Brasília, 30 de outubro de 2026

Seleção

Sumário

Época Negócios - Online

Quinta-feira, 29 de outubro de 2026 | Propriedade Intelectual
Na era da inteligência artificial, proteger informações é proteger o próprio negócio 3

Correio Braziliense - Online

Quinta-feira, 29 de outubro de 2026 | Marco regulatório | INPI
O vale de vinhedos gaúcho que fez história em 2002 e se tornou o primeiro do país… 5

Exame.com

Quinta-feira, 29 de outubro de 2026 | Propriedade Intelectual
Sua empresa usa IA? 7 riscos jurídicos que podem acabar em processo 7

Quinta-feira, 29 de outubro de 2026 | Propriedade Intelectual
Brasil cai uma posição no ranking de inovação global 9

R7

Quinta-feira, 29 de outubro de 2026 | Propriedade Intelectual
Como a nova regulamentação pode impulsionar os estúdios de games brasileiros… 10

Consultor Jurídico

Quinta-feira, 29 de outubro de 2026 | Propriedade Intelectual
Engenharia reversa de IA: propriedade e responsabilidade 13

Na era da inteligência artificial, proteger informações é proteger o próprio negócio



A segurança da informação precisa deixar de ser percebida como um custo operacional ou uma responsabilidade isolada da área de tecnologia e passar a integrar as discussões estratégicas da alta liderança

A inteligência artificial está redefinindo a maneira como as empresas inovam, competem, produzem e se relacionam com seus clientes. Modelos generativos, agentes autônomos e sistemas inteligentes ampliam a produtividade e criam oportunidades de negócios que, até pouco tempo, pareciam distantes. Entretanto, existe uma dimensão dessa transformação que ainda não recebe a atenção proporcional à sua importância, sendo a segurança da informação.

Durante décadas, a proteção de dados foi tratada predominantemente como uma responsabilidade das áreas de tecnologia. Investimentos em infraestrutura, controles de acesso, firewalls, criptografia e mecanismos de prevenção de ataques constituíram a base das estratégias de segurança corporativa. Esse modelo, embora continue necessário, tornou-se insuficiente diante da velocidade e da complexidade introduzidas pela inteligência artificial.

O desafio atual não consiste apenas em proteger sistemas e bases de dados. É preciso proteger o conhecimento organizacional, a **propriedade intelectual**, os processos decisórios e a própria capacidade de competir em um ambiente no qual informações podem ser compartilhadas, processadas e reproduzidas com inteligência artificial (IA).

A primeira mudança está relacionada à democratização do acesso à IA. Ferramentas cada vez mais acessíveis permitem que profissionais de diferentes áreas desenvolvam soluções, automatizem atividades e analisem grandes volumes de informação. O problema surge quando essa utilização acontece sem políticas claras de governança. Informações estratégicas, dados de clientes, documentos internos, contratos e conhecimentos proprietários podem ser inseridos em plataformas externas sem que a organização tenha plena consciência dos riscos envolvidos.

Esse fenômeno, frequentemente associado ao chamado Shadow AI, representa uma nova fronteira de exposição corporativa. Assim como aconteceu com a adoção descontrolada de serviços em nuvem e dispositivos pessoais, a inteligência artificial pode se disseminar dentro das empresas antes que seus mecanismos de controle estejam preparados.

A segunda mudança está na sofisticação das ameaças. A IA também amplia a capacidade de atuação de agentes mal-intencionados. A criação de mensagens fraudulentas altamente personalizadas, a **falsificação** de vozes e imagens e o desenvolvimento de ataques mais sofisticados tornam as práticas tradicionais de segurança progressivamente mais desafiadoras.

Nesse contexto, a confiança passa a ser um ativo particularmente vulnerável. Como distinguir uma comunicação legítima de uma fraude produzida artificialmente? Como validar uma solicitação financeira feita por alguém cuja voz e imagem foram reproduzidas com elevado grau de realismo? Como assegurar que uma informação utilizada em uma decisão empresarial seja confiável?

Essas questões demonstram que a segurança da informação não pode mais se limitar à proteção de ambientes digitais. Ela precisa incorporar a capacidade de verificar identidades, validar informações e preservar a integridade dos processos organizacionais.

Existe ainda uma terceira dimensão, talvez menos evidente, mas igualmente relevante, ou seja, a segu-

Continuação: Na era da inteligência artificial, proteger informações é proteger o próprio negócio

rança dos próprios sistemas de inteligência artificial. Modelos podem ser manipulados por instruções maliciosas, expor informações sensíveis, produzir respostas incorretas ou incorporar vulnerabilidades decorrentes de dados e componentes comprometidos. A utilização de agentes capazes de acessar sistemas corporativos, consultar documentos e executar tarefas amplia ainda mais a importância dos controles de autorização, rastreabilidade e supervisão humana.

Não basta, portanto, perguntar se a empresa está utilizando IA. É necessário compreender quais dados alimentam esses sistemas, quais informações podem ser acessadas, quais decisões podem ser executadas autonomamente e quem responde por eventuais falhas.

Essa transformação exige uma mudança na própria governança corporativa. A segurança da informação precisa deixar de ser percebida como um custo operacional ou uma responsabilidade isolada da área de tecnologia e passar a integrar as discussões estratégicas da alta liderança.

