



Direito,
Inovação
& Tecnologia

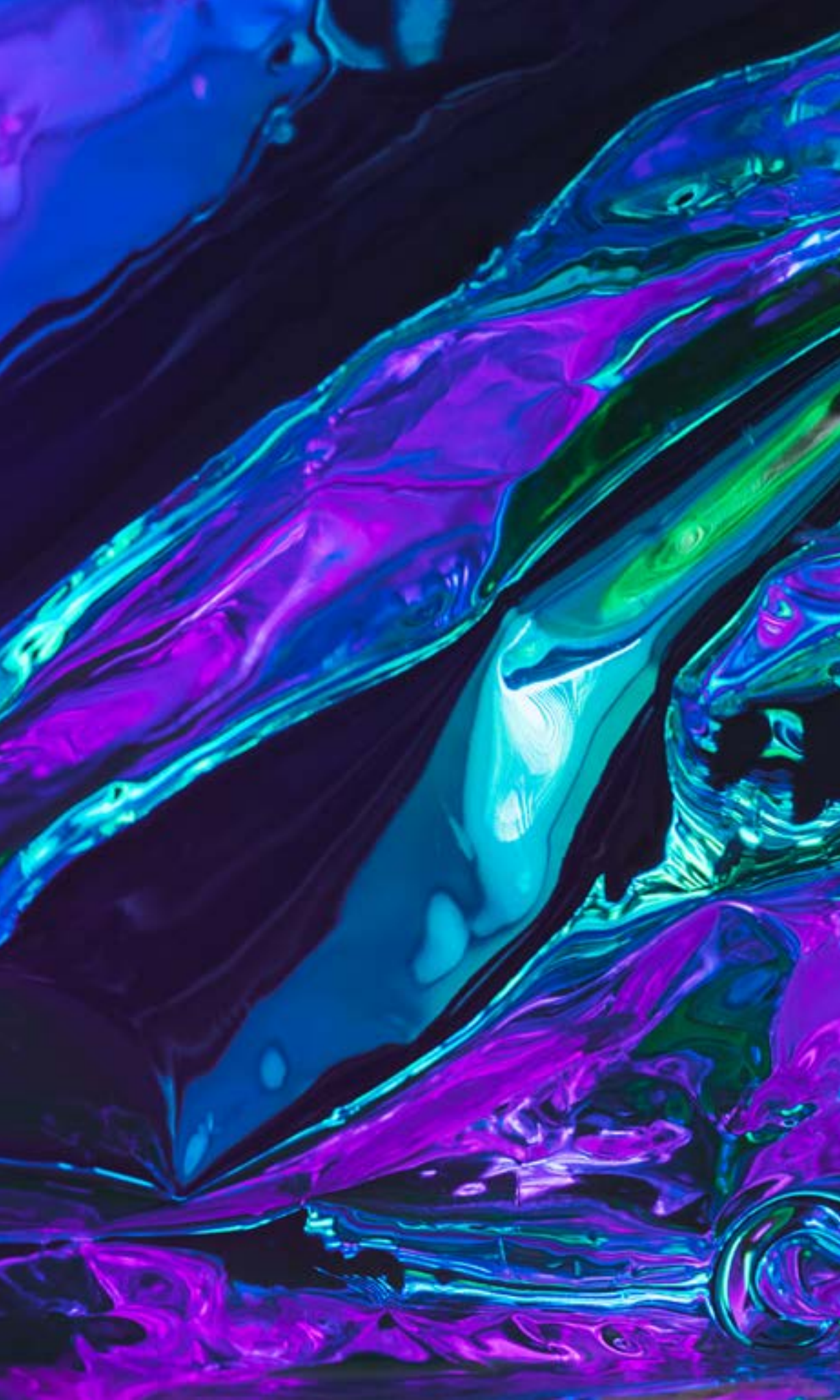
O FUTURO DO DIREITO DIGITAL

*E os impactos causados pelas
tendências de Inovação e Tecnologia*

WWW.VLKLAW.COM.BR

SUMÁRIO

INTRODUÇÃO	3
1. Modelos de Linguagem Pequenos (SLMs)	4
2. Large Action Models/Agentic AI	6
3. Segurança Cibernética e IA na Ciberdefesa	8
4. Deepfakes e Manipulação de Informação.....	9
5.Computação Quântica e Crise da Criptografia	10
6. Privacidade Biométrica e Monitoramento Contínuo	11
7. Cibersegurança para Infraestrutura Crítica.....	12
8. Anúncio ou diversão?	13
9. Web3 e a Economia de Criadores	14
10. Hiperpersonalização e IA Generativa para Marketing ...	16
CONCLUSÃO	18
SOBRE NÓS.....	19



INTRODUÇÃO

O cenário tecnológico e regulatório está em constante evolução, impulsionado por inovações como Inteligência Artificial (IA), computação quântica e a crescente preocupação com a privacidade e segurança de dados. Este material, elaborado pelo VLK Advogados com base nos principais relatórios de tendências no cenário internacional¹, apresenta as oportunidades de inovação estratégicas mais relevantes para o mercado.

Analizamos, de forma objetiva, como essas tendências podem impactar as áreas de Direito Digital, Segurança Cibernética, Inteligência Artificial, Proteção de Dados Pessoais e Legal Marketing, oferecendo insights sobre os aspectos regulatórios e de mitigação de riscos.

1- 2025 Tech Trends Report, Future Today Institute.

https://ftsg.com/wp-content/uploads/2025/03/FTSG_2025_TR_FINAL_LINKED.pdf

2025 Top Strategic Technology Trends, Gartner. Disponível para download em

<https://www.gartner.com/en/articles/top-technology-trends-2025>

Marketing Trends 2025, Kantar. Disponível para download em

<https://www.kantar.com/brazil/inspiration/marcas/10-tendencias-de-marketing-para-2025>

1. Modelos de Linguagem Pequenos (SLMs)



Modelos de Linguagem Pequenos (SLMs) podem igualar ou até superar a performance de seus equivalentes maiores em tarefas específicas, exigindo significativamente menor poder computacional e recursos. Ao operarem on-device, eles oferecem maior eficiência energética, melhoram a proteção e privacidade dos dados e reduzem a necessidade de recursos computacionais sem necessariamente comprometer a eficácia.

