ALÉM DAS FRONTEIRAS FÍSICAS: A EFICÁCIA DA EXTENSÃO DA JURISDIÇÃO E DOS PADRÕES DE SEGURANÇA NA PROTEÇÃO DE DADOS DE SAÚDE EM DETRIMENTO DA *DATA LOCALIZATION*

BEYOND PHYSICAL BORDERS: THE EFFECTIVENESS OF EXTENDING JURISDICTION AND SECURITY STANDARDS IN PROTECTING HEALTH DATA VERSUS DATA LOCALIZATION

Alessandra Londero
Universidade Federal de Santa Maria, Brasil

Valéria Ribas do Nascimento
Universidade Federal de Santa Maria, Brasil

Pillar Crestani
Universidade Federal de Santa Maria, Brasil

DOI: http://dx.doi.org/10.31512/rdj.v25i52.2468 Recebido em: 19.02.2025 Aceito em: 12.10.2025

Resumo: O presente artigo observa a eficácia da proteção de dados pessoais de saúde no contexto da transformação digital e do *Big Data*, onde tais informações tornaram-se ativos econômicos e vetores de vulnerabilidade social. Mediante o método dedutivo e pesquisa bibliográfica, o estudo problematiza a viabilidade da localização física dos dados, ou *Data Localization*, frente à necessidade de fluxos transnacionais para a pesquisa biomédica e a interoperabilidade de sistemas de e-Saúde. A pesquisa compara as diretrizes da Lei Geral de Proteção de Dados e do Regulamento Geral sobre a Proteção de Dados, destacando que a restrição geográfica absoluta pode obstaculizar a inovação sem garantir segurança efetiva na nuvem. Os resultados indicam que a proteção não deve residir no confinamento territorial, mas na extensão da jurisdição legal, assegurando que a tutela jurídica acompanhe o dado independentemente das fronteiras. Conclui-se que a segurança dos dados sensíveis depende da implementação de rigorosa governança e medidas técnicas, como criptografia, anonimização e Relatórios de Impacto, permitindo o fluxo livre de informações com confiança e responsabilidade, em detrimento de barreiras físicas anacrônicas.

Palavras-chave: Fluxo de dados; Eficácia; Saúde; *Data Localization*; Proteção.

Abstract: The present article observes the efficacy of personal health data protection in the context of digital transformation and Big Data, where such information has become economic assets and vectors of social vulnerability. Through the deductive method and bibliographic research, the study problematizes the viability of the physical location of data, or Data Localization, facing the need for transnational flows for biomedical research and the interoperability of e-Health systems. The research compares the guidelines of the General Data Protection Law and the General Data Protection Regulation, highlighting that absolute geographic restriction can hinder innovation without guaranteeing effective security in the cloud. The results indicate that protection should not reside in territorial confinement, but in the extension of legal jurisdiction, ensuring that legal protection accompanies the data regardless of borders. It is concluded that the security of sensitive data depends on the implementation of rigorous governance and technical measures, such as encryption, anonymization, and Impact Reports, allowing the free flow of information with trust and responsibility, to the detriment of anachronistic physical barriers.

Keywords: Data fow; Effectiveness; Health; Data localization; Protection.

Introdução

O mundo está conectado pela transformação digital, a internet revolucionou o funcionamento de tudo, modificou vidas e hábitos, desde a maneira de se fazer pesquisa, de se trabalhar, aprender e ensinar. E não existe um setor que hoje não esteja vinculado a processos digitais, o que resulta no acesso constante de dados coletados o tempo todo, sejam dados gerais ou mesmo pessoais. Esta conjuntura social e econômica é fundamentada no processamento de dados em larga escala, na qual a tecnologia da informação se tornou uma ferramenta indispensável para a construção do conhecimento.

No âmbito específico da saúde, corroborado pelo advento da e-Saúde e do *Big Data*, se percebe uma nova forma de organizar e processar informações de pacientes. Os dados pessoais, anteriormente vistos apenas como registros clínicos, tornaram-se ativos econômicos de alto valor, como se fosse o novo petróleo da era digital, consideradas ferramentas cruciais para diagnósticos precisos, terapias inovadoras e a implementação de uma medicina personalizada e baseada em evidências.

