E-BOOK

TENDÊNCIAS 2025

DIREITO DIGITAL, IA, PROTEÇÃO DE DADOS & CIBER

Abordagem prática do que impactará o seu negócio

VLK ADV

WWW.VLKLAW.COM.BR

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

contato@vlklaw.com.br

Este documento tem como objetivo prover informações para fins educacionais e acadêmicos. Não deve ser interpretado como aconselhamento jurídico.

VLK ADV

WWW.VLKLAW.COM.BR

ÍNDICE

Índice interativo.
Clique para acessar o tema.

INTRODUÇÃO
COMO O DIREITO DIGITAL IMPACTARÁ OS SEUS NEGÓCIOS EM 2025

Empresas de todos os setores são desafiadas a navegar em um ambiente cada vez mais dinâmico, interconectado e regulado (por leis, mercado, normas sociais ou arquitetura/códigos de programação**[1]**). No centro dessa revolução emergem questões complexas que não apenas moldam o futuro do mercado, mas também redefinem os limites entre tecnologia, negócios e sociedade. O Direito Digital, como impulsionador estratégico, é essencial para antecipar, compreender e responder a essas tendências, buscando que a inovação seja segura, ética e alinhada às expectativas empresariais, regulatórias e sociais.

Neste **e-book sobre tendências do Direito Digital para 2025** exploramos os temas mais impactantes para empresas que buscam consolidar sua competitividade em um mercado global, inovador e repleto de desafios.

Abordamos questões críticas, como **Entropia Digital e Complexidade Regulatória,** explorando a complexidade de lidar com legislações diversificadas, que muitas se sobrepõem, em uma economia digital globalizada e **Inteligência Artificial,** que continua a evoluir como motor de eficiência e inovação, mas com seus riscos, suas obrigações legais e novas perspectivas regulatórias.

Discutimos também o **fortalecimento da ANPD e a maturidade da proteção de dados no Brasil,** que trazem não apenas novos desafios de conformidade, mas oportunidades para construir confiança com clientes e parceiros. A importância da **Cibersegurança e Resposta a Incidentes** destaca o risco contínuo e crescente das ameaças cibernéticas para empresas, investidores, clientes e nações. O tema vai muito além da proteção de dados pessoais e segredos de negócios corporativos, pois ataques podem travar as operações de organizações e países. Como prevenir e reagir adequadamente aos ataques e incidentes é fundamental.

A **Governança Digital Estruturada** surge como elemento central para harmonizar inovação, conformidade regulatória e eficiência operacional, fornecendo às empresas estrutura robusta para gerenciar a complexidade tecnológica e regulatória, alinhando estratégias digitais com objetivos de negócios, transparência e responsabilidade ética. O ***Legal Design*** **e a Centralidade do Usuário** apontam para a necessidade de tornar o direito mais acessível, funcional e alinhado às expectativas do cliente na era digital.

Ainda quanto à interação com clientes, destacamos que o marketing, como principal motor de vendas e comumente detentor dos maiores budgets das empresas, tem sido profundamente modificado pela inteligência artificial, permitindo a criação de conteúdos publicitários em massa com personalização. Nesse cenário, a compreensão do **Legal Marketing** e do Direito Digital é fundamental para as companhias nessa jornada de inovação na Economia Criativa.

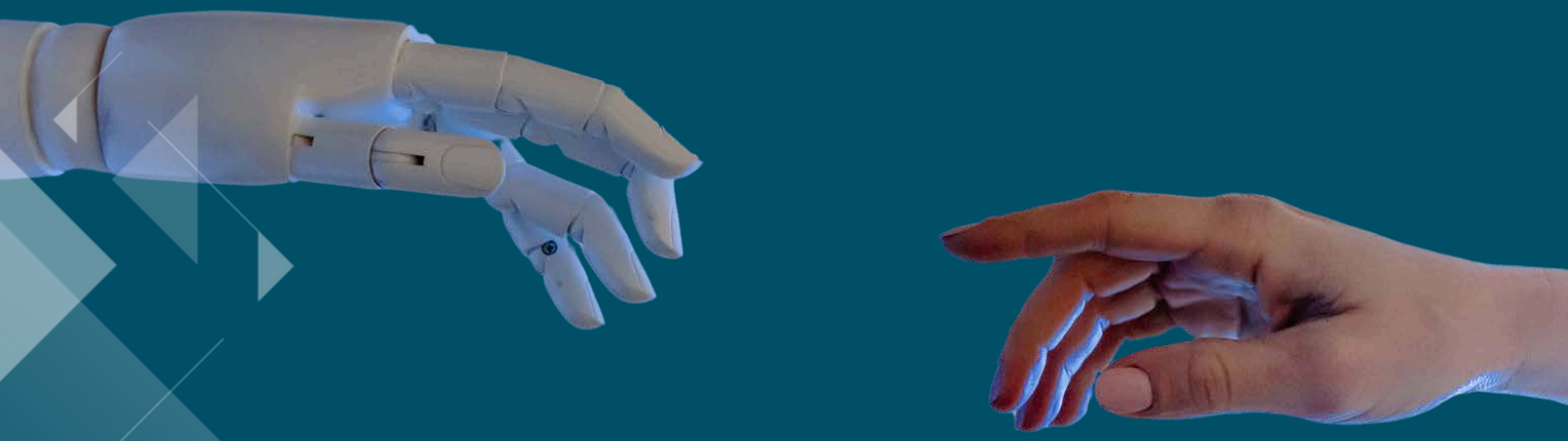
Além disso, exploramos a **Soberania Digital Competitiva,** conceito que posiciona empresas e nações como líderes em inovação, e enfatizamos a **Educação Midiática e Literacia Digital,** mecanismos fundamentais para capacitar a sociedade em um mundo cada vez mais mediado por tecnologia.