Uma perspectiva corroborada pela AEPD (Autoridade de Proteção de Dados espanhola) mostra que, muitas vezes, usar métodos bem planejados funciona melhor do que apostar em modelos de inteligência artificial muito complexos². Em um teste para identificar casos de sobre peso com base apenas na altura e no peso, um modelo simples acertou bem com apenas três exemplos de boa qualidade — mesmo que esses exemplos

fossem gerados artificialmente. Isso aconteceu porque há uma relação quase direta entre altura e peso, o que facilita o trabalho da IA. Por outro lado, modelos mais sofisticados, quando não têm nenhum conhecimento prévio, precisam de muitos dados para aprender sozinhos e podem cometer erros graves até entender como essas variáveis se relacionam.

Esse método otimiza recursos, reforça a minimização de dados e atende à proteção de dados desde o design, elementos fundamentais em normas como o General Data Protection Regulation (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil.

IMPACTOS JURÍDICOS

- **Princípio da Minimização e Segurança:** processamento on device e o uso de menos dados (ou dados sintéticos) pode reduzir o impacto e os

riscos de vazamento de informações, facilitando a conformidade com legislações como LGPD e GDPR, mediante o atendimento aos princípios de minimização e segurança.

- **Accountability:** a adoção de metodologias maduras de desenvolvimento exige maior transparência e documentação sobre estrutura de IA, amostragem de dados e critérios de treinamento. Isso assegura bases legais sólidas para o tratamento de dados, em linha com requisitos de accountability.
- **Propriedade Intelectual:** questões relativas ao uso de bases de dados protegidas no treinamento dos modelos exigem análise detalhada de contratos e acordos de licenciamento.
- **Responsabilidade Proativa:** a incorporação de conhecimento prévio no design do modelo fortalece

2- "Datos e información en Inteligencia Artificial". Disponível em: <https://www.aepd.es/prensa-y-comunicacion/blog/datos-e-informacion-en-inteligencia-artificial>. Acesso em: 26/03/2025.



a responsabilidade proativa – demonstra que, além de cumprir as normas de proteção de dados, a empresa adota medidas para prevenir violações. Essa prática otimiza recursos, reduzindo potenciais riscos (como as “alucinações” de modelos complexos) e aumentando a segurança nos resultados.

