segurança. Esse instrumento permitiria ao órgão contratante avaliar, ainda na fase de planejamento da contratação, se o tratamento de dados pessoais proposto é proporcional, necessário e compatível com as exigências da legislação de proteção de dados.

Por fim, a quarta condição consiste na previsão contratual expressa de protocolos de resposta a incidentes, com definição prévia dos fluxos de reporte entre operador e controlador, de modo a viabilizar o cumprimento dos prazos estabelecidos pela Resolução CD/ANPD nº 15/2024 (ANPD, 2024; ABNT, 2022). Com efeito, na prática, tais protocolos deveriam estabelecer procedimentos claros para identificação,

---

o *Application Security Verification Standard* (ASVS), que define requisitos mínimos de segurança exigíveis contratualmente de fornecedores de software (OWASP, 2021).

registro e classificação de incidentes de segurança, bem como a comunicação imediata da ocorrência ao órgão contratante.

Caberia ainda definir responsabilidades para análise técnica do evento, contenção da vulnerabilidade, preservação de evidências digitais e produção de registros capazes de reconstruir os fatos ocorridos. Esses mecanismos permitiriam que o controlador avaliasse a gravidade do incidente, adotasse medidas de mitigação e cumprisse tempestivamente o dever de comunicação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares potencialmente afetados.

Ainda que essas quatro condições sejam formuladas em termos contratuais, a experiência do Ministério da Saúde indica que sua realização não depende exclusivamente da redação de editais e cláusulas, mas também da existência de uma base normativa interna capaz de estabilizar papéis, fluxos e responsabilidades em matéria de proteção de dados. A partir dessa compreensão, a literatura destaca que a inserção de cláusulas específicas de proteção de dados em contratos administrativos pode funcionar como mecanismo de indução à conformidade normativa por parte das organizações que tratam dados em nome do poder público, ampliando a responsabilização e a transparência no tratamento dessas informações (Oliveira, 2024).

No entanto, ainda se observa uma incipiente compliance de dados no âmbito da Administração Pública federal, apesar de alguns esforços nesse sentido. A título de exemplo, pode-se citar a política de proteção de dados implementada por outro órgão federal: o Ministério do Meio Ambiente e Mudança do Clima (MMA).

O MMA possui decreto regimental que atribui à Ouvidoria competências análogas às do encarregado pelo tratamento de dados previsto no art. 41 da LGPD. Essa previsão confere maior suporte institucional à governança de proteção de dados no órgão. Ao positivá-las em norma regimental, o decreto fortalece a capacidade institucional de exigir dos operadores padrões mínimos de segurança da informação, elaboração de relatórios de risco e observância de protocolos de resposta a incidentes, inclusive aqueles previstos na Resolução CD/ANPD nº 15/2024 e nas normas técnicas da ABNT sobre gestão de incidentes (Brasil, 2024; ANPD, 2024; ABNT, 2020).

Em contraste, no Ministério da Saúde, a governança relacionada à proteção de dados pessoais tem sido estruturada predominantemente por portarias e instâncias colegiadas internas, como o Subcomitê de LGPD instituído pela Portaria GM/MS nº

3.114/2024, o que dispersa competências institucionais e delega a eficácia das normas à especificidade de cada contrato. Consequentemente, na ausência de uma governança de dados institucionalmente ancorada, os instrumentos contratuais tornam-se o principal recurso para mitigar as lacunas do regulamento interno. Essa modelagem traduz a fragilidade do arcabouço normativo interno, sobrecarregando o instrumento contratual, que passa a atuar como o principal mecanismo de viabilização dos deveres de segurança e notificação de incidentes (Brasil, 2020; MGI, 2023). Essa dinâmica de substituição normativa fica evidente na análise do caso Zello e na aplicação heterogênea da LGPD na referida Pasta ministerial.

Nesse contexto, a definição de parâmetros mínimos para futuros contratos de terceirização de tecnologia da informação não pode permanecer condicionada à iniciativa isolada de cada órgão ou à discricionariedade das equipes de contratação. Ao contrário, solução institucionalmente mais coerente consiste na positivação desses requisitos em normas internas estruturantes, como decretos regimentais, resoluções ou portarias de caráter geral, capazes de vincular de maneira uniforme os contratos celebrados pelo Ministério, e servir de referência para os demais órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação, o SISP (Brasil, 2018; Brasil, 2021; MGI, 2025).

