

INTRODUÇÃO AO DIREITO MÉDICO DIGITAL: DESAFIOS JURÍDICOS NA ERA DA SAÚDE CONECTADA

Thelio Queiroz Farias

Advogado, Presidente da Academia de Letras de Campina Grande e
membro da Academia Paraibana de Letras

Ricardo Alves de Souto

Advogado, Escritor e membro da Academia de Letras de Areia

“A tecnologia move o mundo.” Steve Jobs (1955-2011)

O advento da medicina digital representa uma das mais disruptivas transformações da contemporaneidade, com implicações jurídicas ainda em processo de consolidação. O Direito Médico Digital emerge como resposta normativa, ética e técnica à crescente digitalização e novas tecnologias na saúde e à complexidade das relações entre pacientes, médicos, instituições hospitalares e plataformas tecnológicas. Este artigo inaugura academicamente o campo do Direito Médico Digital, introduzindo seus conceitos, fundamentos e desafios.

Fundamentos Teóricos e Normativos do Direito Médico Digital

1.1 O Direito Digital e sua Interseção com a Medicina

O Direito Digital, ramo jurídico voltado à regulação das relações mediadas por tecnologias digitais, encontra na medicina uma área sensível e de alto risco. A presença de dados sensíveis, o sigilo profissional, a responsabilização em ambiente médico-digital e o uso de plataformas on-line para atendimento de pacientes exigem arcabouço jurídico robusto e adaptado às novas realidades como telemedicina, blockchain, perícias médico-digitais, prontuários eletrônicos e diversas outras.

1.2 LGPD, Proteção de Dados Médicos e Direito Médico Digital

A Lei nº 13.709/2018 (LGPD) ocupa papel central no Direito Médico Digital. Dados médicos são classificados como "dados pessoais sensíveis" (art. 5º, II, LGPD), exigindo tratamentos rigorosos de segurança, consentimento e transparência. A quebra do sigilo médico, mesmo acidental, pode ensejar responsabilização civil, administrativa e, em casos extremos, penal. A proteção de tais dados constitui não apenas dever legal, mas imperativo ético-constitucional.

1.3. Telemedicina e Riscos Digitais

A **Telemedicina** pode ser definida como a prática médica mediada por **tecnologias digitais de informação, automação e comunicação**, que possibilitam o atendimento clínico, diagnóstico, monitoramento e até intervenções médicas a distância. Essa modalidade de cuidado em saúde, ao mesmo tempo em que amplia o acesso e a eficiência dos serviços, expõe pacientes, profissionais e instituições a **riscos digitais**, notadamente relacionados à segurança cibernética, à proteção de dados sensíveis e à confiabilidade das plataformas tecnológicas empregadas.

1.3.1. Avanços Normativos e Limitações Estruturais

A telemedicina, inicialmente prevista de forma restritiva pelo Conselho Federal de Medicina (CFM), ganhou maior impulso normativo com a edição da **Resolução CFM nº 2.314/2022**, que regulamentou de modo abrangente o atendimento médico remoto no Brasil. Tal dispositivo normativo autoriza práticas como consultas, monitoramento, diagnósticos e até cirurgias assistidas, ampliando o alcance do ato médico. Entretanto, a resolução ainda apresenta limitações, sobretudo no que concerne à segurança cibernética, à padronização técnica e à clareza quanto às responsabilidades jurídicas em casos de falhas decorrentes da digitalização. A regulamentação atual, embora necessária, permanece insuficiente para acompanhar a velocidade de transformação das tecnologias empregadas em saúde, deixando lacunas normativas que expõem tanto os pacientes quanto os profissionais de saúde a riscos consideráveis.

1.3.2 - A Complexidade dos Riscos cibernéticos na Saúde

A digitalização, automação e nanotecnologia na prática médica amplia, inevitavelmente, a superfície de exposição a ameaças cibernéticas. Riscos como ataques de *ransomware* (uma espécie de *software* malicioso), que sequestram dados hospitalares e paralisam serviços essenciais, já foram registrados em diversos países, inclusive no Brasil. O vazamento de prontuários eletrônicos, contendo informações sensíveis como diagnósticos, prescrições e histórico clínico, representa grave ameaça não apenas à privacidade do paciente, mas também à sua dignidade e integridade moral.

A interseção entre vulnerabilidades técnicas e fragilidades normativas gera um ambiente propício à ocorrência de ilícitos, o que demanda maior atenção do legislador e das autoridades regulatórias. Além disso, as plataformas de telemedicina, muitas vezes terceirizadas, utilizam servidores em nuvem que podem estar localizados em outros países, levantando questões de jurisdição, transferência internacional de dados e cooperação jurídica internacional.