- **Idoneidade do Tratamento:** modelos que precisam de grande volume de dados podem ser inadequados em certas situações, seja por escassez ou ilegítima coleta. Nesse cenário, a escolha de uma arquitetura simples pode ser uma alternativa viável para o cumprimento dos princípios como necessidade e proporcionalidade.

VISÃO VLK:

- Realizar auditorias e avaliações dos processos de tratamento de dados, identificando e mitigando vulnerabilidades.
- Avaliar a real necessidade de informações para treinamentos de IA considerando formatos sintéticos e limitando a coleta a dados estritamente relevantes.
- Elaborar e revisar contratos e políticas internas, incorporando cláusulas específicas para o uso de IA com ênfase na proteção de dados e na propriedade intelectual.
- Implantar mecanismos de governança e *accountability* que garantam a conformidade com as normas de proteção de dados e os princípios de minimização e exatidão, bem como mecanismos para detecção e correção de falhas (inclusive “alucinações”).
- Capacitar equipes com treinamentos específicos sobre metodologias maduras de desenvolvimento e análise de dados, alinhados aos preceitos de responsabilidade proativa e proteção de dados desde o design.

2. Large Action Models/Agentic AI



Os Large Action Models (LAMs) representam uma categoria de inteligência artificial que vai além da simples geração de conteúdos, pois desenvolve a capacidade de antecipar e executar ações no mundo real e são a próxima geração de sistemas de IA que revolucionará os negócios e a sociedade.

Esses sistemas monitoram os comportamentos humanos através de sensores e, com base nessas observações, aprendem a executar tarefas complexas com decisões tomadas em tempo real.

Com o aumento dos dispositivos conectados, esses modelos terão acesso a um volume significativo de dados que lhes permitirá operar de forma autônoma. Em breve, os Personal Large Action Models (PLAMs) poderão

conhecer profundamente as preferências individuais, realizando atividades como agendar reuniões ou efetuar compras. A inteligência artificial "agentic" vai ainda mais longe, estabelecendo seus próprios objetivos e tomando decisões complexas com o intuito de oferecer suporte efetivo às pessoas.

De acordo com o Gartner, é estimado que em 2028 ao menos 15% das decisões das atividades de dia a dia serão realizadas mediante soluções de Agentic AI³.

IMPACTOS JURÍDICOS

- **Cibersegurança:** por terem acesso ampliado a sistemas externos, agentes de IA estão mais expostos a falhas como manipulação de memória, vulnerabilidades em integrações e falhas em ambientes com vários

agentes, o que aumenta o risco de ataques graves.

- **Interações entre agentes:** agentes podem colaborar, competir ou entrar em conflito entre si, gerando dinâmicas imprevisíveis. Isso abre espaço para efeitos em cascata, colusões e novas superfícies de ataque.
- **Capacidade de governar outros sistemas:** Devido à sua persistência e capacidade de coordenação, agentes podem ser usados para monitorar e controlar outros agentes, ajudando a aplicar regras ou mitigar riscos em larga escala.
- **Responsabilidade civil:** se um agente autônomo gera dano, discute-se a responsabilidade do desenvolvedor ou de quem contrata o serviço.