Isso significa estabelecer políticas de uso, classificar informações por nível de sensibilidade, definir critérios para contratação de soluções, avaliar fornecedores, monitorar acessos e estabelecer responsabilidades sobre os sistemas utilizados. Significa também investir na formação das pessoas. Afinal, a tecnologia pode oferecer mecanismos avançados de proteção, mas decisões humanas continuam sendo uma das principais fontes de exposição e, simultaneamente, uma das mais importantes linhas de defesa.

Outro aspecto fundamental é compreender que segurança e inovação não são objetivos concorrentes. Pelo contrário, empresas que conseguem desenvolver ambientes confiáveis para experimentar e escalar soluções de inteligência artificial tendem a construir condições mais sustentáveis para inovar. A ausência de governança pode até acelerar iniciativas no curto prazo, mas cria vulnerabilidades que comprometem os resultados no longo prazo.

O desafio, portanto, não é restringir indiscriminadamente o uso da IA, mas criar condições para que sua adoção aconteça com responsabilidade, transparência e segurança. A governança deve funcionar como um habilitador da inovação, e não como uma barreira burocrática. Na era da inteligência artificial, proteger informações é proteger o próprio negócio.

O vale de vinhedos gaúcho que fez história em 2002 e se tornou o primeiro do país com origem reconhecida para vinhos



Nas prateleiras dos supermercados, alguns produtos brasileiros trazem no rótulo um selo que garante de onde vieram e como foram feitos. Essa história começou em um vale de parreirais na Serra Gaúcha. Em Bento Gonçalves, no Rio Grande do Sul, e em dois municípios vizinhos, o Vale dos Vinhedos recebeu em 2002 a primeira Indicação Geográfica do Brasil e, dez anos depois, conquistou o selo mais exigente para vinhos, abrindo caminho para muitos outros produtos do país.

O que é uma Indicação Geográfica?

Um selo que liga o produto ao lugar onde ele é feito. Segundo a associação de produtores do Vale dos Vinhedos, a **Indicação Geográfica** é um registro concedido pelo **Instituto Nacional da Propriedade Industrial** (**INPI**) que reconhece e garante a origem, a qualidade e as características regionais de um produto ou serviço. Existem duas modalidades: a Indicação de Procedência e a **Denominação de Origem**, mais rigorosa.

O vale foi pioneiro nas duas. Segundo a Embrapa Uva e Vinho, o Vale dos Vinhedos foi a primeira **Indicação Geográfica** reconhecida do Brasil: obteve do **INPI** o registro de Indicação de Procedência em 2002 e, em 2012, foi reconhecido como a primeira **Denominação de Origem** de vinhos do país.

Onde fica o Vale dos Vinhedos?

Entre três cidades da serra. A Embrapa registra que a área da Indicação de Procedência tem 81,23 km² e fica nos municípios de Bento Gonçalves, que concentra 63% do território, Garibaldi, com 30%, e Monte Belo do Sul, com 7%. Já a área da Denominação de Origem é um pouco menor, com 72,45 km².

A tradição vem de longe. Segundo a associação de produtores, a cultura do vinho no vale existe desde meados de 1875, com a chegada dos primeiros imigrantes italianos à região. Foram eles que trouxeram o costume de plantar uvas e fazer vinho em casa, prática que, mais de um século depois, deu origem às vinícolas e ao selo de origem.

Como o vale conquistou os selos?

Foram quase duas décadas de trabalho. Estes são os principais marcos, segundo a linha do tempo da Embrapa Uva e Vinho.

1 1995 Produtores criam a associação do Vale dos Vinhedos e, com a Embrapa, começam o primeiro projeto de **Indicação Geográfica** do país. 2 2001 Chegam ao mercado os primeiros vinhos comerciais com a marca da futura Indicação de Procedência. 3 2002 O **INPI** reconhece a Indicação de Procedência Vale dos Vinhedos, a primeira **Indicação Geográfica** do Brasil. 4 2010 a 2013 Pesquisadores estudam solos e delimitam a área para a **Denominação de Origem**. 5 2012 O **INPI** reconhece a **Denominação de Origem** Vale dos Vinhedos, a primeira de vinhos do Brasil.

O que um vinho precisa ter para usar o selo?

Seguir regras rígidas. Segundo a Embrapa, na Denominação de Origem a produção das uvas e a elaboração dos vinhos precisam ocorrer exclusivamente dentro da área delimitada do Vale dos Vinhedos. A associação de produtores acrescenta que as uvas devem ser 100% da área demarcada e que a colheita é sempre manual.

As uvas também são definidas. Segundo o portal A Lavoura, a Denominação de Origem tem regras de cultivo e de produção mais restritas que a Indicação de Procedência, e um vinho varietal Merlot precisa ter no mínimo 85% dessa uva. Um conselho regulador ligado à associação dos produtores fiscaliza o uso do selo, que aparece no rótulo das garrafas

aprovadas.

Como é o clima de Bento Gonçalves ao longo do ano?

A chuva é bem distribuída, e o inverno é frio. Outubro registra 218 mm em média, enquanto agosto tem 142 mm, e julho tem mínima de 8°C.