Outros tópicos, como **Sustentabilidade Digital e Green Tech, Neurodireitos e Integridade da Informação** abordam os impactos éticos, ambientais e sociais da digitalização.

Este e-book foi desenvolvido para nossos clientes – líderes de empresas que reconhecem a necessidade de ir além da conformidade, utilizando o Direito Digital como alavanca para inovação, segurança e crescimento sustentável.

Cada tema reflete nossa visão de que o **Direito não é barreira, mas catalisador para transformar desafios em vantagens competitivas.**

Sejam muito bem-vindos **ao futuro do Direito Digital com o VLK, onde o Direito impulsiona a Inovação.**



[1] Lawrence Lessig, em seu influente e ainda atual livro Code and Other Laws of Cyberspace (1999) e sua versão revisada Code: Version 2.0 (2006), argumenta que o comportamento no ciberespaço é regulado por essas quatros forças principais, conhecidas como os "modos de regulação".

1) ENTROPIA DIGITAL E COMPLEXIDADE REGULATÓRIA

TENDÊNCIAS PARA 2025

No ambiente digital, "entropia" reflete o caos causado pelo excesso de regulamentações, em decorrência da rápida evolução tecnológica=. Esse desafio se intensifica na economia digital sem fronteiras, em que o intercâmbio global de dados e tecnologias dificulta a conformidade, implementação de normas e preservação da soberania nacional, especialmente sem a harmonização regulatória internacional.

Para as organizações, equilibrar eficiência operacional e conformidade é desafio crescente. No entanto, com planejamento estratégico, ações coordenadas entre os Poderes Executivo e Legislativo e alianças globais, é possível estabelecer ambiente que favoreça a inovação responsável e o equilíbrio regulatório.

POR QUE É TENDÊNCIA?

No Brasil, o cenário regulatório é marcado por planos, estratégias digitais, marcos legais (federais, estaduais e municipais) e regulações setoriais, como:

- Plano Nacional de Internet das Coisas (2019)
- Política Nacional de Inovação e dispõe sobre a sua governança (2020)
- Estratégia Brasileira de Inteligência Artificial (2021 - EBIA)
- Estratégia Brasileira para Transformação Digital (2022 - e-Digital, ciclo 2022-2026)
- Política Nacional de Cibersegurança (2023 - PNCiber)
- Estratégia Brasileira de Educação Midiática (2023 – SECOM)
- Proposta do Plano Brasileiro de Inteligência Artificial (2024 - PBIA)
- Política Nacional da Economia de Dados (tomada de subsídios – 2024)
- Política Nacional de Proteção de Dados Pessoais (em andamento no CNPD)
- Marco Regulatório de IA (em andamento no Congresso)
- Regulação de moderação de conteúdo das plataformas (em andamento no STF e Congresso)

Na União Europeia, iniciativas como o *EU AI Act, GDPR, Digital Services Act, Digital Markets Act, Data Governance Act e Data Act* fazem parte da estratégia da "Década Digital". No entanto, recente relatório solicitado pela Comissão Europeia e elaborado por Mario Draghi**[1]** propõe redução da burocracia e simplificação regulatória para fortalecer a competividade por lá: 60% das empresas europeias identificam a regulação como barreira ao investimento, e 55% das pequenas e médias empresas veem-na como o maior desafio ao crescimento.