- **Privacidade e Proteção de Dados:** LAMs requerem amplo acesso ao ambiente digital do usuário, o que pode conflitar com princípios de minimização de dados.
- **Contratos eletrônicos:** atos praticados por agentes autônomos exigem previsão contratual.
- **Revisão humana (LGPD, art. 20):** decisões automatizadas que afetem direitos do titular devem permitir contestação.
- **Acidentes e perda de controle:** agentes de IA podem cometer erros simples (como respostas erradas), mas também causar situações graves, em que humanos perdem a capacidade de entender, corrigir ou retomar o controle do sistema. Isso inclui riscos como agentes que se replicam sozinhos ou que perseguem objetivos contrários aos interesses humanos.
- **Transparência e Explicabilidade:** desafios na compreensão e documentação dos processos decisórios da IA, que podem afetar a confiança dos usuários e a conformidade com regulamentações.

VISÃO VLK

- Um dos principais desafios é avaliar melhor o desempenho dos agentes e os riscos associados ao seu uso ao longo do tempo, especialmente à medida que se tornam mais autônomos, integram infraestruturas críticas e influenciam decisões de alto impacto.
- Modelagem de ameaças: Elaborar análises detalhadas de risco que levem em conta a evolução das capacidades dos agentes — como o que muda se um agente ganhar acesso a contas bancárias, por exemplo.
- Estabelecer frameworks internos para governança de IA, com comitês de ética e processos de auditoria contínua.
- Desenvolver políticas de transparência que detalhem os algoritmos e processos decisórios, facilitando a explicabilidade e a conformidade regulatória.
- Contratos robustos com cláusulas de responsabilidade e deveres do provedor.
- Oferecer capacitação especializada para equipes técnicas e jurídicas, assegurando a gestão adequada dos riscos emergentes.

3. Segurança Cibernética e IA na Ciberdefesa

Na segurança cibernética, a inteligência artificial pode desempenhar papéis opostos. Por um lado, ela fortalece as defesas ao monitorar transações blockchain e identificar anomalias, encontrar vulnerabilidades em contratos, monitorar tráfego de rede, agilizar respostas a incidentes etc.

Por outro, agentes maliciosos utilizam IA para criar malwares sofisticados, gerar e-mails de phishing convincentes, clonagem de vozes e coordenar ataques automatizados, intensificando o cenário de ameaças digitais. Por isso, as estratégias de defesa deverão se tornar cada vez mais proativas e inteligentes para antecipar e combater os novos ataques.

VISÃO VLK

- Monitorar inputs maliciosos, como injeções de prompts, e outputs contendo dados sensíveis.
- Implementar soluções de segurança de IA que possam detectar e responder a ataques específicos, como envenenamento de dados, evasão de modelo e extração de modelo.
- Implementar planos robustos de resposta a incidentes e auditorias de cibersegurança voltados para IA.
- Adequar práticas de segurança aos padrões regulatórios atuais e emergentes.
- Atualizar e revisar políticas internas de proteção de dados, alinhando-as aos padrões internacionais e exigências regulatórias.
- Revisar contratos com provedores de segurança especialmente quanto às cláusulas de responsabilidade.

IMPACTOS JURÍDICOS:

- **Conformidade e Regulamentação:** exigência de alinhamento com normas de segurança cibernética e proteção de dados, já que falhas podem resultar em impactos legais e regulatórios. No futuro, melhores práticas podem exigir o uso de IA de defesa como parte do estado da técnica em segurança.
- **Responsabilidade Civil:** ampliação dos riscos de danos decorrentes de ataques cibernéticos, com potenciais multas e indenizações que podem afetar significativamente as operações.
- **Litígios Estratégicos:** possibilidade de disputas judiciais em casos de falhas na segurança, especialmente quando há omissão na adoção de medidas preventivas adequadas.

4. Deepfakes e Manipulação de Informação

O avanço dos deepfakes evidencia o potencial da IA em criar conteúdos altamente realistas e cada vez mais indistinguíveis da realidade, substituindo Ados envolvidos. Essa tecnologia, apesar de suas aplicações positivas, acarreta riscos significativos, como a manipulação da opinião pública, fraudes e a disseminação de desinformação.

A capacidade de produzir conteúdos fraudulentos de forma rápida, amplamente acessível e convincente traz desafios éticos e jurídicos relevantes, sobretudo no que tange à proteção aos direitos de personalidade e integridade das comunicações.