âï¸ Verão Dez-Fev Média: 17-27°C Chuva: Alta Época da vindima, a colheita das uvas. ð Outono Mar-Mai Média: 11-25°C Chuva: Média Vinhedos mudando de cor e dias amenos. âï¸ Inverno Jun-Ago Média: 8-20°C Chuva: Média Frio, ideal para vinhos tintos e lareira. ð¸ Primavera Set-Nov Média: 11-25°C Chuva: Alta Brotação das videiras e outubro chuvoso. ð¡ Dica do especialista: a chuva é bem distribuída ao longo do ano, sem estação seca definida. Para ver as parreiras carregadas, prefira o verão, época da colheita. Ao comprar vinho, procure o selo da Indicação de Procedência ou da Denominação de Origem no rótulo.

Temperaturas aproximadas com base no Climatempo. Condições podem variar.

Dom João VI pediu 100 famílias suíças para uma colônia e cerca de 2 mil pessoas embarcaram em 1819 para serra fluminense.

Um vale que abriu caminho para o país

O Vale dos Vinhedos mostra como uma tradição trazida por imigrantes pode virar referência nacional. Os parreirais de Bento Gonçalves, Garibaldi e Monte Belo do Sul conquistaram em 2002 a primeira Indicação Geográfica do Brasil e, em 2012, a primeira Denominação de Origem de vinhos. Hoje, cada garrafa com o selo carrega a história de um vale que ensinou o país a proteger o que nasce da sua terra.

Você precisa percorrer o Vale dos Vinhedos na época da colheita, visitar uma vinícola e procurar o selo de origem no rótulo para entender por que esse vale é um marco do vinho brasileiro.

Sua empresa usa IA? 7 riscos jurídicos que podem acabar em processo



Decisões automatizadas, informações confidenciais e **direitos autorais** estão entre os pontos que exigem atenção de empresas que adotam inteligência artificial

A adoção de inteligência artificial nas empresas pode acelerar tarefas, reduzir custos e apoiar decisões. Mas o uso dessas ferramentas também cria riscos jurídicos quando envolve dados pessoais, conteúdos protegidos por **direitos autorais** ou decisões que afetam funcionários e clientes.

A responsabilidade não depende apenas de quem desenvolveu a tecnologia. A forma como a organização utiliza os sistemas, supervisiona os resultados e protege as informações também pode ser relevante em uma disputa judicial.

Conheça o Pré-MBA em IA da Saint Paul e EXAME, com quatro aulas práticas, online, por R$ 37, e entenda como aplicar a inteligência artificial no ambiente profissional.

7 riscos jurídicos do uso de inteligência artificial nas empresas

1. Vazamento de dados pessoais

Inserir nomes de clientes, documentos, informações financeiras ou dados de funcionários em ferramentas de IA sem avaliar as condições de uso pode expor informações confidenciais.

A Lei Geral de Proteção de Dados (LGPD) estabelece regras para o tratamento de dados pessoais e exige medidas de segurança. Dependendo do caso, uma exposição indevida pode resultar em sanções administrativas e ações de pessoas afetadas.

2. Violação de **direitos autorais**

Textos, imagens, apresentações e campanhas produzidos com inteligência artificial podem reproduzir elementos protegidos por **direitos autorais** ou outros direitos de **propriedade intelectual**.

A **Organização Mundial da Propriedade Intelectual** (OMPI) destaca que a IA generativa levanta questões sobre o uso de obras no treinamento dos modelos e sobre a proteção dos conteúdos gerados.

Antes de publicar uma peça criada com IA, a empresa deve verificar se há elementos de terceiros e quais permissões são necessárias.

3. Discriminação em processos seletivos

Sistemas de IA podem auxiliar na triagem de currículos, na avaliação de candidatos e na gestão de funcionários. Se os critérios utilizados produzirem resultados discriminatórios, porém, a organização poderá enfrentar questionamentos jurídicos.

Um algoritmo que desfavorece candidatos por características associadas a gênero, idade ou raça, por exemplo, pode comprometer a igualdade de oportunidades.

A supervisão humana e a avaliação periódica dos critérios de seleção ajudam a identificar possíveis distorções antes que elas afetem decisões profissionais.

4. Decisões automatizadas sem transparência

A inteligência artificial pode ser usada para analisar crédito, definir perfis de consumidores ou apoiar decisões sobre trabalhadores. Quando o tratamento automatizado de dados pessoais afeta os interesses de alguém, a LGPD prevê o direito de solicitar a revisão da decisão e de obter informações sobre os critérios utilizados.

Isso significa que uma empresa precisa avaliar se consegue explicar como seus sistemas chegam a determinadas conclusões e como atende aos direitos dos titulares de dados.

Continuação: Sua empresa usa IA? 7 riscos jurídicos que podem acabar em processo

Entenda como identificar oportunidades e riscos no uso da inteligência artificial. O Pré-MBA em IA da Saint Paul e EXAME oferece quatro aulas práticas, online, por R$ 37.

5. Divulgação de informações confidenciais

Funcionários podem recorrer a ferramentas de IA para resumir relatórios, analisar contratos ou preparar apresentações. O problema surge quando compartilham informações estratégicas sem autorização ou sem conhecer as condições de armazenamento e utilização dos dados pela plataforma.