Porém, essa digitalização apresenta uma dualidade crítica. Ao mesmo tempo em que os dados de saúde possibilitam avanços científicos, eles se tornaram vetores de discriminação e vulnerabilidade para os seus titulares. O conjunto dessas informações compõe os perfis ou as identidades digitais, possuindo valor político e, sobretudo, econômico, vez que podem ser a matéria prima para o uso de *softwares* diretamente atrelados às novas formas de controle social, especialmente mediante o uso de algoritmos, por isso, a proteção de dados é, em síntese, a proteção da pessoa (Caldeira; Sarlet, 2019).

O processamento massivo de informações sensíveis permite a criação de perfis (*profiling*) e diagnósticos algorítmicos que, se mal utilizados, podem limitar as possibilidades de vida dos indivíduos, manipular comportamentos e gerar estigmatização, consolidando o fenômeno do "paciente de vidro", cuja intimidade é transparente e acessível a terceiros (Molinaro; Sarlet, 2019, p. 189). A gravidade desse cenário é evidenciada por incidentes recentes, como a falha de segurança no sistema do Ministério da Saúde que expôs dados de 16 milhões de pacientes com suspeita de Covid-19 e o vazamento de informações de mais de 200 milhões de brasileiros (Bertoni, 2020).

Diante desse contexto, considerando a chance de risco, a presente pesquisa problematiza a eficácia de medidas focadas estritamente na localização física dos dados (*Data Localization*) para o tratamento utilizado considerando a proteção das informações referentes a saúde do paciente-usuário.

Em um mundo regido pela computação em nuvem (*cloud computing*), o processamento de informações migrou de máquinas locais para *data centers* virtuais e redes transnacionais, tornando a geografia física do armazenamento uma barreira porosa e, muitas vezes, irrelevante para a segurança efetiva (Molinaro; Sarlet, 2019). A e-Saúde e a pesquisa biomédica moderna dependem intrinsecamente de fluxos transfronteiriços de dados para garantir a interoperabilidade de sistemas e o avanço científico, o que pode demonstrar que a restrição geográfica absoluta seja um obstáculo à inovação.

Portanto, a proteção de dados na era da nuvem não deve residir na tentativa anacrônica de confinar o dado a um território físico, mas sim na garantia da extensão da jurisdição da lei. A eficácia regulatória, conforme observado na Lei Geral de Proteção de Dados (LGPD), que é brasileira e no Regulamento Geral sobre a Proteção de Dados (GDPR) europeu, baseia-se na extraterritorialidade: a proteção jurídica deve acompanhar o dado onde quer que ele esteja. O desafio central, que justifica esta investigação, é assegurar que mecanismos de governança, segurança técnica e adequação legal viajem com a informação, garantindo a soberania dos dados e a autodeterminação informativa do paciente, independentemente das fronteiras geográficas por onde esses dados circulam.

Quanto à metodologia empregada no presente artigo, adotou-se o método dedutivo, partindo de uma visão ampla para chegar aos pontos específicos que parte da visão do uso de dados sensíveis de saúde até a proteção efetiva dos dados vinculados a saúde. Em relação à teoria de base, utilizou-se o método sistêmico-complexo, fundamentado nas lições de Capra e Morin, levando em consideração de que modo os resultados influenciam a sociedade. Sobre a abordagem, utilizou-se o método funcionalista. Na aplicação do procedimento, recorre-se a pesquisa bibliográfica, a análise documental e de material disponível em plataformas online, e no que diz respeito à técnica, o levantamento de todas as informações possíveis sobre o assunto se deu através de fichamentos, resumos, análise de documentos, notícias, trabalhos e doutrina, enquadrando a presente pesquisa nos mais variados eixos temáticos contemporâneos.

