Brasília, 06 de outubro de 2026

Seleção

Sumário

IT Forum

Segunda-feira, 05 de outubro de 2026 | Propriedade Intelectual
IA precisa ser defensável desde a concepção, diz David Cass, referência internacion… 3

BOL - Notícias

Segunda-feira, 05 de outubro de 2026 | Patentes
Chinesa Huawei e americana Qualcomm fecham acordo de patentes de 5G e IA 6

IA precisa ser defensável desde a concepção, diz David Cass, referência internacional em cibersegurança



Mostrar o trabalho como padrão mínimo

No Cyber Security Summit realizado nesta segunda-feira (5), em São Paulo, o especialista internacional em segurança da informação, David Cass, defendeu que organizações que adotam inteligência artificial (IA) precisam documentar seus sistemas desde a fase de desenvolvimento, não apenas quando enfrentam um processo judicial. Para Cass, a ausência de registros adequados não é um problema contornável depois do fato.

"A IA precisa ser defensável por design", afirma ele. A mensagem foi dirigida a executivos, engenheiros e líderes de equipes de IA presentes na palestra "When AI Meets the Courtroom: Building Trustworthy AI Systems Through Legal and Technical Governance" ou "Quando a IA encontra os tribunais".

As melhores notícias de tecnologia B2B Acompanhe todas as novidades diretamente na sua caixa de entrada

Cass identificou quatro dimensões que tribunais utilizam ao avaliar sistemas de inteligência artificial como evidência. A primeira é a autenticação, a demonstração de que o modelo produz resultados confiáveis e precisos, e não apenas a verificação técnica de identidade convencional.

A segunda é a confiabilidade e admissibilidade, traduzida nos Estados Unidos pelo estilo Daubert, que examina se o modelo passou por testes documentados, revisão por pares e se há pesquisa publicada sobre ele. A terceira dimensão é a explicabilidade. "Quem em sua organização é capaz de explicar a um juiz e a um júri uma questão técnica tão complexa de uma maneira que possam entender?",

questiona o especialista.

Cass observa que organizações com centenas de milhares de funcionários que só conseguem colocar três pessoas da equipe de ciência de dados para explicar o funcionamento de seus modelos enfrentam um problema grave sob o ponto de vista regulatório.

A quarta, e última, dimensão é a cadeia de custódia da proveniência do modelo: qual versão foi usada, qual modelo de linguagem de grande escala (large language model, ou LLM), como foi implantado, quem autorizou a colocação em produção e qual caminho de testes foi seguido antes da entrega ao usuário final.

OpenAI contrata ex-Google Cloud para liderar parcerias na América Latina

Um dos pontos de maior atenção da palestra foi o que Cass chamou de "problema gêmeo". Ao mesmo tempo em que conteúdo sintético gerado por IA pode ser apresentado como real em disputas judiciais, evidências genuínas passam a ser contestadas sob a alegação de que podem ter sido fabricadas. "Estamos vendo o potencial para material sintético gerado por IA sendo oferecido como real, assim como estamos vendo evidências reais não serem aceitas porque as pessoas alegam que são potencialmente falsas", explica.

A solução, segundo ele, passa por padrões técnicos de engenharia: criptografia, hashing, capacidade de detecção forense e registros de processo certificados que demonstrem como o conteúdo foi gerado. Em setores como indústria farmacêutica e serviços financeiros, esses registros podem precisar de validação por terceiros.

Mostrar o trabalho como padrão mínimo

O especialista também é enfático ao afirmar que o padrão nos tribunais é direto, mas frequentemente ignorado pelas equipes de IA; mostrar o trabalho. O registro de como o sistema foi desenvolvido,

Continuação: IA precisa ser defensável desde a concepção, diz David Cass, referência internacional em cibersegurança

testado e monitorado é o que diferencia uma organização capaz de se defender de uma exposta a sanções.

Ele alerta que advogados já foram punidos por apresentar jurisprudência inventada por sistemas de

IA sem verificação. "Não é possível apenas dizer

'eu confiei na IA'. A culpa da decisão, não é da IA, verificar a saída ainda é uma responsabilidade humana", afirma. A lição se aplica diretamente ao ambiente corporativo: a delegação de decisões para um modelo não transfere a responsabilidade.

Outro risco em crescimento são os litígios de privacidade relacionados ao uso de informações pessoalmente identificáveis (PII) em modelos de inteligência artificial. No Brasil, Cass menciona a Lei Geral de Proteção de Dados (LGPD) e as ações de fiscalização da Autoridade Nacional de Proteção de Dados (ANPD) como mecanismos já em vigor para proteger dados de cidadãos brasileiros. Também cita a resolução do Conselho Nacional de Justiça (CNJ), em vigor desde julho de 2025, que regula o uso de inteligência artificial pelo próprio sistema judiciário.

Arquitetura preparada para disputas

Se aprofundamento, Cass ainda detalha o conceito de arquitetura pronta para disputas. O princípio é registrar como uma testemunha, não como um depurador, o que os desenvolvedores buscam nos logs é diferente do que os tribunais vão examinar.