O risco inclui a exposição de segredos comerciais, estratégias de negócio e informações protegidas por contratos de confidencialidade.

Por isso, empresas precisam definir quais ferramentas podem ser usadas, que dados podem ser inseridos e quais informações devem permanecer em ambientes controlados.

6. Publicidade enganosa e informações falsas

Ferramentas generativas podem produzir informações incorretas, referências inexistentes e afirmações que não correspondem às características reais de um produto ou serviço.

Se uma empresa publica esse conteúdo sem verificação, pode enfrentar questionamentos relacionados à publicidade enganosa e à proteção do consumidor, conforme as circunstâncias.

Um exemplo é divulgar uma característica técnica que o produto não possui ou atribuir a um serviço resultados que não podem ser comprovados. A revisão humana antes da publicação reduz o risco de disseminar informações falsas.

7. Descumprimento de regras em outros países

Empresas que utilizam inteligência artificial em operações internacionais também precisam considerar as normas aplicáveis nos mercados em que atuam.

Na União Europeia, o Regulamento de Inteligência Artificial, conhecido como AI Act, estabelece obrigações e restrições conforme o tipo de sistema e o nível de risco. Há regras específicas para aplicações de alto risco, transparência e determinadas práticas proibidas.

Uma ferramenta utilizada para selecionar candidatos, por exemplo, pode estar sujeita a exigências diferentes das aplicáveis a um sistema que apenas auxilia na redação de textos. O alcance das obrigações depende do uso concreto e das regras vigentes.

Como reduzir os riscos jurídicos do uso de IA?

A prevenção começa com uma política interna que estabeleça ferramentas autorizadas, limites para o compartilhamento de dados e procedimentos de revisão dos resultados. Também é importante treinar os funcionários para reconhecer erros, proteger informações e identificar conteúdos que exijam verificação.

A empresa deve ainda documentar decisões relevantes, avaliar contratos com fornecedores e envolver as equipes jurídica, de segurança da informação e de recursos humanos nos casos de maior risco.

O uso de inteligência artificial não elimina as responsabilidades legais da empresa. Definir regras, supervisionar resultados e acompanhar mudanças na legislação são medidas importantes para aproveitar a tecnologia sem ignorar seus possíveis impactos jurídicos.

Aprenda a aplicar a inteligência artificial com mais segurança no trabalho. Faça o Pré-MBA em IA da Saint Paul e EXAME, com quatro aulas práticas, online, por R$ 37.

Brasil cai uma posição no ranking de inovação global



País é o segundo melhor colocado na América Latina; lista contempla 193 nações

A **Organização Mundial da Propriedade Intelectual** (OMPI) divulgou neste mês seu ranking anual sobre o nível de desenvolvimento e inovação de 139 países no mundo. Entre eles está que, neste ano, assumiu a posição de número 53 da tabela.

O relatório, conhecido como Global Innovation Index (GII), avalia a capacidade e o investimento em inovação de cada nação por meio de 79 indicadores. Em 2025 .

Na versão mais atualizada do GII, o País se tornou o segundo melhor classificado da América Latina e o sexto maior entre as economias de "renda média alta" - comumente conhecidas como "de segundo mundo".

A publicação do índice afirma que a evolução das Inteligências Artificiais afetou positivamente o financiamento de capital de risco e de gastos com pesquisa e desenvolvimento (P&D;).

Enquanto em 2025 o aumento no investimento do setor foi de 3,3%, em 2026, a

De acordo com o documento veiculado pela OMPI, é a única economia da região que inova acima do esperado para seu nível de desenvolvimento pelo sexto ano consecutivo.

Em toda a América Latina, fica atrás apenas do Chile, que ocupa a 51ª colocação do ranking.

Já entre os países de renda média alta, ele está abaixo apenas da Mauritânia (50°), Turquia (45), Tailândia (44), Malásia (34) e China (10).

No topo do ranking, a mudança diante do índice de 2025 é pequena, com alternância apenas entre o sétimo e o oitavo colocado. Sendo assim, em 2026, a ordem é a seguinte:

Suíça (1ª posição em 2025)

Suécia (2)

Estados Unidos da América (3)

República da Coreia (4)

Singapura (5)

Reino Unido (6)

Países Baixos (8)

Finlândia (7)

Dinamarca (9)

China (10)

Os doze últimos colocados fazem parte da África Subsaariana, sendo o menos inovador Chade, que somou apenas 9,5 pontos no índice.

O índice é medido desde 2007 e segue um método de avaliação com base no cálculo desse índice, medido a partir da soma de sete pilares. São eles: a confiança nas instituições de inovação; capital humano e pesquisa; infraestrutura; sofisticação do mercado; sofisticação empresarial; resultados de conhecimento e tecnologia; e resultados criativos.

A publicação levanta, também, as cem cidades consideradas os . Entre elas, há apenas uma cidade brasileira: São Paulo. A capital paulista ficou na 59ª colocação, com destaques para a Universidade de São Paulo (USP) e a Braskem.