Tal medida encontra respaldo nas diretrizes de governança e boas práticas previstas no art. 49 da LGPD e dialoga com o esforço de padronização promovido pelo Programa de Privacidade e Segurança da Informação, PPSI 2.0, cujo framework e guias orientam a formalização de papéis, controles e instrumentos essenciais em matéria de privacidade e segurança da informação (Brasil, 2018; MGI, 2025).

A inexistência, no Ministério da Saúde, de instrumento com densidade normativa comparável ao decreto regimental do Ministério do Meio Ambiente reforça a relevância dessa agenda. Enquanto no MMA as atribuições relacionadas à proteção de dados encontram-se expressamente consolidadas em decreto, no MS distribuem-se entre portarias, colegiados e atos administrativos diversos, o que reduz a centralidade normativa do tema e amplia a dependência de soluções contratuais construídas caso a caso (Brasil, 2023; Brasil, 2024; Brasil, 2025).

A instituição de padrão mínimo nacional, concebido em nível central e dotado de margem para adequação às peculiaridades de cada órgão, permitiria mitigar tais assimetrias, harmonizar a responsabilização dos controladores e oferecer base comum para a incorporação, nos contratos de terceirização de TI, de requisitos

técnicos verificáveis, da exigência de relatórios de impacto e de protocolos estruturados de resposta a incidentes, conforme previsto na LGPD, nos guias de requisitos e obrigações para contratações de TIC e no Regulamento de Comunicação de Incidentes da ANPD (Brasil, 2018; MGI, 2021; ANPD, 2024).

CONCLUSÃO

A análise desenvolvida ao longo deste trabalho demonstrou que a proteção de dados no setor público não se limita à existência de normas jurídicas formais, como a Lei Geral de Proteção de Dados (LGPD). A efetividade da LGPD depende da construção de estruturas institucionais de governança, de mecanismos de rastreabilidade das operações realizadas e da definição clara de responsabilidades entre os agentes envolvidos.

Nesse sentido, o primeiro capítulo examinou os fundamentos normativos da proteção de dados pessoais presentes na LGPD. Dentre eles, destacam-se os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção e responsabilização, bem como as diretrizes relacionadas à governança e à delimitação de responsabilidades entre controlador e operador previstas na Lei nº 13.709/2018 (Brasil, 2018). Ao final, o capítulo evidenciou que a legislação estabelece um modelo baseado em princípios, deveres de documentação e instrumentos preventivos, como os registros de tratamento e o Relatório de Impacto à Proteção de Dados Pessoais. Tais mecanismos são essenciais para garantir transparência, controle e responsabilização no tratamento de dados, sobretudo quando realizado por operadores privados contratados pela Administração Pública.

No segundo capítulo, a investigação voltou-se ao regime das contratações públicas de tecnologia da informação e aos desafios jurídicos associados à terceirização desses serviços. A análise revelou que a crescente dependência de empresas privadas para o desenvolvimento e manutenção de sistemas governamentais cria um cenário de assimetria técnica e informacional entre o ente público e os prestadores de serviço. Essa dinâmica pode comprometer a capacidade do Estado de exercer controle efetivo sobre as operações de tratamento de dados. Observou-se, ainda, que instrumentos contratuais insuficientemente detalhados tendem a gerar lacunas na definição das responsabilidades entre controlador e operador, dificultando a fiscalização e a responsabilização em situações de falha ou incidente de segurança.

A investigação empírica realizada no terceiro capítulo evidenciou de forma concreta essas fragilidades institucionais. A análise do caso envolvendo a empresa

Zello, no contexto dos sistemas de notificação epidemiológica do Ministério da Saúde durante a pandemia de Covid-19, demonstrou como vulnerabilidades técnicas e lacunas na governança de dados podem resultar em exposições massivas de informações sensíveis.