Entre os elementos práticos indicados estão o registro de prompts com entradas e conteúdo recuperado, a identificação da versão e dos parâmetros operacionais do modelo, a manutenção de logs à prova de adulteração, com carimbo de data e hora e a definição de períodos de retenção, equivalentes aos de documentos corporativos.

O palestrante também recomenda testes de reprodução. "Se eu inserir um conjunto de informações naquela tecnologia e outra pessoa inserir exatamente o mesmo conjunto, a resposta deve ser a mesma", diz.

Os pesos dos modelos, responsáveis por essa reprodução, são equações matemáticas e devem ser tratados como pontos críticos, capazes de indicar quais dados são mais relevantes durante o treinamento. "Se a IA for treinada a partir de certos fatores, em que a saída é mais importante do que outras variáveis, não é um bom indicador para lidar com determinados dados", observa.

Durante sua apresentação, o executivo dedicou uma seção somente para **arbitragem**, reconhecida pela legislação brasileira como a alternativa mais ágil ao sistema judicial tradicional. Segundo ele, frameworks de **arbitragem** desenvolvidos para conflitos de IA, como as regras da Judicial Arbitration and Mediation Services (JAMS), contam com espe-

cialistas que eliminam a necessidade de explicar conceitos básicos a juízes e júris leigos. "Você não precisa explicar o que é um token, qual a diferença entre IA agêntica e aprendizado de máquina padrão, ou o que é automação de processo robótico", afirma.

As quatro categorias de disputa mais frequentes identificadas pelo palestrante são violações de **propriedade intelectual**, violações de privacidade de dados, uso indevido de conteúdo sintético e violações de segredos comerciais envolvendo LLMs. Para organizações que negociam contratos envolvendo inteligência artificial, Cass recomenda incluir cláusulas de **arbitragem** e alinhar a engenharia interna com os compromissos assumidos contratualmente.

Governança como vantagem competitiva

A finalização da palestra traz a cereja do bolo quando o assunto é segurança e IA, uma governança bem executada. "Se você faz uma boa governança, a IA pode te deixar à frente, mas o oposto também acontece, deixando muito atrás", declara Cass.

O palestrante ainda cita frameworks do Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) e da Organização Internacional de Normalização (ISO) como pontos de partida para organizações que precisam estruturar avaliações de risco.

Ele alerta para o aumento de responsabilidade nos níveis executivos, onde diretores de segurança da informação já enfrentam processos judiciais, e os conselhos de administração passam a ser cobrados por conhecimento dos riscos de inteligência artificial, ainda que não precisem ser especialistas técnicos.

Cass propõe um roteiro de governança que começa pelo inventário de ativos de IA da organização e pelo mapeamento de contratos que envolvam a tecnologia, avança para a construção de documentação

Continuação: IA precisa ser defensável desde a concepção, diz David Cass, referência internacional em cibersegurança

completa em torno de um modelo específico e culmina na institucionalização do processo para os demais sistemas. "A IA diante de um tribunal deve ser um problema de negócios, não de segurança e nem de uma pessoa na ciência de dados, toda a corporação deve estar preparada", conclui ele.

Chinesa Huawei e americana Qualcomm fecham acordo de patentes de 5G e IA



A chinesa Huawei Technologies fechou um amplo acordo plurianual de licenciamento de **patentes** com a Qualcomm que inclui licenças cruzadas das **patentes** das duas empresas em tecnologias de 5G, computação, IA (Inteligência Artificial) e redes. As companhias informaram hoje que a Qualcomm também comprará algumas **patentes** da Huawei registradas nos Estados Unidos nas áreas de computação, IA, redes e outras tecnologias.

Segundo a Huawei, este é o primeiro acordo de licenciamento com a Qualcomm que cobre tecnologia 5G. A empresa chinesa afirmou ainda que é o primeiro contrato em que licencia e transfere**patentes** de computação, IA e redes para a fabricante americana de chips.

O entendimento ocorre semanas depois de a Huawei ter fechado um acordo de licenciamento cruzado com a HP envolvendo**patentes** usadas em tecnologia Wi-Fi.

O novo negócio reforça que a Huawei segue como uma das maiores detentoras de **patentes** no campo de tecnologia da informação e comunicações, apesar de anos de sanções dos EUA que limitaram seu acesso a semicondutores avançados.

Huawei e Qualcomm não divulgaram os termos financeiros. O fechamento do acordo depende de aprovações regulatórias. A Huawei afirmou que, com a assinatura, o valor esperado de seus contratos de licenciamento de **patentes** até agora ultrapassou US$ 6,9 bilhões.

As duas empresas já firmaram vários acordos ao longo dos anos, com o primeiro assinado há mais de duas décadas.

A Huawei disse que seu primeiro pagamento de licenciamento de **propriedade intelectual** foi para a Qualcomm em 2001 e que sua primeira receita com licenciamento de PI veio da Motorola em 2011. *Conteúdo traduzido com auxílio de Inteligência Artificial, revisado e editado pela Redação do Broadcast, sistema de notícias em tempo real do Grupo Estado

Índice remissivo de assuntos

Patentes 4
Propriedade Intelectual 1,2,3,4