Como a nova regulamentação pode impulsionar os estúdios de games brasileiros no mercado global



Como a nova regulamentação pode impulsionar os estúdios de games brasileiros no mercado global Decreto que detalha o Marco Legal dos Games prevê medidas de financiamento, formação profissional e divulgação de jogos nacionais

O Decreto nº 13.138/2026 regulamenta o Marco Legal dos Games , visando estimular o setor de games no Brasil com medidas de financiamento , formação profissional e promoção de jogos nacionais.

A Ancine propõe reduzir o valor mínimo de empréstimos e taxas de juros para facilitar o acesso ao crédito por estúdios independentes, embora o sucesso dependa das condições oferecidas.

O Game Brasil, uma plataforma pública, será criada para divulgar jogos nacionais, e uma rede nacional de formação profissional será estabelecida para fortalecer a indústria de games.

O sucesso das medidas depende de sua implementação e da capacidade de integrar desenvolvedores, investidores e distribuidores para aumentar a presença internacional dos jogos brasileiros.

Desenvolver um jogo eletrônico exige mais do que criatividade e conhecimento técnico. Para estúdios independentes, o processo envolve financiar meses ou anos de trabalho, formar equipes, conquistar espaço nas plataformas digitais e encontrar um público em um mercado disputado por empresas do mundo inteiro.

É nesse cenário que a regulamentação do Marco Legal dos Games pode abrir novas oportunidades para a indústria brasileira.

Em 14 de outubro, foi assinado o Decreto n.º 13.138/2026, que regulamenta a Lei n.º 14.852/2024 e estabelece diretrizes para estimular o desenvolvimento do setor, ampliar o acesso a mecanismos de fomento e fortalecer a presença dos jogos brasileiros no mercado internacional.

Entre as iniciativas previstas estão mudanças nas linhas de financiamento, ações de formação profissional e a criação de uma plataforma pública para divulgar produções nacionais.

Para Helon Junior, fundador da Hammock Studios, o potencial dessas medidas está na possibilidade de aproximar a capacidade criativa dos desenvolvedores brasileiros das condições necessárias para manter empresas competitivas.

"O país tem profissionais qualificados, capacidade criativa e um mercado consumidor expressivo, mas ainda enfrenta dificuldades para transformar esse potencial em empresas e produtos competitivos", avalia.

Financiamento é um dos principais desafios

Entre os obstáculos enfrentados pelos estúdios independentes está o acesso a recursos para financiar as diferentes etapas de produção. Um jogo pode exigir investimentos desde a criação do primeiro protótipo até os testes, o lançamento, o marketing e a distribuição, enquanto o retorno financeiro pode demorar anos para chegar.

Como parte das medidas anunciadas junto à regulamentação, a Agência Nacional do Cinema (Ancine) deverá propor ao Comitê Gestor do Fundo Setorial do Audiovisual (FSA) a redução do valor mínimo dos empréstimos de R$ 500 mil para R$ 150 mil.

A proposta também prevê diminuir os juros de Taxa Referencial (TR) mais 2% para TR, mais 0,5% ao ano. As mudanças dependem dos procedimentos de aprovação e implementação do fundo.

Na avaliação de Helon, facilitar o acesso ao crédito pode ajudar empresas menores, mas o resultado dependerá das condições oferecidas. Garantias exigidas, faturamento, prazos de pagamento e estágio de

Continuação: Como a nova regulamentação pode impulsionar os estúdios de games brasileiros no mercado global

desenvolvimento de cada projeto são fatores que influenciam a capacidade de um estúdio conseguir financiamento.

Uma equipe que está desenvolvendo seu primeiro protótipo, por exemplo, tem necessidades diferentes

das de uma empresa que já possui um jogo pronto

para chegar ao mercado. Por isso, o empreendedor defende instrumentos capazes de atender a diferentes etapas da produção.

O financiamento público, porém, não resolve sozinho o desafio de construir negócios duradouros. Para o fundador da Hammock Studios, também é necessário ampliar o interesse dos investidores privados pela indústria de games.

Segundo ele, o desenvolvimento de jogos envolve riscos criativos e comerciais, além de ciclos de produção longos. Por isso, investidores precisam compreender que o retorno de um projeto não se limita às vendas iniciais: uma **propriedade intelectual** pode gerar novas oportunidades por meio de sequências, licenciamento e distribuição em diferentes mercados.

Ter um bom jogo não garante sucesso

A competição internacional é outro desafio para os estúdios brasileiros. As plataformas digitais permitem que empresas de diferentes países lancem seus jogos para públicos globais, mas essa facilidade também aumenta a concorrência pela atenção dos jogadores.

"Desenvolver um bom produto não garante que ele será descoberto pelo público", afirma Helon.

Para ele, a estratégia comercial precisa fazer parte do planejamento desde o início do desenvolvimento. Conhecer o público, definir formas de monetização, planejar campanhas de marketing e estabelecer relações com distribuidoras e publishers internacionais são etapas importantes para que um jogo alcance jogadores além do mercado brasileiro.

A profissionalização da gestão também pesa nesse processo. Além de programadores, artistas e designers, um estúdio precisa organizar orçamento, cronograma, processos de produção e estratégias para explorar comercialmente suas criações.

Outro ponto é a **propriedade intelectual**. Criar personagens, universos e histórias próprias pode permitir que os estúdios desenvolvam produtos com potencial de expansão para outros jogos, produtos licenciados e diferentes formatos de entretenimento.