Nesse cenário, os incidentes analisados revelaram falhas relevantes na gestão de credenciais, na implementação de práticas de segurança desde a concepção e na manutenção de registros adequados das operações de tratamento. Sob a ótica técnica, verificou-se a exposição indevida de credenciais de acesso, a ausência de segregação rigorosa entre ambientes e perfis de acesso, a inserção de informações sensíveis diretamente no código-fonte da aplicação e a insuficiência de mecanismos de monitoramento, auditoria e resposta tempestiva a incidentes.

Sob a ótica jurídica, tais falhas evidenciaram a ausência de cláusulas contratuais específicas sobre desenvolvimento seguro, gestão de acessos, testes de segurança, comunicação de incidentes e produção de evidências técnicas, além de fragilizarem a observância dos princípios da necessidade, segurança, prevenção e responsabilização previstos na LGPD. Como consequência, tornou-se mais difícil delimitar objetivamente as responsabilidades entre controlador e operadora, bem como demonstrar a adoção de medidas técnicas e administrativas adequadas para a proteção de dados pessoais sensíveis.

A análise do caso Zello demonstrou que lacunas contratuais e fragilidades institucionais podem comprometer a efetividade da proteção de dados no setor público, especialmente em contextos de tratamento massivo de dados sensíveis. Com efeito, a consolidação de uma cultura de governança em privacidade, aliada ao aprimoramento dos instrumentos contratuais e das práticas administrativas, revela-se condição indispensável para que a LGPD cumpra sua função de assegurar a proteção dos titulares e fortalecer a confiança da sociedade nas estruturas digitais do Estado.

A pesquisa demonstrou, ainda, que a proteção de dados pessoais em contratos de terceirização de tecnologia da informação exige mais do que cláusulas genéricas de conformidade. A Administração Pública deve incorporar critérios técnicos rigorosos na seleção de fornecedores, exigir padrões claros de segurança da informação e estabelecer mecanismos contratuais que assegurem transparência, rastreabilidade e cooperação entre controlador e operador. Instrumentos como o Relatório de Impacto à Proteção de Dados Pessoais, a definição de protocolos de

resposta a incidentes e a manutenção de trilhas de auditoria constituem elementos centrais para a prevenção de falhas sistêmicas.

Por fim, conclui-se que a proteção de dados pessoais na Administração Pública constitui elemento essencial para a preservação da dignidade, da liberdade informacional e da própria legitimidade democrática das instituições. Em uma sociedade cada vez mais orientada pelo tratamento massivo de informações, garantir a adequada segurança e governança desses dados não representa apenas uma exigência jurídica, mas um compromisso institucional com a proteção dos direitos fundamentais dos cidadãos.

REFERÊNCIAS

ALMEIDA, Fernanda Gomes. **A proteção de dados pessoais como um direito fundamental autônomo na atual sociedade da informação**. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal da Bahia, Salvador, 2019. Disponível em: https://repositorio.ufba.br/handle/ri/37640. Acesso em: 7 mar. 2026.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022: tecnologia da informação — segurança da informação, segurança cibernética e proteção da privacidade**. Rio de Janeiro: ABNT, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo sobre a função do controlador, do operador e do encarregado**. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 7 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo sobre segurança da informação para agentes de tratamento de pequeno porte**. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf. Acesso em: 7 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 1, de 28 de outubro de 2021**. Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados. Diário Oficial da União, Brasília, 29 out. 2021. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso em: 9 mar. 2026.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança no âmbito da Autoridade Nacional de Proteção de Dados. Diário Oficial da União, Brasília, 25 abr. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 9 mar. 2026.

BESSA, Leonardo Roscoe. **LGPD: direito ou dever de privacidade?** C**onsultor Jurídico**, São Paulo, 8 fev. 2021. Disponível em: https://www.conjur.com.br/2021-fev-08/leonardo-bessa-lgpd-direito-ou-dever-privacidade. Acesso em: 7 mar. 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

BRASIL. **Constituição (1988). Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Inclui a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 7 mar. 2026.

BRASIL. **Decreto-Lei nº 200, de 25 de fevereiro de 1967**. Dispõe sobre a organização da Administração Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm. Acesso em: 7 mar. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 7 mar. 2026.

BRASIL. **Lei nº 14.133, de 1º de abril de 2021**. Lei de Licitações e Contratos Administrativos. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm. Acesso em: 7 mar. 2026.