A partir desse cenário, empresas tem adotado estratégias de "Segurança à Desinformação" que combina frentes como detecção de deepfake, prevenção de falsificação de identidade a partir da comparação com perfil comportamental da pessoa-alvo e monitoramento de conteúdo prejudicial à reputação.

IMPACTOS JURÍDICOS

- **Direito Penal:** produção e divulgação de deepfakes podem configurar crimes de calúnia, fraude, estelionato e de violência psicológica contra a mulher.
- **Violação de Direitos Autorais e de Personalidade:** a criação e a disseminação de mídia sintética sem autorização podem infringir direitos autorais e direitos de personalidade, acarretando no dever de indenizar.
- **Desinformação e Manipulação:** *deepfakes* podem ser utilizados para disseminar desinformação e agravar

situações de polarização, tal como tem ocorrido na política ao redor do mundo, com potenciais implicações legais.

- **Responsabilidade de Plataformas:** a responsabilidade das plataformas online na identificação e remoção de deepfakes e mídias sintéticas prejudiciais é uma questão jurídica em evolução.
- **Direito Eleitoral:** deepfakes podem influenciar eleições, exigindo medidas rápidas de remoção.

VISÃO VLK

- Implementar ferramentas de monitoramento e verificação da autenticidade de conteúdos digitais.
- Desenvolver estratégias de gestão de crise e resposta rápida a deepfakes difamatórios.
- Elaborar políticas contratuais específicas e mecanismos de reparação para casos de uso indevido de imagem e manipulação de informação.

5. Computação Quântica e Crise da Criptografia



A computação quântica permite fazer cálculos muito rápidos e complexos e especialistas preveem a possibilidade da ineficácia da criptografia que usamos hoje frente a esse contexto. De acordo com o Gartner, "até o ano de 2029 os avanços na computação quântica tornarão a maioria das criptografias assimétricas convencionais inseguras para uso"⁴.

Assim, dado que os computadores quânticos poderão, em um futuro breve, ser capazes de quebrar as "chaves" de segurança que protegem nossas informações, cientistas já trabalham para criar uma criptografia que seja resistente a tais computadores, garantindo a segurança das nossas comunicações e transações digitais.

IMPACTOS JURÍDICOS:

- **Riscos de Exposição de Dados:** se os sistemas atuais forem ultrapassados, informações sigilosas e dados pessoais sensíveis poderão ser decriptados, acarretando violações da LGPD, do GDPR, de confidencialidade e segredo de negócios.
- **Responsabilidade Civil:** contratos de serviços em nuvem poderão ser questionados se não incluam

medidas e cláusulas de atualização tecnológica contínua.

- **Adequação Regulatória:** setores críticos poderão ser obrigados a atualizar os protocolos e normas para incluir padrões mais avançados de segurança, mitigando riscos legais e reputacionais.

VISÃO VLK:

- Conduzir assessments em infraestrutura de segurança para mapear a robustez dos sistemas de criptografia e identificar necessidades de migração para novas soluções.
- Revisão de contratos de fornecedores críticos, incluindo cláusulas de "crypto agility", ou seja, a capacidade dos sistemas de alternar de forma rápida e eficiente os mecanismos de criptografia.
- Desenvolver planos de contingência e relatórios de impacto para proteção de dados, demonstrando *accountability*.

6. Privacidade Biométrica e Monitoramento Contínuo



Tecnologias de reconhecimento facial e coleta de dados biométricos estão em expansão, sendo usadas para prever comportamento humano com aplicações relacionadas a hábito de consumo ou até mesmo identificar orientação política.

Alguns países investem muito em sistemas de vigilância com IA e vendem essa tecnologia para outros, o que pode ser usado para censurar ou oprimir as pessoas. Com isso, cresce a preocupação regulatória: o AI Act, na União Europeia, em algumas circunstâncias, classifica esse tipo de sistema de IA como de Risco Inaceitável, proibindo a identificação biométrica em tempo real em espaços públicos na maioria dos casos bem como em ambientes de trabalho e instituições de ensino.

