

## Visão do Direito



**Deana Weikersheimer**  
Advogada especialista  
em direito digital e sócia  
do WCW Advogados  
Associados



**Marco Tulio Castro**  
Advogado especialista  
em direito digital e sócio  
do WCW Advogados  
Associados



**Felipe Maranhão**  
Advogado especialista  
em crimes cibernéticos.  
Sócio do Tórtima, Galvão &  
Maranhão Advogados

# Riscos digitais e inteligência artificial: a nova fronteira da proteção de dados

**E**m 2024, mais de 84 milhões de contas de usuários brasileiros sofreram violações de segurança, colocando o país na sétima posição mundial em incidentes desse tipo. Vivemos em uma era de transformação digital, em que empresas de todos os portes passaram a depender intensamente das tecnologias da informação, ampliando a exposição a riscos cibernéticos.

Apesar de promover eficiência e inovação, o ambiente digital impõe desafios que, se não forem devidamente enfrentados, comprometem a reputação e a sustentabilidade das organizações. Mais do que investir em ferramentas tecnológicas, é preciso cultivar uma cultura de prevenção e estratégia na gestão de riscos.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº13.709/2018) estabeleceu regras claras para o tratamento de dados pessoais. Negócios de diversos setores devem implementar medidas de segurança, políticas internas e práticas transparentes no uso das informações de seus clientes, colaboradores e parceiros.

A atuação crescente da Autoridade Nacional de Proteção de Dados (ANPD), com a edição de novas diretrizes e a aplicação de sanções

administrativas, demonstra que a fiscalização é uma realidade concreta e em expansão. Descumprir a LGPD pode resultar em sanções pesadas, como multas de até 2% do faturamento da empresa, bloqueio ou eliminação de bancos de dados e proibição do exercício de determinadas atividades.

Os prejuízos, porém, vão além do financeiro. Empresas que perdem o controle sobre os dados que tratam também perdem a confiança de seus clientes, parceiros comerciais e investidores. Casos de vazamento de dados se tornaram frequentes nas manchetes, provando que nem mesmo grandes organizações estão imunes, e a ausência de mecanismos robustos de controle pode gerar consequências severas.

A proliferação da inteligência artificial (IA) também acrescenta uma camada extra de riscos. Ferramentas baseadas em IA otimizam processos, personalizam experiências e apoiam a tomada de decisões. Entretanto, seu uso sem critérios claros pode gerar discriminação algorítmica, decisões pouco transparentes e violações de privacidade. Uma consequência disso é o atual aumento expressivo de ataques de phishing impulsionados por IA generativa, gerando golpes altamente personalizados, difíceis

de detectar e, muitas vezes, focados em equipes de RH, finanças e executivos.

Não se pode deixar de mencionar os chamados deepfakes, ferramentas de clonagem de voz e imagens geradas por IA, que já são utilizados em fraudes corporativas, inclusive em ataques envolvendo sequestro de dados (ransomware). Esses episódios mostram que a IA, se mal gerida, pode representar uma ameaça real à integridade das operações empresariais. A gestão de riscos, nesse contexto, deve considerar não somente a proteção contra incidentes, mas também a análise crítica das tecnologias adotadas.

Ainda assim, se usada com critério, a IA pode ser uma grande aliada na mitigação de riscos. Soluções de monitoramento automatizado, análise preditiva de incidentes e cruzamento de dados para detecção de fraudes são exemplos de aplicações que fortalecem a segurança. Contudo, para trazerem resultados positivos, essas aplicações exigem uma infraestrutura jurídica e ética sólida, com governança de dados, supervisão humana e avaliação contínua dos impactos gerados pelos sistemas inteligentes.

Empresas que priorizam a conformidade com a LGPD e adotam práticas responsáveis no

uso de IA fortalecem sua imagem e constroem relações de confiança. Além disso, facilitam a expansão internacional e protegem seus ativos intangíveis. Para competir em mercados regulados e manter uma boa reputação atualmente, é preciso atender às exigências legais, como o GDPR europeu e a LGPD brasileira.