BRASIL. Ministério da Saúde. **Edital de licitação nº 05/2016**. Disponível em: https://www.comprasnet.gov.br/acesso.asp?url=/edital-250110-05-16-2016. Acesso em: 8 mar. 2026.

BRASIL. Ministério da Saúde. **Estratégia de Saúde Digital para o Brasil 2020–2028**. Brasília: Ministério da Saúde, 2020. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 7 mar. 2026.

BRASIL. Ministério da Saúde. **Política Nacional de Informação e Informática em Saúde**. Brasília: Ministério da Saúde, 2016. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/politica_nacional_informacao_informatica_saude.pdf. Acesso em: 7 mar. 2026.

BRASIL. Ministério da Saúde. **Viva o SUS! O maior sistema público de saúde do mundo é gratuito, universal e do Brasil**. Brasília: Ministério da Saúde, 2025. Disponível em: https://www.gov.br/saude/pt-br/assuntos/noticias/2025/setembro/viva-o-sus-o-maior-sistema-publico-de-saude-do-mundo-e-gratuito-universal-e-do-brasil. Acesso em: 9 mar. 2026.

BRASIL. Tribunal de Contas da União. **Auditoria aponta falhas na aplicação da LGPD por organizações federais**. 2025. Disponível em: https://portal.tcu.gov.br/imprensa/noticias/auditoria-aponta-falhas-na-aplicacao-da-lgpd-por-organizacoes-federais. Acesso em: 7 mar. 2026.

BRASIL. Tribunal de Contas da União. **Referencial básico de governança organizacional para organizações públicas e outros entes jurisdicionados ao TCU**. 3. ed. Brasília: TCU, 2020. Disponível em:

https://portal.tcu.gov.br/data/files/FB/B6/FB/85/1CD4671023455957E18818A8/Referencial_basico_governanca_organizacional_3_edicao.pdf. Acesso em: 7 mar. 2026.

CERT.BR; NIC.BR. **Autenticação**: cartilha de segurança para internet. São Paulo: Comitê Gestor da Internet no Brasil, 2022. Disponível em: https://cartilha.cert.br/fasciculos/autenticacao/fasciculo-autenticacao.pdf. Acesso em: 7 mar. 2026.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo**. 36. ed. Rio de Janeiro: Forense, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo et al. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

EUROPEAN DATA PROTECTION SUPERVISOR. **The history of the General Data Protection Regulation**. 2018. Disponível em: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 7 mar. 2026.

EUROPEAN UNION AGENCY FOR CYBERSECURITY. **ENISA Threat Landscape**: Health Sector (January 2021 to March 2023). Atenas: ENISA, 2023. Disponível em: https://www.enisa.europa.eu/publications/health-threat-landscape. Acesso em: 9 mar. 2026.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a governança de TI**: da estratégia à gestão de processos e serviços. 4. ed. Rio de Janeiro: Brasport, 2014.

FORTINI, Cristiana; VIEIRA, Virginia Kirchmeyer. Terceirização na Administração Pública. In: **Enciclopédia jurídica da PUC-SP**. Tomo de Direito Administrativo e Constitucional. 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2021. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/5/edicao-1/terceirizacao-na-administracao-publica. Acesso em: 9 mar. 2026.

G1. **Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 7 mar. 2026.

G1. **Vazamento de senhas do Ministério da Saúde expõe informações de pacientes com Covid-19**. Disponível em: https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml. Acesso em: 7 mar. 2026.

HADDAD, Ana Estela; LIMA, Nísia Trindade. Saúde digital no Sistema Único de Saúde (SUS). **Interface – Comunicação, Saúde, Educação**, Botucatu, v. 26, 2022.

Disponível em: https://www.scielo.br/j/icse/a/nZkyh3JK8dNkZMkxcPjg9gm/. Acesso em: 7 mar. 2026.

INSTITUTO DE ESTUDOS DE SAÚDE SUPLEMENTAR. **Impacto das fraudes e desperdícios sobre gastos da Saúde Suplementar**. São Paulo: IESS, 2024. Disponível em: https://www.iess.org.br/biblioteca/tds-e-estudos/estudos-especiais-do-iess/impacto-das-fraudes-e-desperdicios-sobre-gastos. Acesso em: 9 mar. 2026.