A vulnerabilidade dos dados de saúde

os dados pessoais propriamente ditos e determinados pela Lei nº 13709/2018, a LGPD (artigo 5º, incisos I e II) fazem menção a informações do indivíduo, que traz à tona a possibilidade de identifica-lo, e mais especificamente sobre os dados pessoais sensíveis que aí versam sobre as características que determinam peculiaridades próprias daquela pessoa, como raça, etnia, convicção religiosa, opinião política, vida sexual, saúde, enfim assuntos que requerem um tratamento especial e apropriado. A definição além da lei nacional, também encontra arcabouço, por exemplo, no GDPR (Regulamento Geral de Proteção de Dados) europeu que destaca a necessidade de ter proteção específica, uma vez que determinado contexto do tratamento de tais dados poderá implicar riscos significativos para os direitos e liberdades fundamentais (Zaganelli; Filho, 2022).

A importância que tais dados carregam faz com que exista vulnerabilidade no seu manejo, visto que qualquer tipo de vazamento pode comprometer tanto o individual, sobre a intimidade e privacidade do paciente, quanto no coletivo, em se tratado de informações que podem desencadear uma crise sanitária de saúde. E em se tratando de tal risco que emerge e necessidade de se ter uma proteção eficaz.

O valor e o risco dos dados de saúde

Essa preocupação com os procedimentos adotados que envolvem esses dados é relacionada com a qualidade que essas informações carregam, pois formam a individualidade que o titular tem garantido através de direitos fundamentais e de privacidade. Por si só isso já demonstra a vulnerabilidade de operações que envolvem dados pessoais, e isso é acentuado quando tais informações se referenciam a questões que envolvem a saúde, que são fornecidas, coletadas, armazenadas e tratadas com o objetivo de preservar a qualidade de vida e bem-estar de pessoas.

A vulnerabilidade dos dados de saúde pressupõe um cuidado atento, pois assim como pode servir para fomentar novas tecnologias que influenciam pesquisas e bases científicas, também podem expor a vida privada causando danos a personalidade e discriminação. E isso acontece porque os dados possuem valor, que vai além do econômico, pode ser social, político, que são relevantes quando podem ser aplicados para determinar perfis digitais que servem de manobra para projetar políticas de influência e algoritmos especialmente de consumo, comprometendo o raciocínio crítico e estimulando o controle social massivo (Caldeira; Sarlet, 2019). A compreensão do poder que a utilização dos dados possui na contemporaneidade é categoricamente descobrir o fogo da revolução tecnológica, pois garante domínio sobre os demais, e mais perigosamente soberania para poucos.

O uso de algoritmos e de *Big Datas* para o armazenamento em nuvem dos dados coletados emerge novas situações, entre elas o "Dataísmo", que conforme Costa, Lima e Gonçalves

(2023), determina que os dados são ferramentas fundamentais que possibilitam a compreensão do mundo, ou seja, é preciso dessa troca frenética e interminável de dados para pertencer ao mundo atual. E também a ideia do "paciente de vidro", onde todos os elementos coletados são disponibilizados, pois além do viés comercial quando são fornecidas informações em clínicas, médicos, farmácias, ainda existe o viés público coletando dados em hospitais, postos de saúde, prontos-socorros, ou qualquer outro agente/instituição vinculada as políticas públicas de saúde. Isto é, informações de bandeja que podem ser utilizadas de inúmeras maneiras e sem o mínimo de transparência caso não estejam protegidas (Molinaro; Sarlet, 2019, p.189).

O risco do vazamento dos dados de saúde incute em catástrofes sanitárias, mas também em uma onda discriminatória. Todo o titular tem o direito de privacidade sobre sua saúde, genética e questões médicas. Cada um sabe sobre si e o que lhe convém diante de doenças físicas e mentais, ninguém pode se utilizar de privilégio de informação para tomar decisões que envolvem a vida de terceiros. Isso pode ser visualizado em contratações de funcionários com base na consulta irregular de bancos de dados protegidos ou até mesmo no preconceito a pessoas com deficiência não visível.