1.3.3. Responsabilidade Civil, Ética e Penal na Telemedicina

A prática da telemedicina não elimina os deveres éticos e legais inerentes ao exercício da medicina. Pelo contrário, introduz novos deveres relacionados à segurança da informação e à governança digital. Em caso de erro médico decorrente de falha tecnológica — como perda de conexão, interpretação inadequada de exames digitais ou uso de softwares de diagnóstico com vieses algorítmicos —, a responsabilização pode ser discutida em múltiplas esferas:

- ✓ **Civil:** indenização por danos morais e materiais ao paciente;
- ✓ **Administrativa:** responsabilização perante os conselhos de classe;
- ✓ **Penal:** possibilidade de imputação de crimes de lesão corporal, crimes contra a honra, ou até de violação de sigilo profissional (art. 154 do Código Penal).

Destarte, a atuação médica digitalizada não exime o profissional de seus deveres éticos e legais. Erros de diagnóstico causados por falhas na rede, violação de dados, ausência de consentimento formal e falta de protocolos digitais de segurança podem ensejar as citadas responsabilidades.

A legislação federal precisa disciplinar normas que regulem um compliance médico-digital autônomo, com governança de dados e protocolos claros, bem como a responsabilidade civil de todos os sujeitos que integram um dos polos da relação Médico-Paciente-Responsável pela segurança e tratamento de dados.

A doutrina contemporânea, como analisada na obra-base, sugere que se trata de responsabilidade solidária, envolvendo não apenas o médico, mas também hospitais, clínicas, desenvolvedores de softwares e fornecedores de infraestrutura tecnológica. Esse modelo, inspirado na lógica da responsabilidade solidária, inclusive objetiva, amparada no Código de Defesa do Consumidor, ganha força diante da complexidade das cadeias digitais em saúde.

2 - Avanços e Fragilidades da Resolução CFM nº 2.314/2022

A **Resolução CFM nº 2.314/2022** constitui marco relevante ao conferir legitimidade normativa administrativa à telemedicina, ampliando o alcance do ato médico no Brasil. Contudo, sua disciplina permanece insuficiente no que se refere à necessidade de leis federais que tratem dos temas em comento. Essa lei federal viria para regular a **cibersegurança das plataformas digitais utilizadas na saúde**, pois estabeleceria protocolos técnicos mínimos, impondo padrões obrigatórios de proteção de dados. Tal lacuna normativa fragiliza a relação médico-paciente no ambiente virtual e cria terreno fértil para a atuação de **agentes maliciosos**, como *hackers* e grupos especializados em **ransomware**, capazes de sequestrar informações clínicas, paralisar sistemas hospitalares e gerar consequências éticas, jurídicas e econômicas de larga escala.

3 - Entre a Ética e o Direito

A digitalização da saúde trouxe inegáveis benefícios, como maior celeridade no atendimento, ampliação do acesso a serviços médicos e integração de dados clínicos em tempo real. Todavia, essa modernização também inaugurou um campo de vulnerabilidades tecnológicas que desafiam não apenas a **ética médica**, mas também o próprio **Direito Penal contemporâneo**.

Do ponto de vista **ético**, a confidencialidade do paciente, pilar histórico da prática médica, encontra-se sob constante ameaça diante da possibilidade de invasões em prontuários eletrônicos, vazamentos de informações sensíveis e manipulação indevida de dados genéticos. O princípio do sigilo profissional, tradicionalmente vinculado à relação médico-paciente, precisa hoje dialogar com a **ética cibernética** exigindo protocolos de segurança digital, responsabilidade institucional e compromisso técnico dos profissionais de saúde.

No âmbito **jurídico-penal**, os incidentes de cibersegurança em saúde podem configurar crimes previstos na legislação brasileira, como a invasão de dispositivo informático (art. 154-A do Código Penal), a interrupção de serviços essenciais (art. 266 do CP) e os delitos de fraude eletrônica, recentemente agravados pela Lei nº 14.155/2021. Além disso, ataques como o **ransomware**, capazes de paralisar hospitais inteiros e colocar vidas em risco, não se limitam a lesões patrimoniais, mas podem ensejar **responsabilidade penal qualificada** pela exposição de pacientes a perigo concreto.

3.1 - A Necessidade de Normas de Cibersegurança nas Relações Médico-Paciente

A consolidação da telemedicina e do uso intensivo de tecnologias digitais na área da saúde exige uma reflexão profunda sobre a insuficiência das normas atualmente vigentes. Embora a **Resolução CFM nº 2.314/2022** represente avanço significativo na regulamentação do atendimento médico a distância, verifica-se a ausência de disposições detalhadas acerca da **cibersegurança médica**, aspecto fundamental para a proteção de pacientes e profissionais.