VISÃO VLK:

- Estruturar políticas rigorosas para a coleta e o tratamento de dados biométricos, priorizando a anonimização e a minimização dos riscos.
- Avaliações de Impacto Algorítmico para sistemas de IA que processem dados biométricos.
- Adequar os processos internos às exigências legais e às melhores práticas internacionais, realizando auditorias periódicas e atualizando os protocolos de segurança.

IMPACTOS JURÍDICOS:

- **Violação de Direitos Fundamentais:** risco elevado de invasão de privacidade, com implicações diretas sobre os direitos à intimidade e à proteção de dados pessoais.
- **Desafios de Conformidade:** necessidade de garantir que o uso de dados biométricos esteja estritamente alinhado às normas legais, como a LGPD e o GDPR, que exigem base legal específica, sob pena de sanções.
- **Responsabilidade e Litígios:** potencial para disputas judiciais em casos de tratamento inadequado ou uso indevido de informações sensíveis, exigindo medidas de segurança robustas.
- **Discriminação e Vieses:** sistemas de reconhecimento facial podem apresentar taxas de erro maiores para grupos minoritários.

7. Cibersegurança para Infraestrutura Crítica

No EU AI Act, IAs que operam em infraestruturas críticas são consideradas de alto risco, e não é à toa. A cibersegurança para infraestruturas críticas enfrenta ameaças cada vez mais sofisticadas, que vão desde biohacking – com o uso de DNA sintético para injetar malwares em pipelines de sequenciamento – até ataques de ransomware direcionados a sistemas industriais, exemplificados por incidentes em plantas bioenergéticas, redes de energia elétrica e sistemas de tratamento e distribuição de água.

Esses riscos, intensificados por fatores geopolíticos e ações de atores estatais, afetam setores como saúde e os data centers de empresas de IA comprometendo a segurança de informações sensíveis.

Em resposta, cresce a necessidade de reforçar as defesas em toda a cadeia, com protocolos rigorosos de criptografia, verificação de identidade e gerenciamento de riscos, garantindo uma supervisão humana constante e uma abordagem proativa para proteger esses ambientes interconectados.

IMPACTOS JURÍDICOS:

- **Interrupção de Serviços e Danos Econômicos:** falhas de segurança podem levar à interrupção de operações essenciais como o fornecimento de água e energia, gerando perdas financeiras substanciais e danos à reputação corporativa.
- **Responsabilidade Civil:** a ineficácia na proteção de infraestruturas críticas pode resultar em sanções severas, indenizações e responsabilização civil.
- **Compliance e Regulamentação:** a necessidade de cumprir com normas rigorosas de cibersegurança existentes e emergentes, nacionais e internacionais, impõe a revisão constante de políticas e protocolos internos.

VISÃO VLK:

- Desenvolver e implementar planos de cibersegurança específicos para infraestruturas críticas, com foco em prevenção, detecção e resposta a incidentes.
- Realizar auditorias regulares e avaliações de risco para identificar vulnerabilidades e adotar medidas corretivas.
- Revisão de contratos de tecnologia operacional, incluindo disposições de segurança.

8. Anúncio ou diversão?

O setor de publicidade está se reinventando para se aproximar cada vez mais do universo do entretenimento, dado o desafio crescente de engajamento para os conteúdos de marca numa sociedade digital acometida por um verdadeiro dilúvio de informações. Isso significa usar formatos originais e interessantes que dialoguem com o que as pessoas já gostam de assistir, escutar ou ler.

A inteligência artificial é uma grande aliada neste contexto, pois permite criar anúncios mais personalizados e direcionados para cada pessoa. Além disso, as empresas estão explorando oportunidades em inserir suas marcas e serviços em contextos como games imersivos, coproduções cinematográficas, conteúdos para fast TV ou até mesmo patrocinar a realização de novelas em redes sociais.

As empresas perceberam que, se o conteúdo tiver natureza de entretenimento, as pessoas terão uma conexão mais profunda com a marca,

transcendendo a relação meramente transacional/comercial.