E infelizmente foi algo que já aconteceu no Brasil, em 2020 na época da Pandemia de Covid-19, quando por quebra de segurança o Ministério da Saúde sofreu uma falha e divulgou informações de mais de 200 milhões de brasileiros que utilizaram plano de saúde ou o aplicativo da plataforma vinculado ao Sistema Único de Saúde (Bertoni, 2020). Isso demonstra que já existem erros e que mesmo as plataformas vinculadas a entes públicos não conseguem garantir total proteção ao acesso indevido ou irregularidades. Se já se tem conhecimento sobre possíveis erros, por que se insiste na utilização da transferência de dados pessoais?

A necessidade do fluxo de dados

O fluxo de dados facilita o acesso à saúde. Isso decorre há muito tempo, através da troca de informações, de resultados de pesquisas, de experimentos e diagnósticos que profissionais da saúde divulgam, mas além disso, e impulsionado pelo isolamento social causado pelo Coronavírus, também se amplificou a disponibilidade de cuidados médicos com a telemedicina e demais plataformas *onlines* que puderam manter um nível de funcionalidade de serviço de saúde no país e no mundo todo.

A telemedicina pôde proporcionar que pessoas enfermas conseguissem atendimento sem se expor ao risco de Covid-19, ou mesmo que pessoas com doenças já existentes não precisassem sair de casa para continuar com seus tratamentos de maneira segura. Porém essa segurança à exposição do vírus pode colocar em risco a segurança à privacidade, afinal as plataformas que mantem os sistemas de comunicação entre paciente e médico são alimentadas com dados pessoais e dados sobre a saúde. E por mais que existam regulações de uso e garantias de sigilo do Código

de Ética Médica, ainda existe a chance da falha e de vazamento de dados (Filho; Zaganelli, 2022, p. 217).

Além das consultas *online* também existem dispositivos específicos de busca utilizados por profissionais da saúde, para consultar exames, laudos, medicamentos, novos tratamentos e estudos ou os códigos da CID (Classificação Internacional de Doenças), por exemplo (Caldeira; Sarlet, 2019, p.11). E assim se percebe que as transferências das informações podem ultrapassar fronteiras, encontrando respostas inclusive em servidores internacionais, onde estão a maioria das nuvens de armazenamento.

É importante ressaltar que esse uso transfronteiriço de dados, principalmente no que tange a saúde, é extremamente necessário, pois influencia diretamente no desenvolvimento médico, e qualquer tipo de barreira, inclusive territorial pode acarretar em prejuízos a pesquisas biomédicas e a interoperabilidade de sistemas de crises de saúde (Molinaro; Sarlet, 2019, p. 188). Assim se compreende o papel da troca de dados, mas mais ainda o motivo de se ter uma proteção eficaz com eles. E para tanto o próximo subcapítulo trata da proteção de *Data Localization*, e se é a adequada para a garantia da guarda dos dados relacionados a saúde.

A problemática da proteção por território e a garantia de adequação internacional

A proteção do uso de dados é um direito de todos, e, portanto, deve ser garantido por medidas que realmente funcionem. E para analisar essa eficácia é preciso observar o que é apresentado juridicamente no Brasil, pela LGPD e então comparar com a GDPR da União Europeia e com algumas aplicações das leis norte-americanas, e assim observar como essa proteção por localização acontece e se de fato cumpre com seu objetivo de anteparo, mais ainda se ela é suficiente, ou se carece de complemento.

O modelo de transferência internacional e adequação

Tanto o Brasil quanto os países da União Europeia possuem regulamentação sobre as transferências de dados, a LGPD e a GDPR. Ambas dispõem de diretrizes, conceitos técnicos e regras para o tratamento dos dados pessoais, com foco na privacidade e segurança contra vazamentos, e intrinsicamente aos dados relacionados a saúde. Cabe compreender primeiramente o que cada uma fala sobre o assunto.

Apesar da lei nacional ter inspiração na lei da Europa, elas possuem disparidades no tratamento a dados sensíveis. A LGPD menciona no seu artigo 11 quais são as situações que exigem tratamento de dados pessoas sensíveis, como quando houver consentimento para finalidades específicas, ou então mesmo sem o consentimento, mas em situações que possam comprometer a segurança pública, cumprimentos legais, a vida de terceiros e principalmente a

alínea "f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária" (Brasil, 2018). Já a GDPR trata seus dados sensíveis proibindo seu tratamento como regra geral, restando como exceção algumas possibilidades fundamentadas (Filho; Zaganelli, 2022, p. 220).