Olhando essa temática sob a perspectiva de IA (aprofundaremos esse tópico no Capítulo 2), atualmente há diversos países buscando equilibrar inovação e mitigação de riscos por meio de legislações abrangentes ou específicas, estratégias nacionais e esforços multilaterais, como os Princípios de IA da OCDE e iniciativas da UNESCO, ISO e Conselho da Europa. No geral, as estratégias começam com diretrizes éticas antes de evoluir para legislações formais, refletindo a complexidade da tecnologia.**[2]**

No Brasil, em abril de 2024, por exemplo, o TCU analisou o impacto da regulação de IA**[3]** sobre a Estratégia Brasileira de IA (EBIA)**[4]**, tendo destacado riscos como estagnação tecnológica, barreiras a startups, perda de competitividade e dificuldade de retenção de talentos. O órgão recomendou abordagem regulatória ágil, setorial e adaptável à evolução tecnológica, evitando entraves à inovação.

A interação entre regulações emergentes e aquelas já em vigor, tanto globais quanto nacionais, impõe desafios às empresas, que precisam desenvolver estruturas robustas para gerenciar riscos, responsabilidades e conformidade. Organizações que antecipam e se adaptam a essa complexidade regulatória estão mais bem posicionadas para competir e inovar com segurança no ambiente global,**[5]** podendo influenciar, inclusive, para a simplificação regulatória.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO?

Inconsistência regulatória: divergências entre normas dificultam a conformidade, especialmente para empresas multinacionais, ao impor requisitos contraditórios ou duplicados.

Custo de conformidade: empresas enfrentam elevados investimentos em consultoria jurídica, tecnologia e treinamento para atender a múltiplos e novos regulamentos. Falhas na adaptação diante da complexidade regulatória aumentam os riscos de multas e indenizações, mudanças operacionais forçadas e danos reputacionais, demandando estruturas internas robustas.

Barreiras à inovação: *startups* e pequenas empresas, que têm recursos mais limitados, podem ser particularmente prejudicadas pela sobrecarga regulatória, o que desestimula inovações globais.

Dispersão de recursos: governos e empresas perdem eficiência ao multiplicar esforços regulatórios, atrasando impactos práticos e resultados efetivos.

Falta de clareza para o mercado: iniciativas regulatórias descoordenadas criam incerteza jurídica, desestimulando investimentos e restringindo o potencial de inovação.

SUGESTÕES DO VLK

A harmonização regulatória é essencial para superar os desafios da inconsistência normativa, altos custos de conformidade e incertezas jurídicas. Ambiente regulatório alinhado favorece a inovação e a segurança jurídica, sem comprometer direitos fundamentais, eliminando redundâncias e criando soluções eficazes.

Políticas públicas e marcos regulatórios devem ser convergentes, inclusive entre setores, para minimizar conflitos. Reguladores como Anatel, Bacen, CADE, ANPD e Susep precisam priorizar acordos de cooperação, garantindo atuação complementar e evitando sobreposições *(bis in idem).*

Na economia digital global, cadeias de valor são dinâmicas e interconectadas. A competitividade das organizações brasileiras e seu acesso a tecnologias globais dependem da participação ativa do país na formulação de políticas internacionais. Isso exige esforços coordenados entre governo, empresas e reguladores para fomentar o diálogo entre jurisdições nacionais e internacionais.

Reguladores devem estabelecer padrões alinhados globalmente, reduzindo barreiras para empresas multinacionais e promovendo a inovação responsável. Essa abordagem equilibrará desenvolvimento econômico com segurança jurídica, posicionando o Brasil de forma estratégica no cenário global.

__[1]__ Apresentado à Comissão Europeia em 9 de setembro de 2024, Draghi enfatiza a necessidade de desburocratizar processos e simplificar a regulamentação na UE. Ele sugere a criação de uma Vice-Presidência dedicada à simplificação regulatória e a implementação de metodologias para quantificar os custos das novas leis, especialmente aquelas que afetam pequenas e médias empresas (PMEs). Destaca a importância de aumentar os investimentos em inovação, particularmente em setores como inteligência artificial, para que a Europa não fique atrás de concorrentes como os Estados Unidos e a China. Ele sugere o fortalecimento do Conselho Europeu de Inovação e a criação de "sandboxes" regulatórias para promover a experimentação tecnológica. Vejam os reports e artigo sobre o tema:
https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf
https://commission.europa.eu/document/download/ec1409c1-d4b4-4882-8bdd-3519f86bbb92_en?filename=The%20future%20of%20European%20competitiveness_%20In-depth%20analysis%20and%20recommendations_0.pdf
https://www1.folha.uol.com.br/colunas/ronaldolemos/2024/09/europa-critica-lei-de-ia-que-o-brasil-quer-copiar.shtml
__[2]__ Sobre o tema, vale acompanhar o Global AI Law and Policy Tracker https://iapp.org/media/pdf/resource_center/global_ai_law_policy_tracker.pdf.
__[3]__ Foram avaliados os PLs 21/2020, 2338/23, 4.025/23 e 3.592/23.
__[4]__ Acórdão616/2024 - https://pesquisa.apps.tcu.gov.br/doc/acordao-completo/616/2024/Plen%C3%A1rio
__[5]__ Relatório de Governança Digital Organizacional 2024 da IAPP.