Cabe aos empresários e gestores adotarem práticas estruturadas de gestão de riscos, envolvendo o mapeamento dos dados tratados, a revisão de contratos com fornecedores de tecnologia, a implementação de políticas de segurança da informação e o treinamento contínuo das equipes. Neste caso, agir preventivamente costuma ser mais eficaz — e menos oneroso — do que remediar os danos após um incidente.

A gestão de riscos no ambiente digital não é apenas uma questão técnica, mas sim uma obrigação legal e um imperativo estratégico. Observar a legislação de proteção de dados e adotar uma abordagem responsável em relação ao uso da inteligência artificial são condições fundamentais para a perenidade dos negócios no século 21. Ignorar essas exigências significa colocar em risco não somente os dados que a empresa detém, mas sua própria existência.

## Visão do Direito



**Deana Weikersheimer,**  
Lucas Rosa Dohmen, advogado especialista em direito à saúde e sócio do Dhomen & Matta Advogados

## Estatuto ainda é insuficiente para enfrentar o principal problema do sistema de saúde

**O**novo Estatuto dos Direitos do Paciente chega com uma proposta relevante: reunir, em um só lugar, diversos direitos que já existiam, mas que, muitas vezes, estavam dispersos em diferentes normas e pouco acessíveis à população.

Entre esses direitos, a lei reforça pontos importantes, como o acesso à informação clara sobre diagnóstico e tratamento (art. 12), o consentimento informado (art. 14), o acesso ao prontuário médico (art. 19) e a participação do paciente nas decisões sobre sua própria saúde (art. 11). Também garante o respeito à privacidade e à confidencialidade das informações (arts. 15 e 16).

Na prática, porém, esses direitos já eram amplamente reconhecidos por outras normas, como o Código de Defesa do Consumidor e as regras éticas da área da saúde. Ou seja, a nova lei

cumprir um papel importante de organização e reforço — mas não representa a mudança estrutural que o sistema precisa.

E é justamente aí que está o ponto mais sensível: se esses direitos já existem há tanto tempo, por que ainda são tão frequentemente desrespeitados?

Sem informação adequada, não há autonomia.

Sem respeito à prescrição do médico assistente, não há acesso real ao tratamento. E sem acesso efetivo, não há dignidade — ainda que ela esteja garantida no papel. Hoje, não são raros os casos em que pacientes precisam recorrer à Justiça para conseguir tratamentos, exames ou medicamentos. E, mesmo quando há decisão judicial favorável, o cumprimento pode ser lento ou incompleto — em alguns casos, com consequências irreversíveis.

A própria lei, ao tratar dos mecanismos de

implementação (art. 23), concentra-se em medidas como divulgação de informações, realização de pesquisas e recebimento de reclamações. Embora importantes, essas iniciativas não criam instrumentos suficientemente eficazes para garantir que os direitos sejam respeitados no dia a dia.

Os impactos desse cenário vão além do paciente individual. Quando um plano de saúde não cumpre sua obrigação, muitas pessoas acabam recorrendo ao Sistema Único de Saúde (SUS) como alternativa. O resultado é um efeito em cadeia: a sobrecarga do sistema público, que passa a absorver demandas que já deveriam estar cobertas pela saúde suplementar.

Não se pode perder de vista que o direito à saúde é um dever do Estado — e, no caso da saúde suplementar, esse dever é compartilhado com as operadoras. No entanto, quando esse modelo falha, o que se observa é uma distorção:

o custo retorna ao sistema público ou recai diretamente sobre o paciente.

Enquanto isso, debates mais estruturais sobre o funcionamento do setor — como a atualização das regras dos planos de saúde e a criação de mecanismos mais eficazes de fiscalização e responsabilização — seguem com tímido avanço no país.

Diante desse cenário, a nova Lei dos Direitos do Paciente deve ser vista como um marco relevante do ponto de vista formal, mas ainda de impacto limitado na prática. Ela reforça direitos, mas não enfrenta, de forma direta, o principal desafio do sistema de saúde: garantir que esses direitos sejam efetivamente cumpridos.

No fim das contas, não basta reconhecer direitos no papel. O verdadeiro avanço acontece quando eles são respeitados na prática — e isso ainda depende de mudanças mais profundas, especialmente no campo da fiscalização, da regulação e da responsabilização.