Outra diferença considerada é sobre dados de menores de idade, onde a GDPR acaba sendo mais permissiva deixando o consentimento por conta de pessoas maiores de 16 anos, já no Brasil requer que os responsáveis aprovem a coleta dos dados até completar a maioridade, 18 anos. Também existe divergência quanto ao vinculo de responsabilidade entre controlador e operador na lei brasileira, já na lei europeia existe a discriminação prevista. Se nota ainda disparidade nas questões que envolvem Relatórios de Impacto e prazos de comunicação de cometimento de irregularidades às autoridades, quando a lei internacional é mais específica a aprimorada com relação a nacional (Filho; Zaganelli, 2022).

Em um panorama geral se percebe um maior detalhamento da GDPR, mas não significa que não existam carências, assim como também se observa na LGPD. Fato é que ambas ainda que possuindo deficiências são mais criteriosas e restritas se comparadas a lei norte-americana. Os Estados Unidos focam na autorregulação[1], diferente da análise da proteção de mesmo nível, ou seja, por se aterem mais em leis setoriais acabam causando problemas de jurisdição, restando claro que o problema está relacionado mais a legislação do país de destino do que a distância propriamente dita (Guidi, 2021, p. 179).

Observando de modo simples a atuação do poder regulatório sobre a proteção do fluxo de dados é interessante que se considere os direitos que devem ser priorizados, a privacidade do indivíduo precisa prevalecer, independente dos fins. Mas deixar isso a cargo de autoridades ou de políticas internas ainda identifica um problema de adequação que pode comprometer as relações internacionais sobre as transferências de dados, e prejudicar principalmente aqueles que se submetem a soberania digital dos que detêm mais poder.

O papel da *Data Localization*

A garantia de fluxo de dados é muito importante, move máquinas que tratam de saúde, de economia, de ambiente, porém não é só por isso que não se deve considerar a proteção pela localização. Ademais é interessante compreendê-la como uma exceção, como por exemplo, nos casos em que se exigia a localização física de tratamentos de dados para possibilitar a fiscalização real, pois os dados que não estavam armazenados no território não poderiam ser supervisionados pelas autoridades.

Porém se exige um cuidado para que essa possibilidade de exceção não seja considerada como foi a Diretiva 2006/24/CE da União Europeia que foi invalidada em 2014, pois exigia

1 Monitoram suas decisões e aplicação de medidas legais a partir da situação, considerando caso a caso e conforme a necessidade.

a guarda de metadados mas não o conteúdo das transferências. Assim violando direitos fundamentais, pois não possuía autorização judicial muito menos critérios de atuação de penalização. Ou seja, a descrição do regulamento deve ser minuciosa, apresentando justificativas e meios válidos e em conformidade com o cumprimento dos direitos legais.

A proteção pelo território onde estão sendo armazenados os dados, tem sua contribuição na segurança contra vazamentos, mas com a realidade da maioria dos países que não possuem nível considerado de soberania digital não seria eficaz. Dadas as possibilidades frente ao papel da *Data Localization* e a necessidade urgente de proteção de dados pessoais, o último capítulo apresenta algumas possibilidades e destaca o que seria mais adequado para a preocupação de informações relacionadas a saúde.

Extensão da jurisdição e padrões de segurança como solução efetiva

Quando se fala em solução efetiva cabe destacar que essa efetividade diz sobre as observações feitas e também sobre os regulamentos analisados, não se trata de uma resposta definitiva, mas sim o mais adequado possível com os institutos existentes atualmente.

A resposta mais apropriada por hora, é de que a proteção por localização, mantendo os dados armazenados no Brasil, não seria o mais eficaz, até porque não existe recurso tecnológico, humano e econônico para isso, mas estender a jurisdição da lei brasileira (extraterritorialidade) e impor padrões técnicos rigorosos, com governança e medidas técnicas.