1) ENTROPIA DIGITAL E COMPLEXIDADE REGULATÓRIA

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	O volume de regulações no Direito Digital continuará crescendo, trazendo dificuldade em harmonizar a governança corporativa. Com isso, advogados e reguladores precisarão adotar práticas interdisciplinares para lidar com a crescente complexidade.
POR QUE É TENDÊNCIA?	Expansão do cenário regulatório marcado por planos, estratégias digitais e marcos legais, no Brasil e no mundo, os quais, ao invés de dialogarem, muitas vezes se sobrepõem.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	A interação entre regulações emergentes e pré-existentes, tanto globais quanto nacionais, impõe desafios às empresas, que precisam desenvolver estruturas robustas para gerenciar riscos, responsabilidades e conformidade. Ou seja, divergências entre normas gera inconsistência regulatória, insegurança jurídica, custo de conformidade, barreiras à inovação, dispersão de recursos e falta de clareza para o mercado sobre políticas de Estado.
SUGESTÕES DO VLK	A harmonização regulatória é essencial para superar esses desafios. Trata-se de estratégia de coesão indispensável para eliminar redundâncias e criar soluções eficazes. Políticas públicas e marcos regulatórios devem ser convergentes, inclusive entre setores, para minimizar conflitos. A competitividade das organizações brasileiras e seu acesso a tecnologias globais dependem de participação ativa do país na formulação de políticas internacionais. Isso exige esforços coordenados entre governo, empresas e reguladores para fomentar o diálogo entre jurisdições nacionais e internacionais. É fundamental o monitoramento dos principais projetos de lei, consultas públicas e tomadas de subsídios que possam afetar o negócio, antecipando os impactos e buscando influenciar positivamente o seu texto, de forma a refletir o melhor cenário para o país e para os cidadãos. Essa antecipação também é importante para possibilitar ajustes à governança, de forma gradual.

2) REGULAÇÃO E GOVERNANÇA DA INTELIGÊNCIA ARTIFICIAL

TENDÊNCIAS PARA 2025

A inteligência artificial (IA) é tecnologia essencial para a competitividade de nações e empresas. A revolução do aprendizado de máquina e a crescente disponibilidade de dados impulsionam avanços científicos e promovem crescimento econômico e social, além de contribuírem para a solução de desafios globais.

Por outro lado, os riscos e desafios da IA podem ser proporcionais à sua magnitude. Entre eles estão a concentração de poder em poucos países e empresas, a amplificação de vieses discriminatórios, violações de propriedade intelectual e direitos de terceiros (tanto no treinamento de modelos quanto no conteúdo gerado), escalada da desinformação, desafios à proteção de dados pessoais e segurança cibernética, além de transformações profundas no mercado de trabalho, que exigem esforços significativos de capacitação.

Nesse contexto, surge a discussão de novas abordagens regulatórias para a IA. Embora as organizações possam adotar governança própria para alinhar os riscos aos seus objetivos estratégicos, regulação equilibrada pode ser importante para garantir padronização mínima e segurança jurídica, favorecendo o ecossistema de inovação. No entanto, carga regulatória excessiva pode restringir o avanço tecnológico e limitar o desenvolvimento de aplicações de IA.

Diversas nações estão discutindo como e em que nível regular a IA. Há certo consenso global sobre a necessidade de regulação, mas divergências significativas sobre a abordagem ideal (especialmente, entre principiológico e prescritivo). O desafio é encontrar o equilíbrio entre incentivar inovação e desenvolvimento econômico, enquanto se protege direitos individuais e coletivos, garantindo a evolução responsável dessa tecnologia transformadora.

POR QUE É TENDÊNCIA?

Em 2025 são esperados avanços significativos no desenvolvimento de marcos regulatórios para a IA, com destaque no Brasil para o PL 2338/2023 e a consolidação da Política Brasileira de Inteligência Artificial (PBIA), promovida pelo Governo Federal.

No cenário internacional, a entrada em vigor do *AI Act***[1],** na União Europeia, é marco histórico como a primeira legislação abrangente para regulação da IA**[2]**. Sua aplicação extraterritorial amplia o impacto global, influenciando práticas e padrões fora do bloco europeu. Iniciativas como o *AI Pact***[3]**, a criação de órgãos especializados para supervisão e

a formulação de códigos de boas práticas reforçam esse movimento, buscando estabelecer diretrizes mais claras e eficazes**[4]**.

Organizações como ONU, OCDE e Conselho da Europa também desempenham papéis cruciais, promovendo frameworks focados em princípios éticos, transparência e responsabilidade**[5]**. Esses esforços visam mitigar riscos relacionados à segurança, discriminação e outros impactos adversos da IA, criando ambiente de confiança global.