O Brasil conta com referências culturais que podem inspirar produções capazes de dialogar com públicos estrangeiros. Para Helon, o desafio é garantir que empresas brasileiras tenham condições de transformar esse repertório em propriedades intelectuais próprias e participar do valor econômico gerado por elas.

Divulgação e formação de profissionais

A regulamentação também prevê medidas voltadas à visibilidade dos jogos nacionais. Entre elas está o Game Brasil, plataforma pública e gratuita destinada a catalogar e divulgar jogos desenvolvidos no país, com informações sobre os criadores e os locais em que os títulos podem ser encontrados. A iniciativa busca facilitar o contato entre as produções brasileiras e o público.

A formação profissional aparece como outro eixo das medidas, com previsão de uma rede nacional de espaços voltados à formação, experimentação, pesquisa e desenvolvimento de jogos. A proposta é fortalecer a cadeia produtiva, aproximando a preparação de novos profissionais das necessidades do setor.

Na visão do fundador da Hammock Studios, a formação precisa caminhar junto com a criação de oportunidades de trabalho. O Brasil já tem profissionais qualificados que participam de grandes produções internacionais, mas precisa ampliar a capacidade de desenvolver projetos de maior porte dentro do próprio país.

Isso exige empresas capazes de contratar equipes, manter projetos em andamento e oferecer perspectivas de carreira em áreas que vão além da programação, como produção, gestão, marketing e desenvolvimento de negócios.

O impacto das novas medidas dependerá, portanto, de sua implementação e da capacidade de alcançar empresas de diferentes tamanhos.

Crescimento dos estúdios, geração de empregos qualificados, aumento do faturamento e maior presença internacional estão entre os indicadores que podem ajudar a avaliar os resultados ao longo do tempo.

Para a indústria brasileira, o desafio não é apenas criar jogos de qualidade, mas construir condições para que esses projetos encontrem financiamento,

Continuação: Como a nova regulamentação pode impulsionar os estúdios de games brasileiros no mercado global

conquistem jogadores e se transformem em negócios sustentáveis.

A regulamentação estabelece novas possibilidades para esse caminho, enquanto a execução das medidas e a capacidade de articulação entre desenvolvedores, investidores e distribuidores serão determinantes para ampliar a participação do Brasil no mercado global.

Search Box Busque no R7 Brasil Financiamento Games Indústria Marketing

âPara saber tudo do mundo dos famosos, siga o canal de entretenimento do R7, o portal de notícias

da Record, no WhatsApp

Engenharia reversa de IA: propriedade e responsabilidade



Engenharia reversa pode ser definida como processo de analisar sistema para identificar seus componentes e relações existentes entre eles

Opinião

A engenharia reversa pode ser definida como o processo de analisar um sistema para identificar seus componentes e as relações existentes entre eles, de modo a criar representações desse sistema em outra forma ou em um nível mais elevado de abstração [1]. Em termos mais diretos, cuida-se de extrair conhecimento ou saber técnico a partir de um artefato produzido pelo ser humano [2], percorrendo o caminho inverso ao da criação, do produto acabado à lógica que o originou, sem que se disponha do projeto ou do código original. Longe de constituir mera curiosidade técnica, a prática cumpre funções socialmente valiosas, que vão da garantia de interoperabilidade entre sistemas à identificação de falhas de segurança, passando pelo estudo acadêmico e pelo estímulo à concorrência e à inovação.

Essa importância se intensifica com a expansão dos sistemas de inteligência artificial, cuja presença no cotidiano econômico e social cresce em ritmo acelerado [3]. Modelos cujo funcionamento permanece opaco até mesmo para quem os desenvolve passam a ser objeto de investigação, reprodução e exploração por terceiros. É nesse ponto que a engenharia reversa se converte em problema jurídico de dupla face. De um lado, projeta-se sobre a **propriedade intelectual**, pois tangencia a tênue fronteira que separa compreender uma tecnologia de dela se apropriar indevidamente. De outro, projeta-se sobre a responsabilidade civil, na medida em que a reconstrução de um sistema pode originar aplicações derivadas capazes de causar danos a terceiros.

O problema jurídico, portanto, não está em qualificar a engenharia reversa como atividade necessariamente lícita ou ilícita, mas em estabelecer critérios que distingam a análise legítima de uma tecnologia das condutas que ultrapassam os limites juridicamente admissíveis. A mesma técnica capaz de viabilizar a compatibilidade e a correção de vulnerabilidades pode servir à violação de segredos empresariais, ao descumprimento de obrigações contratuais e à criação de ferramentas aptas a lesar interesses alheios. O juízo jurídico, por isso, não deve recair apena sobre a técnica em si, mas sobre a finalidade perseguida, os meios empregados e os direitos atingidos. Compreender o funcionamento de um programa não autoriza a reprodução de elementos protegidos, assim como os interesses econômicos do titular não bastam para transformar toda investigação independente em conduta reprovável.

