



A persistente assimetria de dados entre os mercados de Bolsa e Balcão

André Morino (*)

No mercado financeiro brasileiro, vivemos um cenário de importantes avanços regulatórios. Medidas como as Resoluções CVM 175 e CVM 135 trouxeram mudanças importantes, como a exigência de precificação de ativos de balcão e o aumento da transparência dos dados. No entanto, na prática, quando comparamos os mercados de bolsa e balcão, notamos que o acesso às informações ainda acontece de forma assimétrica, o que, considerando a complexidade dos ativos OTC (Over-The-Counter), resulta em um aumento significativo da dificuldade de precificação e, consequentemente, em um maior risco de liquidez para esses papéis.

Para entendermos melhor os impactos dessa realidade e como essa assimetria acontece, podemos destacar três diferenças principais entre bolsa e balcão. A primeira diz respeito à formação dos preços. Na bolsa, há um livro de ordens e um spread de compra e venda (bid-ask spread) visível, no qual o mercado dita o preço de forma centralizada. Já no mercado de balcão, o preço não está previamente estabelecido nem centralizado. O valor é definido na negociação direta entre os dealers e dependerá das informações que cada uma das partes possui sobre o ativo. Ou seja, a formação do preço depende das informações às quais os investidores têm acesso.

A segunda diferença diz respeito à centralização dos dados sobre as negociações realizadas. As operações do mercado de balcão são registradas, mas a granularidade das informações disponibilizadas ao público é limitada. Ou seja, os dados públicos normalmente são disponibilizados de forma consolidada, por volume diário e preço médio, com um dia de defasagem.

Se considerarmos ativos de crédito privado com poucas negociações, é possível passarmos semanas ou até meses sem que seja registrada nenhuma operação. Esse cenário cria uma dinâmica extremamente desafiadora para os modelos de precificação. Afinal, mesmo sem negócios registrados, esses papéis precisam ser precificados diariamente.

A terceira diferença — e talvez a mais subestimada — é também a maior virtude do mercado de balcão. Ela diz respeito à complexidade dos ativos e ao acesso aos seus eventos corporativos.

Para se ter uma ideia do desafio, considere a emissão de um CRA comum. O cálculo do preço exige o cadastro de até 50 parâmetros distintos, extraídos de um documento jurídico geralmente disponibilizado em PDF. Superada a barreira do cadastro inicial, novos desafios surgem. Toda essa parametrização não garante a precificação correta durante a vigência do ativo. Ao longo da vida do papel, podem ocorrer pagamentos extraordinários, repactuação de fluxos ou de remuneração, e até um evento de crédito do devedor. Cada um desses eventos precisa ser incorporado ao processo de precificação

— sob pena do ativo ser marcado a um valor errado.

E onde estão essas informações? Em documentos de assembleias de credores, muitas vezes publicados apenas no site da securitizadora ou do agente fiduciário, sem padronização, sem centralização, sem obrigação de formato.

Esse é o problema. Mas é também a razão do mercado de balcão existir. A mesma flexibilidade contratual que torna cada CRA um quebra-cabeça de precificação é o que permite personalizar a dívida de acordo com a necessidade do devedor. Um bônus padronizado, negociado em bolsa, não pode se adaptar ao fluxo de caixa de uma safra, à sazonalidade de um projeto de infraestrutura ou à estrutura de garantias de um devedor específico. Um ativo de balcão pode. E é exatamente essa capacidade de customização que justifica sua existência como classe de ativo.

O preço dessa flexibilidade, porém, é a opacidade operacional: cada personalização contratual é também uma nova fonte de informação dispersa, que precisa ser garimpada, interpretada e incorporada corretamente ao preço. Não há como ter uma coisa sem a outra.

Toda essa problemática possui algumas causas estruturais que precisam ser consideradas para melhorar o acesso aos dados no mercado de balcão. Entre elas, podemos destacar a necessidade de um repositório centralizado obrigatório para todos os eventos de crédito privado, além da padronização do formato e do timing de divulgação. Hoje, não há padronização e cada emissor ou agente fiduciário divulga as informações de uma forma, em um local e em um momento específico.

Soma-se a esse contexto estrutural o fato de algumas fontes de confirmação indispensáveis para a precificação ainda serem cobradas, o que cria uma barreira adicional de custos e contribui ainda mais para a ampliação dessa assimetria. Quando temos um ativo líquido, como os negociados no mercado de bolsa, todas as fontes convergem para um preço de referência bem estabelecido. Porém, o cenário muda quando falamos de ativos ilíquidos, especialmente em um ambiente marcado pela assimetria de informação.