Nessa linha, segue levantamento realizado pelo *AI Governance Report 2024*, resumindo os esforços normativos e procedimentais para governar a IA**[6]**:

Além dos novos e futuros marcos regulatórios, é importante considerar a aplicação de legislações existentes ao contexto da IA no Brasil, como a LGPD, o Código de Defesa do Consumidor e o Código Civil, as quais inclusive já foram tomadas como referência para decisões judiciais e administrativas.

a) A Terceira Turma do STJ**[7]** reconheceu que decisões automatizadas podem gerar riscos (como discriminação, perda de autonomia e resultados enviesados), especialmente quando baseadas em dados desatualizados ou irrelevantes. Diante disso, decidiu que, em casos graves que representem risco ao funcionamento da plataforma ou à segurança dos usuários, o perfil de um usuário pode ser suspenso

imediatamente, desde que haja transparência, ele seja informado sobre os motivos e seja oportunizado o contraditório**[8]**. Se for confirmada a violação dos termos de uso, após a análise da defesa do usuário, o descredenciamento definitivo será considerado legítimo, sem abusividade, embora o caso ainda possa ser submetido a revisão judicial, se necessário.**[9]**

b) Em outro caso de 2024, a ANPD suspendeu cautelarmente a nova política de privacidade da Meta no Brasil, que permitia o uso de dados pessoais para treinar sistemas de IA generativa. A decisão foi motivada por problemas como: base legal inadequada (legítimo interesse), especialmente para dados sensíveis; falta de transparência na comunicação aos usuários; restrições excessivas ao exercício dos direitos dos titulares; e riscos no tratamento de dados de crianças e adolescentes, em desacordo com a LGPD. Em 30 de agosto, após a Meta apresentar plano de conformidade, a ANPD autorizou a retomada parcial do uso de dados para treinamento de IA, com restrições e maior controle sobre transparência e direitos dos titulares.**[10]**

Outro ponto complexo e relevante é a proteção de direitos autorais para treinamento de IA**[11]**. A discussão envolve a aplicabilidade do Fair Use – doutrina que permite o uso de obras protegidas em determinadas circunstâncias – adaptada ao contexto do treinamento de IA, o chamado *Fair Training***[12]**.

Diversos litígios nos EUA ajudam a ilustrar a complexidade desse debate. Casos como Richard Kadrey v. Meta e Doe v. GitHub apontam que o uso de conteúdo protegido por IA pode infringir direitos autorais. No caso do GitHub, o tribunal considerou que nem mesmo o risco de 1% de reprodução não autorizada no treinamento do *Copilot* justificava a continuidade do processo. Já em The New York Times v. OpenAI e Microsoft se questiona o uso indevido de grandes volumes de dados qualificados para treinamento, resultando em outputs similares às obras originais.

Já acordos como o da OpenAI com a *Associated Press* demonstram alternativas cooperativas, nas quais o uso de conteúdo protegido é remunerado e ocorre dentro de parâmetros transparentes.

O avanço regulatório em IA para 2025, no Brasil e no mundo, deverá buscar equilibrar inovação com proteção de direitos. Iniciativas como o Marco Legal da IA, o *AI Act* e casos recentes envolvendo a ANPD e decisões no STJ reforçam a importância de transparência, governança e alinhamento à legislação. Questões emergentes, como direitos autorais no treinamento de IA, destacam a necessidade de discussão profunda entre reguladores e os diversos setores da sociedade para promover confiança e garantir inovação responsável.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO?

A IA é recurso poderoso na solução de grandes desafios da humanidade, mas que requer literacia, ética e pensamento crítico. Em pesquisa da Cisco, de 2023**[13]**, 62% dos consumidores expressaram preocupação com o uso de IA e 60% disseram já ter perdido confiança em organizações por causa dela. Embora 48% acreditem que a IA possa melhorar suas vidas, a maioria dos consumidores (77%) enfatiza que as organizações devem ser responsáveis ao usar IA. Para reduzir preocupações, 72% indicam que ficariam mais confortáveis se as aplicações de IA fossem auditadas para evitar vieses e 75% gostariam de mais transparência e envolvimento humano nos processos decisórios da IA.

A confiança digital envolve mitigar os riscos da IA, especialmente diante de problemas com a falta de precisão, erros e alucinações; complexidade da explicabilidade; violação de propriedade intelectual; perigo da potencialização de vieses sociais discriminatórios; aumento na escala e sofisticação da desinformação; e proteção de dados pessoais e segurança cibernética. O Gartner projeta que, até 2026, organizações que adotarem práticas éticas e responsáveis em IA terão 50% mais resultados positivos em negócios e aceitação do usuário.

