ISSN:2594-6153

Experiência do Paciente ou Vigilância? Os Limites Jurídicos da Coleta e Utilização de Dados na Saúde Digital

Beatriz Scandolera, Luciana Rodrigues Pimentel, Patrícia Cristina Vasques de Souza Gorisch

Universidade Santa Cecília (UNISANTA), Santos-SP, Brasil

E-mail: scandolera.adv@gmail.com

Resumo: A transformação digital da saúde amplia a coleta e utilização de dados pessoais para personalizar serviços e aprimorar a experiência do paciente. Entretanto, o uso crescente dessas informações pode ultrapassar a finalidade assistencial e produzir formas de monitoramento e perfilização. Este estudo analisa os limites jurídicos dessa utilização, com enfoque na proteção de dados pessoais de saúde. A pesquisa é qualitativa, descritiva e analítica, baseada em revisão bibliográfica, normativa e documental. Os resultados indicam que a personalização não legitima coleta ou utilização ilimitada de dados, devendo o tratamento observar finalidade, necessidade, transparência, segurança e proteção dos direitos fundamentais do titular.
Palavras-chave: Saúde Digital; Proteção de Dados; LGPD; Dados Sensíveis; Privacidade.

Patient Experience or Surveillance? Legal Limits on Data Collection and Use in Digital Health

Abstract: The digital transformation of healthcare expands the collection and use of personal data to personalize services and improve patient experience. However, the increasing use of such information may exceed healthcare purposes and create forms of monitoring and profiling. This study analyzes the legal limits of such practices, focusing on the protection of health data. The research is qualitative, descriptive, and analytical, based on bibliographic, normative, and documentary review. The findings indicate that personalization does not justify unlimited data collection or use, which must comply with purpose limitation, necessity, transparency, security, and protection of the data subject's fundamental rights.
Keywords: Digital Health; Data Protection; LGPD; Sensitive Data; Privacy.

Introdução

A transformação digital vem modificando a prestação dos serviços de saúde, ampliando o uso de prontuários eletrônicos, aplicativos, plataformas digitais, telemedicina e sistemas destinados à personalização da experiência do paciente. Entretanto, a utilização dessas tecnologias depende da coleta e do tratamento de informações relacionadas aos pacientes e, nesse diapasão, a Lei Geral de Proteção de Dados Pessoais (LGPD) classifica os dados referentes à saúde como dados pessoais sensíveis e estabelece regras específicas para seu tratamento [1].

O Ministério da Saúde também reconhece a proteção de dados como premissa da transformação digital do Sistema Único de Saúde (SUS), especialmente diante da crescente

integração e compartilhamento de informações [2]. Assim, o problema surge quando a coleta de dados, inicialmente justificada pela melhoria da assistência ou da experiência do paciente, passa a alcançar finalidades distintas, como perfilização, personalização comercial, análise comportamental ou compartilhamento de informações, e a própria Autoridade Nacional de Proteção de Dados (ANPD) mantém, em sua Agenda Regulatória 2025-2026, os dados pessoais sensíveis de saúde como tema prioritário, destacando especialmente os limites do compartilhamento com finalidade econômica [3].

Nesse contexto, a digitalização produz uma tensão entre dois interesses igualmente relevantes: de um lado, a utilização de dados pode melhorar a continuidade, eficiência e personalização do cuidado; de outro, a ampliação da capacidade de coleta, cruzamento e utilização das informações pode comprometer a privacidade e a autodeterminação informativa do paciente. Diante disso, o presente artigo busca responder ao seguinte problema de pesquisa: em que medida a coleta e utilização de dados pessoais de saúde para aprimorar a experiência do paciente pode ultrapassar a finalidade assistencial e configurar formas juridicamente problemáticas de monitoramento e perfilização?