IMPACTOS JURÍDICOS

- **Transparência:** a Lei 8.078/90 (CDC) e as regras de autorregulamentação publicitária do CONAR (Conselho Nacional de Autorregulamentação Publicitária) exigem indicação clara quando houver conteúdo publicitário. A ausência de ostensividade pode configurar publicidade abusiva e antiética. Contratos com criadores de conteúdo devem prever obrigação de rotular publis e patrocínios, evitando práticas enganosas ou abusivas (principalmente para público infantil).
- **Responsabilidade solidária:** ainda que as marcas não estejam diretamente envolvidas na produção deste tipo de conteúdo, podem ser questionadas e responder por violações de terceiros como influenciadores e embaixadores que agem em seu nome.

VISÃO VLK:

- Obter suporte jurídico para campanhas e ações de marketing mediante análise e elaboração de contratos estratégicos com agências e criadores de conteúdo, bem como revisão de peças e ativações publicitárias para identificação de potenciais riscos.
- Elaboração de guias orientativos voltados ao marketing, garantindo conformidade com LGPD, Código do Consumidor, Código do CONAR, Lei de Direitos Autorais, Lei de Propriedade Industrial e demais diretrizes setoriais.
- Fortalecimento da literacia em legal marketing tanto do time jurídico como das áreas de marketing, agências parceiras e time de influenciadores, utilizando técnicas de visual law e linguagem simples.



9. Web3 e a Economia de Criadores

A Web3 — a nova fase da internet, marcada pela descentralização e pelo controle dos usuários sobre seus dados e criações — está revolucionando a forma como artistas e criadores monetizam seu trabalho: ferramentas de IA permitem que qualquer pessoa produza músicas, vídeos ou jogos sem habilidades técnicas; já o blockchain (um sistema de registro digital seguro) certifica a origem das obras, oferecendo mais segurança quanto à procedência de determinado ativo digital.

Neste contexto, um artista pode vender uma música como NFT (um certificado digital único), que inclui em seu arquivo

uma lógica de smart contract que garante que ele receba parte dos lucros toda vez que a obra for revendida. Plataformas como Decentralized Pictures usam votação coletiva para financiar filmes independentes, e projetos como The Rights simplificam contratos de direitos autorais em segundos usando blockchain. Fãs também ganham poder: em comunidades online (DAOs), eles ajudam a decidir projetos de artistas e são recompensados com acesso exclusivo. Em resumo, a Web3 torna a criação mais acessível, dá controle total aos criadores e transforma fãs em parceiros, endereçando questões como pirataria e intermediários.

IMPACTOS JURÍDICOS:

- **Jurisdição e Governança:** determinar a jurisdição aplicável e a governança em casos de litígios ou disputas pode ser complexo devido à natureza global e descentralizada das transações em *blockchain*.
- **Proteção de Direitos Autorais:** embora haja rastreabilidade quanto à origem do ativo digital, ainda persistem desafios na proteção e remuneração dos criadores, diante da facilidade de reprodução e distribuição de conteúdos no ambiente digital, com relação ao uso indevido total ou parcial de obras de terceiros.

- **Identificação das Partes:** a anonimização das partes envolvidas pode dificultar a aplicação de leis de identificação e verificação de usuários.
- **Proteção de Dados:** considerando a característica de imutabilidade da blockchain, o atendimento de direitos dos titulares como por exemplo a correção ou eliminação de dados pessoais contidos em determinado bloco pode ser um desafio ao cumprimento da LGPD.

VISÃO VLK:

- Análise profunda quanto às características que envolvem o ambiente específico da Web3, seja uma plataforma de jogos descentralizados, de NFT, de criptoativos ou DAOs, incluindo aspectos relacionados à jurisdição, privacidade, propriedade intelectual.
- Desenvolver estratégias de proteção da propriedade intelectual, orientando os criadores quanto aos melhores mecanismos de remuneração e segurança.



10.

Hiperpersonalização e IA Generativa para Marketing:

Uso avançado de dados e IA para criar experiências de marketing altamente personalizadas e conteúdo gerado artificialmente.