Governar a IA é um desafio, dada a complexidade de sua cadeia de valor. As obrigações devem ser proporcionais ao papel de cada agente (desenvolvedor, distribuidor, aplicador, usuário) e ajustadas ao risco associado ao uso da tecnologia. Empresas que adotam abordagens éticas e proativas estão mais bem posicionadas para equilibrar inovação e confiança, além de estarem mais próximas da conformidade do possível futuro Marco Legal brasileiro, que deve contemplar a seguinte estrutura:

- **Direitos:** direitos para a pessoa (ou grupo de pessoas) afetadas por sistemas de IA, como (i) explicação, sobre a decisão ou recomendação; (ii) contestação e solicitação de revisão da decisão ou recomendação; e (iii) revisão humana das decisões;

- **Categorização dos Riscos:** lista de sistemas de IA classificados como de risco excessivo (uso proibido) e de alto risco. Prevendo, ainda, a capacidade do Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA) editar a lista, acrescendo novos sistemas, e os critério com que deve fazê-lo;

- **Governança dos Sistemas de Inteligência Artificial:** conjunto de controles, que devem ser adotados, no desenvolvimento ou na aplicação de soluções de IA, especialmente para as de alto risco, como: documentação adequada da IA (testes da confiabilidade e segurança da IA e do grau de supervisão humana); medidas para IA que produz conteúdo sintético; avaliação de Impacto Algorítmico; e medidas para Sistemas de Inteligência Artificial de Propósito Geral e Generativa;

- **Acreditação, Certificação e Avaliação de Conformidade:** a Autoridade Competente (coordenadora do SIA) e as autoridades setoriais poderão acreditar organismos que procederão a avaliação de conformidade dos sistemas, por prazo determinado a ser fixado pelo SIA;

- **Códigos de conduta e programas de governança ética de IA:** previsão próxima ao previsto na legislação de proteção de dados para os programas de governança em dados, os quais poderão ser consideradas indicativo de boa-fé por parte do agente e será levada em consideração pela autoridade competente e demais autoridades setoriais para fins de aplicação de sanções administrativas;

- **Comunicação de Incidentes Graves:** o agente de IA deverá comunicar à autoridade setorial a que se encontre sujeito a ocorrência de incidentes graves, especialmente aquelas em que exista risco à vida, integridade física, violação de direitos fundamentais ou ao funcionamento de operações críticas de infraestruturas;

- **Direitos Autorais:** regulamenta o uso de conteúdo protegido no desenvolvimento de IA. Prevê o dever, como regra, de remunerar os autores residentes em território nacional (ou de países com regras equivalentes) e a faculdade de os autores proibirem a utilização de suas obras para treinamento de IA**[14]**;

- **Supervisão e Fiscalização:** composição e atribuições do SIA, distribuindo as competências entre a autoridade competente, coordenadora do SIA (a princípio, a ANPD) e as autoridades setoriais. A lógica é valorizar e reforçar as competências regulatória, sancionatória e normativa das autoridades setoriais em harmonia com as correlatas gerais da autoridade competente que coordena o SIA. Atividades econômicas em que não haja ente regulador setorial específico, a autoridade competente exercerá essas competências;

- **Sanções:** novas sanções por descumprimento da lei que, além de serem cumuláveis com aquelas previstas em outros normativos (incluindo a LGPD), podem implicar em multas de até R$:50 milhões ou 2% do faturamento bruto, por infração.

- **Responsabilidade Civil:** em síntese, se mantêm as normas de responsabilidade civil já aplicáveis, prevendo-se, no entanto, o direito de inversão do ônus da prova, em caso de hipossuficiência ou onerosidade excessiva em decorrência das características da IA; e

- **Fomento à Inovação Sustentável:** novos incentivos e novas regras que objetivam garantir que o desenvolvimento e a aplicação da IA se operem de forma econômica e socialmente sustentáveis, incluindo: *sandbox*; proteção dos trabalhadores; medidas de incentivos e sustentabilidade; e incentivo a microempresas, empresas de pequeno porte e startups.

- **Prazo para implementação e disposições finais:** além de definir os prazos de *vacatio legis* (que variará em acordo com os dispositivos, mas será de até 730 dias), prevê uma série de hipóteses em que o SIA deverá elaborar regulamentos simplificados, incluindo: (i) padrões e formatos abertos e livres, ressalvados se foram de alto risco ou de propósito geral; (ii) fomento nacional; (iii) projetos de interesse público; (iv) incentivo à inovação e pesquisa cientifica e tecnológica no ambiente produtivo, para capacitação e autonomia tecnológica.

SUGESTÕES DO VLK

Para mitigar os impactos dessa tendência, é recomendado que as empresas se antecipem e fiquem atentas às exigências legais, criando governança robusta para sistemas de IA, alinhada com guias e melhores práticas internacionais. Investir em conscientização e processos que garantam a conformidade com as normas globais de IA pode ser a chave para a competitividade no mercado.