Proteção de ideias, obras literárias e combate à concorrência desleal

No ordenamento brasileiro, essa avaliação pode envolver, conforme o objeto analisado, a Lei de Direitos Autorais (Lei 9.610/98), a Lei do Software (Lei 9.609/98) e a Lei de **Propriedade Industrial** (Lei 9.279/96). A Lei do Software confere ao programa de computador a tutela própria das obras literárias [4], protegendo a forma de expressão do código, e não as funcionalidades que ele realiza. A Lei de Direitos Autorais caminha na mesma direção ao excluir expressamente de sua proteção as ideias, os procedimentos, os métodos e os sistemas como tais [5]. A Lei de **Propriedade Industrial**, por sua vez, reprime a concorrência desleal e a exploração indevida de segredos de negócio [6]. A resposta jurídica depende, assim, do bem protegido por cada regime, dos meios utilizados e dos interesses envolvidos, não havendo qualificação única e predeterminada para a engenharia reversa.

A tutela conferida ao programa de computador, portanto, não impede o estudo de seu comportamento externo nem a construção independente de soluções que cumpram funções equivalentes. A fronteira entre a análise permitida e a cópia vedada situa-se na distinção entre a ideia e a expressão, linha tênue e casuística que o intérprete precisa percorrer antes de afirmar que determinada reconstrução configura ilícito.

Inteligência artificial amplia riscos de violação de direitos

É na inteligência artificial, entretanto, que essa engenharia de regimes revela a sua maior tensão. Semelhança funcional não equivale, de forma automática, à violação de direito autoral, assim como a magnitude do investimento realizado não gera, por si só, exclusividade sobre a ideia, o método ou a funcionalidade envolvidos. Há situações em que a prática apenas evidencia um limite inerente ao sistema de exclusividade, e outras em que efetivamente o tensiona. É o que se observa na disponibilização de jogos e programas reconstruídos a partir de seus originais, cuja semelhança substancial pode configurar violação de direitos ou mesmo concorrência desleal, sobretudo quando o resultado se vale do investimento alheio para competir no mesmo mercado.

Esse risco tornou-se mais tangível com as ferramentas de inteligência artificial voltadas à programação, capazes de automatizar etapas de engenharia reversa e de descompilação, a ponto de já existirem soluções que acoplam assistentes de código a jogos para produzir alterações customizadas de forma quase automatizada [7]. Não se trata de hipótese nova, já que a reconstrução de títulos como Super Mario 64, Grand Theft Auto III e Zelda: Ocarina of Time já rendeu versões adaptadas disponibilizados na internet e reações dos titulares [8]. Soma-se a isso a opacidade algorítmica, a dificuldade de compreender como a própria máquina chega aos seus resultados [9], que converte a investigação técnica, muitas vezes, na única via capaz de explicar, depois do dano, como ele ocorreu.

Responsabilidade civil avalia abuso de direito

Sob a perspectiva da responsabilidade civil, os artigos 186, 187 e 927 do Código Civil oferecem os parâmetros para examinar a ilicitude, o abuso de direito e o dever de reparar [10]. Sua aplicação, todavia, exige a identificação concreta dos pressupostos pertinentes, sem que a simples utilização da técnica seja convertida em fundamento automático de indenização. Importam a conduta efetivamente praticada, os direitos atingidos e a relação entre o comportamento do agente e o resultado lesivo.

Esse exame é complexo diante das cadeias tecnológicas que a inteligência artificial costuma formar. Uma pessoa pode realizar a engenharia reversa de um modelo; outra, desenvolver uma aplicação a partir dos resultados obtidos; e uma terceira, colocá-la em circulação ou dela extrair finalidade diversa. A mera sucessão cronológica de intervenções não estabelece, por si só, o nexo causal, e a contribuição técnica em determinada etapa não acarreta responsabilidade por todos os danos subsequentes, pois entre a investigação e o prejuízo final podem existir decisões autônomas de desenvolvimento, comercialização e uso.

É nesse ponto que a chamada ingerência tecnológica, compreendida como o controle material, cognitivo e operacional efetivamente exercido sobre o sistema de inteligência artificial, apresenta-se como perspectiva a explorar para a imputação, do desenvolvedor que define os parâmetros ao agente que coloca o sistema em operação [11]. Transposto para a engenharia reversa, o enfoque poderia auxiliar a localizar, dentro da cadeia, quem detinha o domínio sobre a etapa geradora do dano, sem conduzir nem à responsabilização automática de quem apenas compreendeu uma tecnologia, nem à impunidade de quem, controlando o sistema derivado, negligenciou os deveres que lhe eram exigíveis.

Esse enfoque é relevante porque a vítima, na maioria das vezes, não dispõe de capacidade técnica para reconstituir a origem do dano nem para demonstrar qual elo da cadeia o produziu. Daí a pertinência da distribuição dinâmica do ônus da prova prevista no artigo 373, §1º, do CPC [12] e da inversão prevista no artigo 6º, inciso VIII, do CDC [13], instrumentos cuja projeção sobre danos relacionados à inteligência artificial é expressamente contemplada em propostas legislativas em tramitação [14]. Fazer recair o encargo probatório sobre quem detém o controle técnico do sistema tende a prestigiar a paridade de armas diante da assimetria informacional inerente a essas relações.

