Documento apresenta as diferentes fases de testes do projeto-piloto, e tem o foco na produção de evidências, na gestão de riscos e no aprendizado regulatório

A Agência Nacional de Proteção de Dados (ANPD) publicou, nesta quarta-feira (19), a metodologia de testagem do Sandbox Regulatório em Inteligência Artificial e Proteção de Dados, documento que apresenta os procedimentos de supervisão, monitoramento e avaliação das soluções dos participantes do projeto-piloto. Desenvolvida pelo Centro de Inteligência Artificial e Aprendizado de Máquina da Universidade de São Paulo (CIAAM/USP), a metodologia foi validada pela Comissão de Sandbox da Agência e busca avaliar aspectos relacionados à transparência, explicabilidade e proteção de dados pessoais em sistemas de inteligência artificial.

>> Confira a Metodologia de Testagem do Sandbox Regulatório em IA e Proteção de Dados

O sandbox regulatório é um ambiente controlado e supervisionado no qual soluções inovadoras são testadas em condições definidas, permitindo ao regulador acompanhar riscos, produzir evidências e extrair aprendizados para aperfeiçoar a regulação. Um dos objetivos da metodologia utilizada é assegurar a confiabilidade e a possibilidade de comparação dos resultados. Para isso, as informações fornecidas pelos participantes são confrontadas com documentos, registros técnicos, resultados de testes e pareceres especializados, inclusive da própria Agência. O acompanhamento da evolução das soluções ao longo da experimentação visa identificar riscos e oportunidades de aprimoramento, além de gerar subsídios para decisões futuras da ANPD.

A escolha da inteligência artificial como objeto deste projeto-piloto considera os desafios que essas tecnologias apresentam para a proteção de dados pessoais, em especial, de crianças e adolescentes. Por isso, a transparência algorítmica é um dos pontos centrais da experimentação, com atenção à explicabilidade e ao acesso a informações sobre decisões automatizadas.

>> Confira o Radar Tecnológico sobre Inteligência Artificial Generativa

Metodologia em ciclos

A testagem é organizada em seis ciclos. O primeiro possui estrutura específica para adaptação ao ambiente experimental e coleta das informações iniciais dos participantes. A aplicação prática dessa fase foi registrada no 1º Relatório Parcial de Monitoramento – Fase de Teste, Ciclo 1. Esse primeiro ciclo, de caráter preparatório, teve foco no alinhamento metodológico, na organização das atividades e na estruturação das condições técnicas e regulatórias para as etapas seguintes.

Do segundo ao sexto ciclo, as atividades são divididas nas três fases “Preparação e Detalhamento”, “Experimentação e Gestão de Riscos”, e “Avaliação e Ajuste”. Esse formato permite que os resultados de cada etapa orientem a próxima, e garantem que o processo seja ajustado de acordo com novos elementos identificados durante a experimentação.

Na fase de Preparação e Detalhamento, são levantadas informações sobre arquitetura das soluções, fluxos de dados, controles de segurança, tratamento de dados pessoais, maturidade tecnológica, coordenação regulatória e medidas de transparência. Na etapa seguinte, são realizados os testes e o acompanhamento contínuo dos riscos e das medidas de mitigação. Já na fase de Avaliação e Ajuste, os resultados são consolidados em pareceres e relatórios que registram avanços, limitações, riscos, lacunas regulatórias e recomendações para os ciclos seguintes.

No sandbox regulatório, as informações são revistas a cada ciclo e podem ser atualizadas diante de mudanças técnicas, regulatórias, organizacionais ou operacionais, como alterações na arquitetura, nos fluxos de dados, nos controles de segurança ou no nível de risco. Dessa forma, novos desafios identificados durante os testes passam a integrar as etapas seguintes de avaliação, permitindo que o próprio ambiente experimental seja aperfeiçoado a partir das evidências produzidas.

O desenvolvimento do projeto é resultado de um processo iniciado com o Estudo Técnico sobre Sandbox Regulatório, de 2023, e que incluiu a Consulta à Sociedade sobre o Sandbox Regulatório de IA e Proteção de Dados. A iniciativa também está alinhada ao Guia Referencial de Sandbox Regulatório, da Advocacia-Geral da União.

Fonte: ANPD, em 19.08.2026.