O marketing contemporâneo aposta na hiperpersonalização, com campanhas e conteúdos que são gerados sob medida para o perfil de cada consumidor. Com o uso de IA generativa e big data, marcas criam peças exclusivas – desde e-mails adaptados ao perfil até anúncios diferenciados que envolvam, por exemplo, o deepfake de imagem e voz de personalidades mencionando o nome do consumidor. Assim, surge uma nova perspectiva para o marketing, tendo a tecnologia como importante aliada para personalizar em alta escala, potencializando a conversão de vendas e a comunicação com o público-alvo.

No entanto, por outro lado, despontam desafios relevantes relacionados à privacidade e à responsabilidade pelo conteúdo.

IMPACTOS JURÍDICOS:

- **Proteção de Dados e Privacidade:** riscos relacionados ao tratamento intensivo de dados pessoais para personalização, com exigência rigorosa de transparência e medidas de segurança.
- **Manipulação e Discriminação:** potencial risco para a criação de mensagens que possam, inadvertidamente, reforçar vieses ou discriminar determinados grupos, gerando responsabilização e danos à reputação da empresa.
- **Conformidade Publicitária:** desafio em assegurar que as campanhas hiperpersonalizadas estejam em conformidade com as normas de autorregulamentação publicitária e proteção ao consumidor, evitando práticas enganosas e falta de transparência.

VISÃO VLK:

- Desenvolver políticas internas robustas para o uso ético de dados em campanhas de marketing, com mecanismos claros de transparência.
- Realizar auditorias regulares nos processos de coleta e tratamento de dados, garantindo a conformidade com a LGPD e regulamentos internacionais.
- De acordo com a Kantar⁵, 36% dos profissionais de marketing entrevistados reconhecem que não possuem as *skills* e conhecimentos necessários para explorar plenamente as ferramentas de IA generativa. Neste sentido é fundamental capacitar as equipes de marketing por meio de treinamentos práticos, assegurando que as comunicações sejam acessíveis, éticas e em conformidade com a legislação.

5- Marketing Trends 2025, Kantar. Disponível para download em <https://www.kantar.com/brazil/inspiration/marcas/10-tendencias-de-marketing-para-2025>

Conclusão

As tendências de inovação mapeadas para este ano anunciam mudanças profundas que já estão impactando - ou muito em breve impactarão - o cenário regulatório e empresarial. Reconhecer os sinais de mudança rapidamente e atuar de maneira proativa para inovar com responsabilidade e em conformidade legal pode ser determinante para as empresas assumirem um lugar de vanguarda em seu segmento de mercado.

Ao inovar antes do restante do mercado, a organização pode liderar novos nichos, definir padrões e fortalecer sua posição estratégica, inclusive mediante o endereçamento de desafios legais perante autoridades e órgãos reguladores, influenciando positivamente o cenário regulatório.

Sobre nós

O VLK Advogados entende o Direito como instrumento para impulsionar a inovação, o sucesso dos negócios e uma sociedade mais próspera e justa.

Participamos ativamente da construção de marcos regulatórios e de centenas de projetos inovadores, o que nos permite antecipar tendências e gerar segurança jurídica para viabilizar negócios nas seguintes áreas:

- Governança Ética e Proteção de Dados
- Inteligência Artificial
- Segurança Cibernética e Resposta a Incidentes
- Economia Criativa, Legal Marketing e Propriedade Intelectual
- Legal Design e Visual Law
- Advocacy e Regulação Estratégica de Tecnologia
- Contencioso Estratégico

COMUNICACAO@VLKLAW.COM.BR



AUTORES



GISELE KARASSAWA

gisele@vlklaw.com.br



RONY VAINZOF

rony@vlklaw.com.br



MATEUS LAMONICA

mateus.lamonica@vlklaw.com.br

E-book "O FUTURO DO DIREITO DIGITAL – E os impactos causados pelas tendências de Inovação e Tecnologia", Maio de 2025.

CC BY-ND - Esta licença permite cópia e distribuição do material em qualquer meio ou formato apenas de forma não adaptada e apenas desde que a atribuição seja dada ao criador. A licença permite o uso comercial.