As organizações devem ponderar o melhor *framework* para governança de IA**[15]** e consolidá-los mediante medidas, como:

- **Prioridade Estratégica:** tudo começa pelo board, pois é onde se define a estratégia, a responsabilidade final e a cultura ética da organização. Isso garante alinhamento estratégico, mitigação de riscos e credibilidade perante stakeholders e reguladores. Ou seja, alinhar IA aos objetivos corporativos, valores éticos e frameworks regulatórios.

- **Literacia em IA:** capacitar e aprimorar a cultura organizacional, do conselho, executivos, e colaboradores em aspectos éticos, regulatórios e estratégicos da IA é fundamental. Ela capacita as pessoas a compreenderem os benefícios e as limitações das tecnologias de IA, identificando oportunidades de aplicação e avaliando riscos éticos e de conformidade;

- **Mapeamento:** mapear aplicações de IA desenvolvidas, implementadas ou utilizadas.

- **Cadeia de Valor:** identificar os papéis desempenhados como "agentes de IA" em cada aplicação. Enquadrar a organização para cada aplicação como desenvolvedor ou aplicador, por exemplo;

- **Grau de risco:** classificar o grau de risco das aplicações de IA conforme o seu uso e finalidades;

- **Gestão de IAs de terceiros:** avaliar riscos no uso de sistemas de IA de terceiros, especialmente os de propósito geral;

- Definir medidas de governança adequadas, com base nos riscos, finalidades e papéis desempenhados;

- Estruturar um programa de governança com comitês de ética, políticas e cláusulas contratuais claras;

- Realizar Avaliações de Impacto Algorítmico para aplicações de IA de alto risco;

- Monitorar continuamente o programa, estabelecendo métricas e responsáveis.

Além disso, adotar perspectiva sociotécnica é crucial, dado que processos técnicos são influenciados por valores e normas humanas. Avaliações éticas e sociais devem ser incorporadas no design e desenvolvimento de IA**[16]**, considerando:

- A lógica por trás das decisões do sistema;
- A origem e a qualidade dos dados utilizados;
- Medidas para garantir resultados justos, como testes de viés e treinamento de usuários;
- O impacto do sistema nos indivíduos e ações para minimizar consequências negativas; e
- Responsabilidades claras sobre decisões, desenvolvimento e monitoramento.

De acordo com o risco da IA, empresas têm buscado implementar testes rigorosos e avaliação pré-implementação, trabalhando na melhoria contínua dos modelos de IA e na incorporação de validação ou revisão humana, quando necessário. Também estão fortalecendo as medidas de segurança em torno dos dados usados para treinar e operar sistemas de IA, além de garantir que contratos com fornecedores de IA respeitem regras de confidencialidade. Fora isso, as empresas estão optando por personalizar ou desenvolver seus próprios modelos de IA para atender às necessidades específicas do seu negócio, o que também ajuda a mitigar os riscos associados ao uso de soluções genéricas.

Ao combinar governança estruturada com reflexões sociotécnicas, as organizações podem mitigar riscos, fortalecer a confiança e se posicionar de forma estratégica em um mercado cada vez mais regulado e em transformação legal.