Resumidamente, enquanto na bolsa o preço é um fato, no mercado de balcão o preço é resultado de um modelo. E, para ser eficiente, esse modelo depende, necessariamente, do acesso às informações. O horizonte ideal é que todos os dados brutos essenciais para o monitoramento e a precificação de ativos de balcão se tornem públicos, granulares e acessíveis a todos os participantes. É esse movimento que irá aumentar a liquidez e favorecer o avanço das negociações, tornando o mercado, efetivamente, mais seguro e transparente. É nessa direção que precisamos caminhar.

(*) Sócio e gerente de Market Data da LUZ Soluções Financeiras.

IA na medicina: novas regras reforçam responsabilidade e proteção de dados

“O médico deve empregar a IA exclusivamente como ferramenta de apoio”

As novas regras para o uso de inteligência artificial (IA) na medicina entraram em vigor no dia 26 de agosto e passam a estabelecer parâmetros para médicos, hospitais e demais instituições de saúde que utilizam a tecnologia. A Resolução nº 2.454/2026, do Conselho Federal de Medicina (CFM), determina que a IA deve funcionar como ferramenta de apoio, sem substituir a autonomia e o julgamento do médico, além de ampliar as exigências relacionadas à transparência e à proteção dos dados dos pacientes.

A regulamentação alcança diferentes aplicações da IA na área médica e estabelece critérios de governança, auditoria, monitoramento e avaliação de riscos. Na prática clínica, um dos principais pontos é a definição de que diagnósticos, prognósticos, prescrições e decisões terapêuticas continuam sob responsabilidade do profissional, mesmo quando sistemas automatizados participam da análise das informações.

Segundo Gustavo Clemente, especialista em Direito Médico e da Saúde, pós-graduado em Lei Geral de Proteção de Dados e sócio do Lara Martins Advogados, a norma deixa clara a posição da IA como instrumento auxiliar. “O médico deve empregar a IA exclusivamente como ferramenta de apoio, mantendo-se como responsável final pelas decisões clínicas, diagnósticas, terapêuticas e prognósticas. No plano ético-profissional, portanto, a responsabilidade permanece centrada no médico, independentemente do grau de sofisticação do sistema utilizado”, explica.

A resolução também prevê uma proteção ao profissional contra responsabilização indevida quando a falha for atribuível exclusivamente



ao sistema de IA, desde que fique comprovado que a ferramenta foi utilizada de maneira diligente, crítica e ética.

Para o especialista, entretanto, essa previsão não deve ser interpretada como uma blindagem automática. Em situações que envolvam danos ao paciente, a eventual responsabilidade civil dos diferentes participantes — médico, instituição de saúde e fornecedor da tecnologia — deverá ser analisada conforme as circunstâncias de cada caso e à luz da legislação aplicável. “A resolução define de forma inequívoca a responsabilidade ético-profissional do médico, mas não resolve toda a complexidade da responsabilidade civil envolvendo hospitais, clínicas e desenvolvedores dos sistemas. Essas situações deverão ser avaliadas caso a caso, considerando, entre outras normas, o Código Civil, o Código de Defesa do Consumidor e os contratos existentes entre as partes”, ressalta o advogado.

Outro ponto central da regulamentação é o tratamento de informações dos pacientes. Por serem considerados dados pessoais sensíveis pela Lei Geral de Proteção de Dados (LGPD), os dados de saúde devem receber proteção reforçada quando utilizados por ferramentas de inteligência artificial.

A resolução determina que o médico zele pela confidencialidade, integridade e segurança das informações e proíbe a utilização de sistemas que não ofereçam padrões mínimos de segurança compatíveis com dados sensíveis. O compartilhamento dessas informações com ferramentas de IA também deverá ocorrer apenas quando estritamente necessário e amparado por base legal adequada. “A eficiência ou o custo de uma ferramenta não são suficientes para justificar sua adoção. Médicos e instituições precisam avaliar se a tecnologia oferece segurança adequada para tratar dados de saúde”, afirma Clemente.

A norma também incorpora o conceito de privacy by design, pelo qual a proteção da privacidade deve estar presente desde a concepção e durante todo o ciclo de vida dos sistemas. Entre as medidas previstas estão mecanismos como anonimização e criptografia, além da proteção contra perda, alteração, acesso não autorizado e vazamento de informações. “A resolução não substitui a LGPD. Ela reforça e especifica seus cuidados dentro do ambiente clínico. A proteção dos dados precisa fazer parte do próprio desenho da tecnologia, e não ser acrescentada posteriormente”, destaca.