Extraterritorialidade

Para poder compreender a possibilidade da extensão da jurisdição da lei do Brasil, é imprescindível entender o que a LGPD diz sobre a territorialidade, isto é, sobre o tratamento de dados coletados no país, ainda mais, a abrangência da aplicação da lei com base na conexão da atividade de tratamento com o território brasileiro ou com indivíduos nele localizados.

A própria aplicação da Lei de Dados é regida pela extraterritorialidade, e age sobre todas a operações de tratamento de dados coletados de pessoas naturais ou jurídicas, de direito público ou privado, independentemente de onde estejam situados, mesmo que fora do país, ou onde estão localizadas as empresas, desde que cumpram com os requisitos específicos de conexão com o Brasil.

Conforme dispõem o artigo 3° da LGPD:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de

> indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional (Brasil, 2018).

Como disserta o artigo os critérios que estabelecem a territorialidade para a aplicação da LGPD referente as operações realizadas em território nacional, também quando os bens ou serviços oferecidos são realizados no país, ou seja, empresas estrangeiras que ofertam produtos para brasileiros, mesmo que não possuem sede aqui devem se comprometer com a lei. Ainda quando os indivíduos que adquiriram bens ou serviços residam no Brasil, mesmo que estrangeiros, e quando a coleta dos dados tenha sido realizada em solo brasileiro, lembrando que é considerado o momento cujo titular forneceu a informação (Brasil, 2018).

Considerando a esfera da saúde, para a proteção de vazamento dos dados se nota o uso de algumas normas oriundas da legislação e de Códigos de Ética, até mesmo na utilização de dados na investigação médica e nas práticas clínicas e nas ofertas de mercado (Molinaro; Sarlet, 2019, p. 187). Por tal entendimento é possível dizer que a territorialidade na LGPD é expansiva, busca proteger o dado e o titular que está no Brasil, estendendo a jurisdição da lei brasileira a agentes de tratamento globais que interagem com o mercado ou com cidadãos brasileiros, desencadeando de certa maneira a extraterritorialidade.

Governança e medidas técnicas

Em conjunto com a o fluxo transfronteiriço de dados e a extraterritorialidade e considerando a necessidade de uma adequação de segurança para a garantia da privacidade dos usuários se fala também em governança e medidas técnicas previstas legalmente e que são implementadas de acordo com a situação concreta.

No artigo 46, a LGPD, está manifesto:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Assim, a proteção real que também contempla previsões de Resoluções da Anvisa e do Ministério da Saúde, vem a partir de medidas administrativas como criptografia, anonimização e pseudonimização para garantir a segurança para o dado em si, e não somente para o servidor onde ele se encontra para o tratamento final (Filho; Zaganelli, 2022, p. 225).

É indeclinável enfatizar que tendo em vista que o setor da saúde, que constantemente é suscetível a ataques por carregar considerável número de informações, também se propõem a utilizar como precaução a realização e o devido reconhecimento dos Relatórios de Impacto à Proteção de Dados (RIPD). Que ao versar sobre dados de alto risco, como os de saúde, forma uma investigação mais específica sobre possíveis riscos para então ir para o processamento.

Tais relatórios são documentos de competência dos controladores, previsto na lei nacional e que descrevem todos os processos realizados com os dados pessoais, que podem gerar qualquer tipo de perigo a proteção as liberdades e direitos civis ou que contribuam na mitigação de danos (Filho; Zaganelli, 2022, p. 226). Servem para orientar o modo de operação e para constar em informativos de governança vinculados a ANPD (Agência Nacional de Proteção de Dados) no auxílio no desenvolvimento de padrões, metodologias de aplicação e observância dos princípios norteadores contemplados na própria LGPD.

Ainda como medida de adequação de segurança no que tange a relação com a saúde, vale ressalvar a autodeterminação através do uso do Consentimento Livre e Informado, que mesmo quando prestados diretamente, a concessão do uso é para processos específicos e definidos, mesmo que utilizados em *Big Datas* (Guidi, 2021, p. 101). Isto significa, que mesmo em concordância, deve ser cumprida a finalidade pela qual o dado foi informado, concebendo ainda a responsabilidade e o comprometimento dos profissionais envolvidos, desde a coleta até a exclusão dos dados pessoais (Caldeira; Sarlet, 2019, p. 14).