ISTOÉ DINHEIRO. **Ransomware**: entenda o crime que derrubou o site do Ministério da Saúde. 10 dez. 2021. Disponível em: https://istoedinheiro.com.br/ransomware-entenda-o-crime-que-derrubou-o-site-do-ministerio-da-saude/. Acesso em: 9 mar. 2026.

JOTA. **ConecteSUS**: apagão e vulnerabilidade do tratamento de dados. 12 jan. 2022. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/conectesus-apagao-vulnerabilidade-tratamento-de-dados. Acesso em: 9 mar. 2026.

KHOURI, Paulo Roque. **Direito do consumidor na sociedade da informação**. Curitiba: Juruá, 2013.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice; BORELLI, Alessandra (coord.). **LGPD**: Lei geral de proteção de dados pessoais comentada. 4. ed. São Paulo: Revista dos Tribunais, 2022.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 2. ed. São Paulo: Saraiva Educação, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei geral de proteção de dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, 2018.

MOURA, Téssio Rauff de Carvalho; OLIVEIRA, Arlley Cavalcante de. A aplicação da LGPD nos contratos de terceirização do poder público. **Revista Direito UNIFACS**, Salvador, n. 282, 2023. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/8587. Acesso em: 7 mar. 2026.

OLIVEIRA, Kátia Adriana Cardoso de. Formação de jurisprudência administrativa pela ANPD: estudo de casos das sanções aplicadas. **Revista Digital de Direito Administrativo**, Ribeirão Preto, v. 11, n. 2, p. 89-109, 2024. Disponível em: https://revistas.usp.br/rdda/pt_BR/article/view/216721. Acesso em: 9 mar. 2026.

OLIVEIRA, Tatiana Reinehr de. **Padrões mínimos para a estratégia de inteligenciamento urbano à luz do direito e das políticas públicas**: uma aplicação a Brasília. 2024. Tese (Doutorado em Direito) – Centro Universitário de Brasília (CEUB), Brasília, 2024.

OPEN WORLDWIDE APPLICATION SECURITY PROJECT. **OWASP Mobile Top 10**: M1 — Improper Credential Usage. [S.l.]: OWASP Foundation, 2023. Disponível em: https://owasp.org/www-project-mobile-top-10/2023-risks/m1-improper-credential-usage. Acesso em: 9 mar. 2026.

OSTEC. **Sete conceitos do security by design**. 2022. Disponível em: https://ostec.blog/geral/sete-conceitos-security-by-design/. Acesso em: 7 mar. 2026.

PECK, Patrícia. **Direito digital**. 6. ed. São Paulo: Saraiva, 2018.

PODER360. **Sites do Ministério da Saúde sofrem ataque hacker e estão fora do ar**. 10 dez. 2021. Disponível em: https://www.poder360.com.br/governo/sites-do-ministerio-da-saude-sofrem-ataque-hacker-e-estao-fora-do-ar/. Acesso em: 9 mar. 2026.

TELESÍNTESE. **Site do Ministério da Saúde e o app do ConecteSUS sofrem ataque hacker**. 10 dez. 2021. Disponível em: https://telesintese.com.br/site-do-ministerio-da-saude-e-o-app-do-conectesus-sofrem-ataque-hacker/. Acesso em: 9 mar. 2026.

VAINZOF, Rony. LGPD e relatório de impacto à proteção de dados. **Consultor Jurídico**, São Paulo, 28 jun. 2021. Disponível em: https://www.conjur.com.br/2021-jun-28/rony-vainzof-lgpd-relatorio-impacto-protecao-dados/. Acesso em: 9 mar. 2026.

VALE, Luís Manoel Borges do; OLIVEIRA, Rafael Carvalho Rezende. **LGPD na Administração Pública**. Rio de Janeiro: Forense, 2025. ISBN 978-85-3099-573-7.

WELIVESECURITY. **Falha do Ministério da Saúde expõe dados de mais de 243 milhões de brasileiros**. 2020. Disponível em: https://www.welivesecurity.com/br/2020/12/04/falha-do-ministerio-da-saude-expoe-dados-de-mais-de-243-milhoes-de-brasileiros. Acesso em: 7 mar. 2026.