Paciente deverá ser informado sobre uso da IA
As novas regras também produzem efeitos diretos

na relação entre médico e paciente. Quando a IA for utilizada como apoio relevante no cuidado, diagnóstico ou tratamento, o paciente deverá receber informações claras e acessíveis sobre seu uso.

Além disso, a autonomia do paciente deve ser respeitada, inclusive diante da recusa informada da utilização da tecnologia. A norma também impede que o médico delegue à IA, sem a devida mediação humana, a comunicação de diagnósticos, prognósticos ou decisões terapêuticas. “O dever não se resume a dizer ao paciente que uma inteligência artificial está sendo utilizada. É preciso fornecer informação suficiente para que ele compreenda o papel daquela tecnologia no seu atendimento, seus limites e como ela participa do processo de decisão médica”, explica.

O uso da IA como apoio à decisão médica também deverá ser registrado no prontuário. Para Gustavo, a exigência aumenta a transparência e ganha importância jurídica porque permite reconstruir posteriormente o processo que levou a determinada conduta clínica.

Na avaliação do advogado, a nova regulamentação procura estabelecer uma fronteira entre inovação tecnológica e responsabilidade humana. “A IA pode auxiliar o médico, mas não pode assumir o lugar do profissional nas decisões críticas. A relação médico-paciente, a escuta, a empatia e a responsabilidade pela decisão clínica continuam sendo humanas”, conclui.

(Fonte: Gustavo Clemente: especialista em Direito Médico e da Saúde (EBRAD), pós-graduado em Administração Hospitalar (IPEP) e em Lei Geral de Proteção de Dados (LGPD) pelo Instituto Legale, sócio do Lara Martins Advogados).

Geração Z é maior vítima de tentativas de fraude de identidade

Volume de ocorrências entre a Geração Z cresceu 27,3% na comparação com o mesmo período de 2025. A expansão da vida financeira e digital dos mais jovens está criando também novos pontos de atenção para a proteção da identidade. No primeiro semestre de 2026, a Geração Z ultrapassou X, Millennials e Baby Boomers e passou a concentrar o maior volume de tentativas de fraude de identidade entre as gerações analisadas pelo Mapa da Fraude da Serasa Experian, primeira e maior datatech do Brasil e líder em soluções antifraude. Foram cerca de 505 mil ocorrências envolvendo esse público, alta de 27,3% em apenas um ano.

O movimento ajuda a desconstruir a percepção de que as tentativas de fraude de identidade estão associadas principalmente aos consumidores mais velhos. À medida que públicos mais jovens ampliam sua participação em jornadas como abertura de

digitais, aumentam também os pontos de contato nos quais criminosos podem tentar utilizar identidades falsas ou dados de terceiros.

“Existe uma percepção de que as pessoas mais velhas são sempre o principal alvo das fraudes, mas os dados mostram que os criminosos direcionam suas tentativas para diferentes gerações, especialmente aquelas com maior atividade econômica e digital”, explica o Diretor de Autenticação e Prevenção a Fraude, Leandro Bartolassi. “No caso da Geração Z, a entrada no sistema financeiro, com a abertura das primeiras contas, o acesso ao crédito e a contratação de novos serviços, amplia as possibilidades de relacionamento com empresas, mas também cria novos pontos de atenção. Isso não significa que uma geração seja mais vulnerável, mas que os fraudadores acompanham os públicos e as jornadas com maior potencial de exploração”, completa.

Fraude avança entre diferentes gerações

Embora a Geração Z tenha apresentado o maior volume e o avanço mais expressivo entre os principais grupos geracionais, o crescimento não ficou restrito aos mais jovens. A Geração X aparece logo atrás, com aproximadamente 484 mil tentativas de fraude de identidade no semestre e alta de 19,5% em relação ao mesmo período de 2025. Entre os Millennials, foram cerca de 389 mil ocorrências, crescimento de 19,2%.

Para a datatech, o cenário reforça que idade, isoladamente, não determina a exposição às tentativas de fraude de identidade. Os criminosos acompanham a digitalização das jornadas e as oportunidades de exploração em diferentes momentos da vida do consumidor, o que amplia a importância de mecanismos de validação capazes de identificar inconsistências desde o primeiro contato entre uma pessoa e uma empresa.