Considerações finais

A *Data Localization* é uma medida de segurança, porém apresenta limitação, principalmente no que diz respeito aos dados sobre a saúde, já que estes dependem muito do fluxo que ocorrem entre entidades e muitas vezes fora das fronteiras nacionais, diferente da necessidade de precisar manter os dados armazenados no próprio território que faz a fiscalização. Para conseguir uma proteção efetiva deve haver uma combinação de medidas de segurança.

A eficácia da proteção de dados na era digital não reside no confinamento geográfico dos dados, mas na capacidade da legislação nacional de alcançar o tratamento de dados onde quer que ele ocorra, desde que haja conexão com o território ou os cidadãos do país.

A Lei 13.709/2018 adota um critério de aplicação que independe da localização física dos dados ou da sede da empresa, incide sobre qualquer operação de tratamento realizada no território nacional, ou que tenha por objetivo a oferta de bens ou serviços no Brasil, ou ainda quando os dados objeto de tratamento tenham sido coletados aqui (Davariz; Obregon, 2019).

Sobre o modelo, inspirado no regulamento europeu, se estabelece que a proteção jurídica acompanha o dado. O GDPR, por exemplo, aplica-se ao tratamento de dados de titulares que se encontrem na União Europeia, mesmo que o controlador ou operador não esteja estabelecido na União, desde que as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares ou com o controle do seu comportamento (Davariz; Obregon, 2019). A aplicação extraterritorial visa evitar que empresas transfiram suas operações para países com leis fracas, como paraísos de dados, apenas para fugir das obrigações legais. Historicamente, a pressão para criar regras supranacionais ou extraterritoriais surgiu justamente para evitar que fluxos de dados fossem usados para contornar legislações nacionais mais estritas.

Em vez de proibir a saída do dado, por uma localização forçada, as fontes indicam que o sistema moderno foca no fluxo livre com confiança. Isso é operacionalizado através de mecanismos que permitem a transferência internacional apenas para destinos que ofereçam garantias de proteção equivalentes.

A transferência é permitida para países que proporcionem um grau de proteção de dados pessoais adequado ao previsto na lei de origem. Na União Europeia, a Comissão pode reconhecer um país terceiro como adequado (Adequacy Decision), permitindo o livre fluxo (Rodrigues; Gunther; Comar, 2020). No Brasil, a LGPD também prevê que a transferência é permitida para países que proporcionem grau de proteção compatível, porém ainda não definido pela ANPD.

Na ausência de uma decisão de adequação do país, os agentes de tratamento podem utilizar cláusulas contratuais específicas, que precisam ser aprovadas pela autoridade nacional e que obrigam o importador dos dados a respeitar padrões de segurança e direitos dos titulares (Guidi, 2021). No entanto, é importante notar que essas cláusulas não são um cheque em branco após decisões judiciais europeias, entende-se que as cláusulas só são válidas se, na prática, o país de destino permitir o cumprimento dessas garantias.

A simples existência de acordos não garante proteção se a lei do país de destino permitir vigilância excessiva, isso pode ferir direitos fundamentais, permitindo acesso aos dados de forma incompatível com as garantias legais demonstrando que o foco deve ser a análise rigorosa da legislação do destino, e não apenas a localização do servidor.

A proteção efetiva do dado de saúde depende mais de como ele é guardado e gerido do que onde ele está armazenado. As fontes enfatizam a necessidade de medidas que tornem o dado ininteligível para terceiros não autorizados e processos que garantam a responsabilidade das instituições. A proteção de dados deve ser incorporada desde a concepção do produto ou serviço e ser a configuração padrão (Costa; Lima; Gonçalves, 2023). Isso significa dizer que sistemas de saúde devem ser arquitetados para coletar o mínimo de dados necessários e protegê-los nativamente, sem exigir que o usuário configure a segurança. A configuração padrão deve ser a mais restritiva para proteger a privacidade.