Objetivos

O presente estudo tem como objetivo analisar os limites jurídicos da coleta e utilização de dados pessoais de saúde em ambientes digitais, especialmente quando empregadas sob a justificativa de aprimoramento da experiência do paciente. Busca-se identificar os limites impostos pela LGPD e pelos princípios da proteção de dados, bem como, distinguir práticas legítimas de personalização da assistência de formas excessivas de monitoramento, perfilização ou utilização econômica das informações.

Material e Métodos

Trata-se de pesquisa qualitativa, descritiva e analítica, fundamentada em revisão bibliográfica, normativa e documental. Foram analisados a Constituição Federal, a Lei nº 13.709/2018 (LGPD), normas e documentos da Autoridade Nacional de Proteção de Dados e do Ministério da Saúde, além de literatura científica relacionada à proteção de dados e à transformação digital da saúde.

Isso posto, a análise busca confrontar as possibilidades de utilização tecnológica dos dados com os princípios de finalidade, adequação, necessidade, transparência, segurança e proteção dos direitos fundamentais dos titulares [1-4].

Resultados

Os resultados demonstram que os dados de saúde recebem proteção jurídica reforçada, pois a LGPD os classifica como dados pessoais sensíveis e estabelece hipóteses específicas para seu tratamento, inclusive para a tutela da saúde, além de impor princípios que devem orientar todas as operações realizadas com dados pessoais [1]. A ANPD também reconhece que o tratamento de dados de saúde apresenta peculiaridades próprias e permanece entre os temas prioritários de sua agenda regulatória, especialmente diante da possibilidade de utilização econômica dessas informações [3].

No campo institucional, o Ministério da Saúde reconhece a proteção de dados como elemento fundamental da transformação digital do SUS, especialmente diante da ampliação da interoperabilidade e do compartilhamento de informações por meio de sistemas digitais [2]. Além disso, a Rede Nacional de Dados em Saúde e as plataformas SUS Digital, regulamentadas pelo Decreto nº 12.560/2025, reforçam essa tendência de integração dos dados de saúde [4].

A pesquisa também identificou que o conceito de tratamento previsto na LGPD é amplo, abrangendo coleta, utilização, acesso, armazenamento, avaliação, controle, comunicação e transferência de informações [1] e, dessa forma, o risco jurídico não está restrito ao momento da coleta, mas alcança todo o ciclo de vida do dado.

Verificou-se, ainda, que a personalização da assistência e o monitoramento do paciente não são juridicamente equivalentes, uma vez que o tratamento necessário à continuidade do cuidado pode possuir finalidade assistencial legítima, enquanto a utilização das mesmas informações para perfilização, publicidade ou obtenção de vantagem econômica exige análise específica de compatibilidade com a legislação de proteção de dados.

Discussão

A análise demonstra que a transformação digital da saúde não deve ser compreendida como incompatível com a privacidade. Ao contrário, a utilização adequada dos dados pode contribuir para a continuidade do cuidado, integração dos serviços e personalização da assistência. O problema jurídico surge quando a justificativa genérica de “melhor experiência

do paciente" passa a legitimar uma coleta de informações superior àquela efetivamente necessária para a finalidade pretendida.

A LGPD estabelece que o tratamento deve observar, entre outros, os princípios da finalidade, adequação, necessidade, transparência e segurança [1]. Assim, a coleta de determinada informação para uma finalidade assistencial não significa autorização para sua utilização irrestrita em outras atividades, mas sim que a finalidade declarada deve guardar correspondência com o tratamento efetivamente realizado.

A questão torna-se ainda mais sensível diante da possibilidade de cruzamento de informações. Nesse sentido, dados aparentemente distintos podem, quando associados, permitir inferências sobre hábitos, condições clínicas, comportamento ou vulnerabilidades do indivíduo. A ANPD reconhece, inclusive, que dados utilizados para formação de perfil comportamental podem constituir dados pessoais quando vinculados a pessoa identificada ou identificável [1,6].