Deveres de conduta para corrigir vulnerabilidades

Ademais, a responsabilidade civil não cumpre aqui apenas função reparatória. Sua dimensão preventiva impõe deveres de conduta que antecedem o dano, como corrigir vulnerabilidades conhecidas, informar riscos e interromper usos perigosos. A engenharia reversa voltada à descoberta de falhas pode ser socialmente útil quando orientada à correção, e juridicamente censurável quando empregada para explorar a vulnerabilidade descoberta. O mesmo vale para a reprodução de funcionalidades que viabilizem fraudes, falsificações ou conteúdos lesivos. O divisor não está apenas na técnica, mas na finalidade e nos deveres observados por cada agente.

A engenharia reversa, assim, não opera como presunção absoluta de ilicitude nem como escudo contra a responsabilidade civil. Ela evidencia os limites dos modelos tradicionais de exclusividade, sem suprimir a tutela dos ativos intelectuais ou das pessoas lesadas, subsistindo o dever de indenizar sempre que a conduta, os meios empregados e os resultados o justifiquem.

Mais do que indagar se a investigação técnica é permitida em tese, o tema desafia a delimitação dos direitos de exclusividade e a atribuição de responsabilidade em cadeias tecnológicas complexas. A ingerência tecnológica desponta, nesse horizonte, como uma perspectiva possível, entre outras, para orientar a identificação dos deveres de conduta e da eventual contribuição de cada agente com o ato. Ao redirecionar o foco da rejeição genérica à técnica para a governança real do risco e o enfrentamento das assimetrias probatórias, abre-se espaço para equilibrar a liberdade de inovar, a proteção da **propriedade intelectual** e a justa reparação das vítimas, oferecendo balizas mais seguras tanto na estruturação preventiva dos contratos quanto na condução de eventuais disputas judiciais.

[1] CHIKOFSKY, Elliot J.; CROSS II, James H. Reverse engineering and design recovery: a taxonomy. IEEE Software, v. 7, n. 1, 1990, p. 13-17.

[2] SAMUELSON, Pamela; SCOTCHMER, Suzanne. The law and economics of reverse engineering. Yale Law Journal, v. 111, 2002, p. 1577.

[3] Sobre a expansão e a relevância econômica da inteligência artificial, cf. STANFORD UNIVERSITY. AI Index Report 2025. Stanford: Institute for Human-Centered Artificial Intelligence, 2025; e GROSSMANN, Luís Osvaldo. Brasil salta de 35º para 16º em ranking de inteligência artificial: talento e IA responsável puxam. In: Convergência Digital. Disponível aqui.

[4] Art. 2º, Lei 9.609. O regime de proteção à **propriedade intelectual** de programa de computador é o conferido às obras literárias pela legislação de direitos autorais e conexos vigentes no País, observado o disposto nesta Lei.

[5] Art. 8º, Lei 9.610. Não são objeto de proteção como direitos autorais de que trata esta Lei:

I - as idéias, procedimentos normativos, sistemas, métodos, projetos ou conceitos matemáticos como tais;

[6] Art. 195, Lei 9.279. Comete crime de concorrência desleal quem: ( )

XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

[7] Cf. UNIVERSAL-MODDER. Point Claude at any game: skills, tools and the fal MCP that let Claude Code mod almost any PC game you own. GitHub, 2026. Disponível aqui. Acesso em: 12/10/2026; e ALPHASIGNAL. Universal Modder lets Claude Code build playable game mods automatically. AlphaSignal, 30 set. 2026. Disponível aqui. Acesso em: 12/10/2026. Registre-se que, segundo seus idealizadores, tais ferramentas não distribuem os arquivos do jogo nem o código descompilado, limitando-se a gerar modificações e conversores.

[8] Cf., respectivamente, Nintendo lawyers file copyright complaints against Super Mario 64 PC port (TorrentFreak, 8 maio 2020, aqui); Take-Two Is Suing Reverse-Engineered GTA 3 and Vice City Fan Project Creators (IGN, 2021, aqui); e Ocarina of Time's source code has been reverse engineered (Kotaku, 2022, aqui). Acesso em: 12/10/2026.

[9] Nesse sentido: LU, Sylvia. Algorithmic opacity, private accountability, and corporate social disclosure in the age of artificial intelligence. Vand. J. Ent. & Tech. L., v. 23, 2020, p. 114; e BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. Big data & society, v. 3, n. 1, 2016, p. 4.

[10] Destaca-se o parágrafo único do art. 927: "Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem".

[11] FLUMIGNAN, Wévertton Gabriel Gomes. Responsabilidade civil e inteligência artificial: a ingerência tecnológica como critério de imputação. In: ConJur, 22 jan. 2026. Disponível aqui. Acesso em: 12/10/2026.

[12] Art. 373, §1º, CPC. Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada ( ).

[13] Art. 6º, VIII, CDC. São direitos básicos do consumidor: ( )

VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências.

[14] Art. 37, PL nº 2.338/2023. O juiz inverterá o ônus da prova quando a vítima for hipossuficiente ou quando as características de funcionamento do sistema de IA tornarem excessivamente oneroso para a vítima provar os requisitos da responsabilidade civil.

Índice remissivo de assuntos

Denominação de Origem 3,4
Direitos Autorais 5,6
Entidades 5,6,7
Marco regulatório | INPI 3,4
Propriedade Industrial 3,4,11,12,13,14
Propriedade Intelectual 1,2,5,6,7,8,9,10,11,12,13,14