Para proteger dados sensíveis de saúde, é essencial adotar tecnologias como a criptografia, que torna o dado ilegível sem a chave de acesso, e a anonimização, que desvincula o dado do titular. Que, diante do grande volume de dados na saúde, em *Big Data*, medidas robustas de segurança são cruciais para evitar vazamentos que levem à discriminação. Não basta ter segurança técnica, se faz preciso governança. Isso inclui a demonstração ativa do cumprimento da lei. As instituições devem manter inventários de dados, documentar decisões de segurança e realizar Relatórios de Impacto à Proteção de Dados para tratamentos de alto risco, como é o caso de dados genéticos ou de saúde em larga escala.

A segurança depende também de fatores humanos, precisa se criar uma cultura de privacidade nas instituições de saúde cada vez maior e mais preocupada, com capacitação contínua dos profissionais para evitar falhas humanas que levem à exposição de prontuários e dados

sensíveis, mesmo que a LGPD disponha sobre a existência de redes fechadas e procedimentos realizados em espaço controlado e seguro. É imprescindível a efetividade da proteção, mesmo que para isso se utiliza um conjunto de medidas de adequação de segurança.

Referências

CALDEIRA, Cristina; SARLET, Gabrielle Bezerra Sales. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. **Civilistica.com**, a. 8, n.1, 2019.

COSTA, Danilo da; LIMA, Isadora Souza; GONÇALVES, Jonas Rodrigo. A lei geral de proteção de dados pessoas nos serviços de saúde públicia. **Revista Processus de Políticas Públicas e Desenvolvimento Social**, ano 5, n. 10, jul/dez, 2023.

DAVARIZ, Caroline Aparecida Vianna; OBREGON, Marcelo Fernando Quiroga. A proteção dos dasdos pessoais na internet enquanto direito humano à privacidade de tutela internacional. **Revista Derecho y Cambio Social**¸n. 58, out/dez, 2019.

FILHO, Douglas Luis Binda; ZABANELLI, Margareth Vestis. A lei geral de proteção de dados e suas implicações na saúde: as avaliações de impacto no tratamento de dados no âmbito clínico-hospitalar. **Revista Bioética y Derecho**. Ed. 54, 2022. P. 215-232.

GUIDI, Guilherme Berti de Campos. **Proteção de dados pessoais:** a composição de sistemas pelo direito internacional. Tese de doutorado, da Universidade de São Paulo, Faculdade de Direito, São Paulo, 2021.

MOLINARO, Carlos Alberto; SARLET, Gabrielle Bezerra Sales. Questões tecnológicas, éticas e normativas da proteção de dados pessoais na área da saúde em um contexto de *Big Data*. **Direitos Fundamentais & Justiça**, ano 13, n. 41, jul/dez. 2019. Belo Horizonte, p. 183-212.

RODRIGUES, Luciano Ehlke; GUNTHER, Luiz Eduardo; COMAR, Rodrigo Thomazinho. A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade: os limites da intervenção do Estado. **Brazilian jornal of Law & International Relations/Relações Internacionais no Mundo**¸vol. 2, 2020. Disponível em: https://openurl.ebsco.com/EPDB%3Agcd%3A12%3A25062140/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A143597203&crl=c&link_origin=scholar.google.com. Acessado em 6 jan. 2026.

SANTOS, Diego Costa Barbosa; MOURA, Gabriel Aparecido Salvador de; LIMA, Jordão Horácio da Silva. E-Saúde e os desafios à proteção da privacidade no Brasil: uma análise de gestão de dados pessoais de pacientes no âmbito da lei n° 13.709/2018. **Revista Raízes no Direito**, Faculdade Evangélica Raízes, Anápolis, v. 13, n. 2, ago/dez 2024, p. 95-119.

Declaração

Durante a elaboração deste artigo científico, a ferramenta de pesquisa NotebookLM com Inteligência Artificial do Google foi utilizada como suporte de revisão gramática, sugestão de aprimoramento textual e tradução para língua estrangeira. O conteúdo gerado pela IA foi subsequentemente revisado e validado criticamente pela autora, que assume responsabilidade pela integridade e precisão das informações apresentadas.