Nesse cenário, a fronteira entre experiência e vigilância não está na utilização da tecnologia em si, mas na finalidade e na extensão do tratamento, pois um sistema destinado a lembrar consultas ou acompanhar determinado tratamento possui finalidade distinta de uma ferramenta que utiliza o histórico de saúde para construir perfis comportamentais ou direcionar estratégias comerciais.

A questão também possui relevância econômica, haja vista que a própria Agenda Regulatória da ANPD para 2025-2026 estabelece como tema prioritário os dados pessoais sensíveis de saúde, destacando a possibilidade de regulamentação ou restrição ao compartilhamento desses dados entre controladores com objetivo de obtenção de vantagem econômica [3]. Assim, o debate ultrapassa a proteção individual da privacidade e alcança a governança dos dados no mercado de saúde.

Em 2026, a ANPD também instaurou processo de sanção relacionado a falhas na proteção de dados sensíveis de aproximadamente 500 mil pacientes após incidente de segurança envolvendo organização responsável pela gestão de unidades públicas de saúde [5]. O caso demonstra que a digitalização não produz apenas riscos abstratos: a concentração de grandes volumes de informações de saúde também amplia as consequências potenciais de falhas de segurança e governança.

Desse modo, a experiência do paciente não pode ser utilizada como justificativa genérica para ampliar indefinidamente a coleta e utilização de seus dados. A inovação em saúde deve ser acompanhada por mecanismos de governança capazes de demonstrar quais

informações são coletadas, para qual finalidade, por quanto tempo, com quem são compartilhadas e quais medidas protegem o titular contra usos incompatíveis com a finalidade originalmente estabelecida.

Conclusões

A transformação digital pode aprimorar a experiência do paciente, mas não afasta os limites jurídicos impostos à coleta e utilização de dados pessoais de saúde. A análise demonstra que a personalização da assistência deve estar vinculada a finalidade legítima, necessidade, transparência, segurança e respeito aos direitos fundamentais do titular. A utilização de dados para perfilização, monitoramento ou finalidades econômicas exige controle jurídico específico, especialmente diante da natureza sensível das informações de saúde. Conclui-se que o desafio contemporâneo não consiste em escolher entre inovação e privacidade, mas em estabelecer limites capazes de permitir a inovação sem transformar o paciente em objeto permanente de monitoramento.

Referências

1. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm . Acesso em: 19 set. 2026.
2. BRASIL. Ministério da Saúde. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Ministério da Saúde, [s. d.]. Disponível em: https://www.gov.br/saude/pt-br/acesso-a-informacao/lgpd . Acesso em: 14 set. 2026.
3. BRASIL. Autoridade Nacional de Proteção de Dados. Agenda Regulatória para o biênio 2025-2026. Brasília, DF: ANPD, 2024. Atualizada em 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/regulacao/agenda-regulatoria-1/agenda-regulatoria-2025-2026 . Acesso em: 19 set. 2026.
4. BRASIL. Decreto nº 12.560, de 23 de julho de 2025. Dispõe sobre a Rede Nacional de Dados em Saúde e sobre as Plataformas SUS Digital e regulamenta o art. 47 e o art. 47-A, caput, § 1º e § 2º, da Lei nº 8.080, de 19 de setembro de 1990. Brasília, DF: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/d12560.htm . Acesso em: 19 set. 2026.
5. BRASIL. Autoridade Nacional de Proteção de Dados. ANPD instaura processo de sanção contra OS por falha na proteção de dados de 500 mil pacientes. Brasília, DF: ANPD, 2026. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-instaura-processo-de-sancao-contra-organizacao-social-por-falha-na-protecao-de-dados-de-500-mil-pacientes-de-unidades-publicas-de-saude . Acesso em: 19 set. 2026.
6. BRASIL. Autoridade Nacional de Proteção de Dados. Perguntas frequentes: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: ANPD, [s. d.]. Disponível em:

https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes . Acesso em: 14 set. 2026.