A simples previsão em forma de resolução não se traduz, na prática, em mecanismos de defesa adequados contra-ataques cibernéticos sofisticados, como **ransomware**, **phishing** (tipos de ciberataque feitos por criminosos disfarçados de pessoas ou entidade confiáveis) e **engenharia social**. A vulnerabilidade das plataformas digitais utilizadas por hospitais, clínicas e consultórios cria riscos de proporções éticas, jurídicas e sociais, colocando em xeque a própria dignidade da pessoa humana ao expor dados íntimos e fragilizar a confiança na relação médico-paciente.

Diante desse cenário, impõe-se a criação de **normas específicas e detalhadas** que disciplinem a cibersegurança em saúde. Essas normas devem:

1. **Estabelecer protocolos obrigatórios de segurança digital:** autenticação multifatorial, criptografia avançada e monitoramento contínuo das plataformas médicas.
2. **Criar padrões nacionais de interoperabilidade e segurança** em prontuários eletrônicos e sistemas de teleatendimento, reduzindo vulnerabilidades técnicas.
3. **Exigir planos de resposta a incidentes cibernéticos** que incluam notificação compulsória de autoridades competentes e comunicação transparente aos pacientes afetados.
4. **Determinar responsabilidades compartilhadas** entre médicos, instituições hospitalares e fornecedores de tecnologia, evitando a concentração indevida de ônus em apenas um agente.
5. **Incluir auditorias regulares de conformidade digital**, de forma semelhante ao que já ocorre em setores financeiros e bancários.

Nesse contexto, ganha relevo a implementação de um **compliance médico-digital**, entendido como conjunto estruturado de políticas, procedimentos e controles internos destinados à **prevenção, detecção e resposta a riscos cibernéticos**. Tal sistema, além de atender às exigências da LGPD e do Marco Civil da Internet, deve ser integrado à lógica do **Direito Médico-Digital**, prevenindo ilícitos e assegurando que a atuação médica digital respeite os princípios de segurança cibernética do paciente.

Conclusão

O exame das transformações introduzidas pela digitalização da saúde demonstra que o **Direito Médico Digital** emerge como campo autônomo, indispensável à compreensão e à regulação das novas relações estabelecidas entre médicos, pacientes, instituições de saúde e plataformas tecnológicas. A intensificação da telemedicina, a expansão dos prontuários eletrônicos e o uso de tecnologias de automação e comunicação expõem, de um lado, o potencial inovador da medicina digital, mas, de outro, revelam vulnerabilidades éticas, jurídicas e técnicas que ainda carecem de tratamento normativo mais sólido e abrangente.

Constatou-se que, embora a **Resolução CFM nº 2.314/2022** represente avanço normativo relevante, sua disciplina é insuficiente diante da complexidade dos riscos cibernéticos contemporâneos.

Assim, conclui-se que o Direito Médico Digital não é apenas uma adaptação pontual do Direito Médico tradicional, mas sim um **novo paradigma jurídico**, vocacionado a enfrentar os desafios da era da saúde conectada. A sua consolidação, além de contribuir para a efetividade dos direitos fundamentais, também representa passo decisivo para assegurar que a inovação tecnológica em saúde se desenvolva de modo ético, seguro e em consonância com os valores constitucionais da dignidade da pessoa humana e da proteção integral do paciente.

Referências:

FARIAS, Thélío Queiroz; SOUTO; e Ricardo Alves de. **Direito digital**. 1. ed. Leme, SP: EDIJUR, 2024. p. 288.

. HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital Transformação digital Desafios para o Direito**. Ed. Forense, 2022.

. MUCELIN, Guilherme (organizador). **Direito Digital Direito Privado e Internet**. Editora FOCO, 2024.

. ROBERTO, Wilson Furtado; e ZAMORA, Guilherme Manuel. **Dicionário de Direito Digital**. Ed. Mizuno, 2025.

. VECCHIO, Fabrizio Bon; SOUTO, Ricardo; e FARIAS, Thélío. **Direito médico digital**. Leme, SP: AM2, 2025. p 252.

. VECCHIO, Fabrizio Bon; SOUTO, Ricardo; FARIAS, Thélío Queiroz; **Crimes cibernéticos: entre a prevenção e a conformidade**. 1. ed. Porto Alegre, RS: Instituto Ibero-americano de Compliance, 2025.