A inteligência artificial já não é uma promessa distante nem um tema restrito às áreas de tecnologia. Ela atravessa processos, influencia decisões, reorganiza rotinas e redefine a forma como nos relacionamos com dados. No setor de previdência complementar fechada, isso não é diferente. A IA começa a aparecer em análises preditivas, sistemas de apoio à decisão, comunicações automatizadas, ferramentas de organização de informações e soluções contratadas de terceiros. A pergunta que precisamos enfrentar não é se vamos utilizá-la, mas com que grau de maturidade institucional estamos fazendo isso.

Em recente reflexão sobre os riscos associados ao uso de IA, surge um ponto que considero central: o risco não está apenas no mau uso, mas também na subutilização. Subutilizar é perder vantagem competitiva, eficiência e capacidade analítica. Usar sem controle, por outro lado, pode gerar riscos severos – viés, erros, impactos reputacionais e violações à LGPD. Entre esses dois extremos, o que faz diferença é governança.

Os riscos da inteligência artificial são, por natureza, transversais. Não se limitam a uma dimensão técnica. Há o risco ético, quando decisões automatizadas podem afetar direitos fundamentais, gerar discriminação ou exclusão. Há o risco técnico, ligado à complexidade dos modelos, à opacidade e à dificuldade de explicabilidade – a chamada “caixa-preta”, em que decisões são tomadas sem que se compreenda claramente como se chegou a determinado resultado. Há o risco operacional e estratégico, quando a dependência tecnológica, os custos de implementação ou a inviabilidade de longo prazo comprometem a sustentabilidade financeira. E há o risco legal e de privacidade, especialmente relevante em um setor que lida com grande volume de dados sensíveis, históricos e financeiros.

Esses riscos se interconectam. Uma solução mal parametrizada pode gerar viés, impactar direitos, produzir questionamentos regulatórios e afetar a reputação institucional. Uma ferramenta externa utilizada sem critérios pode expor dados pessoais e gerar responsabilização. A inteligência artificial não cria um novo universo de risco isolado; ela potencializa e acelera riscos já existentes, exigindo controles mais robustos.

É nesse contexto que a discussão sobre IA própria ou de terceiros ganha relevância. Desenvolver internamente ou contratar no mercado são decisões estratégicas. Mas, em ambos os casos, a responsabilidade permanece com a entidade. Não há terceirização de dever fiduciário. Se um sistema automatizado falha, se um bot executa operação indevida ou se uma comunicação gerada por IA induz comportamento inadequado, a pergunta inevitável é: quem responde? Sem definição clara de responsabilização, não há governança efetiva.

A integração da IA à governança corporativa exige coerência com estruturas já consolidadas. Segregação de funções, supervisão, controles internos e reporte à alta gestão continuam sendo pilares. A IA deve dialogar com os modelos de gestão de riscos e compliance, inserindo-se no arcabouço de GRC, e não funcionando à margem dele. Isso implica mapear riscos, avaliar impactos, definir controles preventivos e corretivos e acompanhar o ciclo de vida das soluções tecnológicas.

É aqui que a política institucional de uso de inteligência artificial se torna instrumento essencial. Não como formalidade, mas como diretriz estruturante. Uma política madura precisa definir propósito e limites de uso: para que cada solução foi implantada, qual valor gera e quais são suas fronteiras. Deve exigir avaliação prévia de riscos, com checklist que contemple viés, impacto à privacidade, conformidade legal, riscos reputacionais e continuidade do negócio. Precisa estabelecer auditorias e revisões periódicas, com testes regulares de vieses, falhas e segurança, além de prever fluxo de reporte e resposta a incidentes.

Também é recomendável que a governança de IA tenha assento formal, por meio de comitê multidisciplinar que envolva tecnologia, jurídico, compliance, riscos e áreas de negócio. Cada

solução deve ter responsável claramente designado, com nome e cargo associados às decisões críticas. Controles de acesso, registro de logs, mecanismos de explicabilidade e possibilidade de auditoria não são luxo; são requisitos mínimos de maturidade.

Nesse cenário, o Programa Anual de Fiscalização e Monitoramento da Previc, ao reforçar a supervisão baseada em risco, a fiscalização indireta e a atenção a temas transversais como segurança cibernética e transparência, sinaliza que o ambiente regulatório acompanha essa evolução. O PAF 2026, ao abranger 111 entidades e reforçar a lógica de fiscalização segmentada, com ênfase em monitoramento contínuo, temas transversais e uso de tecnologia, confirma um movimento já em curso: a supervisão baseada em risco está mais estruturada, mais orientada por dados e menos dependente de modelos puramente reativos. Esse dado, embora relevante, é apenas o pano de fundo de uma discussão mais ampla que precisa acontecer dentro das próprias entidades.

O que realmente merece nossa atenção não é apenas como seremos supervisionados, mas como estamos nos organizando para governar um ambiente cada vez mais digital. A inteligência artificial deixou de ser um conceito abstrato para se tornar ferramenta operacional. Ela está presente em sistemas de apoio à decisão, em análises preditivas, em comunicações automatizadas e em soluções contratadas de terceiros. Muitas vezes, porém, sua utilização ocorre de forma fragmentada, sem inventário formal, sem classificação de risco específica e, sobretudo, sem clara atribuição de responsabilidade.

Não estou falando sobre aprender a programar algoritmos. Não é esse o desafio central para o nosso setor. O ponto é maturidade institucional. Governança de IA não é saber usar ferramentas sofisticadas; é saber estabelecer limites, critérios, controles e fluxos de supervisão. É compreender que decisões influenciadas por tecnologia continuam produzindo efeitos humanos concretos. Quando um modelo sugere um perfil de investimento, quando um sistema automatiza uma comunicação, quando uma ferramenta organiza informações sensíveis, há impactos que transcendem a eficiência operacional.

Não se trata de frear inovação. A inteligência artificial pode e deve ser utilizada para melhorar processos, qualificar análises e aumentar eficiência. O que não podemos é permitir que a busca por agilidade comprometa o ativo mais valioso do nosso sistema: a confiança. A previdência complementar é, por essência, compromisso de longo prazo. Ela exige prudência, responsabilidade fiduciária e visão estratégica.

Elevar o nível de maturidade sobre o uso de IA significa reconhecer que tecnologia é acelerador, mas governança é direção. Se o futuro da operação será cada vez mais digital, nossa responsabilidade institucional precisa ser ainda mais sólida. A pergunta que permanece é simples e profunda: estamos estruturando a inteligência artificial com o mesmo rigor com que estruturamos investimentos, solvência e conformidade? Se a resposta ainda não for plenamente afirmativa, o momento de agir é agora.

***Germana Vogt** é Advogada, Coordenadora do Grupo de Estudos de Previdência Complementar da CESPC (Comissão Especial de Seguros e Previdência Complementar) da OAB/RS e Membro da Comissão de Ética e Compliance da FEDERASUL

Fonte: Abrapp em Foco, em 27.02.2026.