[1] E-Book AI Act. 20 pontos de atenção para o Brasil, 2ª Edição. https://vlklaw.com.br/wp-content/uploads/2024/07/2a-edicao-E-book-AI-Act-UE-2.pdf
[2] Navegue pelo nosso Mapa Interativo do AI Act para entender melhor o novo Regulamento Europeu. https://vlklaw.com.br/wp-content/uploads/2024/04/AI-Act-Mapa-Interativo-de-Obrigacoes-e-das-Categorias-de-Riscos-VLK-Advogados.pdf
[3] Artigo sobre as novidades do AI Act. https://vlklaw.com.br/wp-content/uploads/2024/07/Novidades-sobre-o-EU-AI-Act.pdf
[**4]** Entenda aqui melhor o tema: https://vlklaw.com.br/wp-content/uploads/2024/11/First-Draft-General-Purpose-AI-Code-of-Practice-Comissao-Europeia.pdf
[5] UNESCO e as novas abordagens regulatórias para IA: Reflexões para o Brasil. https://vlklaw.com.br/wp-content/uploads/2024/09/UNESCO.pdf
[6] AI Governance in Practice Report 2024 (IAPP e FTI). Disponível em: https://static2.ftitechnology.com/docs/white-papers/AI+Governance+in+Practice+Report-2024+-+IAPP+-+FTI-Technology.pdf
[7] STJ - REsp: 2135783 DF 2023/0431974-4, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 18/06/2024, T3 - TERCEIRA TURMA, Data de Publicação: DJe 21/06/2024.
[8] A decisão cita que seriam os casos, por exemplo, de comportamento inadequado do motorista em razão de assédio ou importunação sexual, racismo, crimes contra o patrimônio, agressões físicas e verbais, dentre outras questões que envolvem não somente o contratante, senão o consumidor, seu bem-estar, segurança e dignidade
[9] Riscos e oportunidades da regulamentação de decisões automatizadas e IA pela ANPD - https://www.conjur.com.br/2024-nov-27/riscos-e-oportunidades-da-regulamentacao-de-decisoes-automatizadas-e-inteligencia-artificial-pela-anpd/
[10] Meta cumpre exigências da ANPD e poderá retomar, com restrições, o uso de dados pessoais para treinamento de inteligência artificial - https://www.gov.br/anpd/pt-br/assuntos/noticias/meta-cumpre-exigencias-da-anpd-e-podera-retomar-com-restricoes-o-uso-de-dados-pessoais-para-treinamento-de-inteligencia-artificial?utm_source=chatgpt.com
[11] Direitos autorais e treinamento de inteligência artificial. https://www1.folha.uol.com.br/tec/2024/12/direitos-autorais-e-treinamento-de-inteligencia-artificial.shtml
[12] As teses favoráveis ao Fair Training são: os dados são utilizados como insumos técnicos para ensinar o modelo sobre as relações estatísticas entre os seus elementos, não sendo relevante o conteúdo autoral em si para o seu treinamento; a aprendizagem de máquina é comparável ao processo humano de autoaprendizagem indutivo; é possível coibir práticas anticompetitivas e abusivas vedando o uso de dados exclusivamente extraídos para o treinamento de sistema de concorrente; o Fair Training não impede a responsabilização dos agentes pelos resultados (outputs) que violem direitos autorais; e aumento da concorrência, evitando que apenas grandes empresas monopolizem o treinamento de modelos devido aos custos de licenciamento.
[13] Privacy's Growing Importance and Impact. CISCO 2023 DATA PRIVACY BENCHMARK STUDY. Disponível em: Grau de risco: classificar o grau de risco das aplicações de IA conforme o seu uso e finalidades;
Gestão de IAs de terceiros: avaliar riscos no uso de sistemas de IA de terceiros, especialmente os de propósito geral;
Definir medidas de governança adequadas, com base nos riscos, finalidades e papéis desempenhados;
Estruturar um programa de governança com comitês de ética, políticas e cláusulas contratuais claras;
Realizar Avaliações de Impacto Algorítmico para aplicações de IA de alto risco;
Monitorar continuamente o programa, estabelecendo métricas e responsáveis.
[14] Direitos autorais e treinamento de inteligência artificial. Disponível em: https://www1.folha.uol.com.br/tec/2024/12/direitos-autorais-e-treinamento-de-inteligencia-artificial.shtml
[15] Como ISO/IEC 38507:2023 e ISO/IEC 42001:2023; AI Risk Management Framework (NIST); Standard for Transparency of Autonomous Systems (IEEE); AIGA AI Governance Framework (Universidade de Turku); EU AI Act; e Projeto de Lei 2.338/23 (Brasil).
[16] Leslie, D., Rincón

2) REGULAÇÃO E GOVERNANÇA DA INTELIGÊNCIA ARTIFICIAL

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Devemos ter a aprovação do Marco de IA brasileiro em 2025, o qual, somado aos reflexos da eficácia do AI Act na União Europeia, servirá de referência global, sendo importante acompanhar sua adoção e regulamentações. Ainda, diante das legislações já aplicáveis (como a LGPD, o CDC e Código Civil), o olhar atento dos órgãos setoriais competentes e o aumento da utilização das aplicações de IA nos mais variados contextos, deve haver maior incidência de regulamentações setoriais, fiscalizações e decisões judiciais sobre o tema. Com isso, aspectos de explicabilidade (maior transparência e rastreabilidade), com frameworks que priorizem explicação acessível, possibilidade de revisão das decisões automatizadas e avaliação de impacto algorítmico, devem ser exigidos das organizações, de acordo com o risco no contexto de uso da IA, que deverão adotar governança ética sobre o assunto, também atentando para diversidade, redução de vieses e maior precisão.
POR QUE É TENDÊNCIA?	Em 2025 são esperados avanços significativos no desenvolvimento de marcos regulatórios para a IA, com destaque no Brasil para a evolução do PL 2338/2023 e a consolidação da Política Brasileira de Inteligência Artificial (PBIA), promovida pelo Governo Federal. No cenário internacional, a entrada em vigor do AI Act, na União Europeia, é marco histórico como a primeira legislação abrangente para regulação da IA. Sua aplicação extraterritorial amplia o impacto global, influenciando práticas e padrões fora do bloco europeu. Iniciativas como o AI Pact, a criação de órgãos especializados para supervisão e a formulação de códigos de boas práticas reforçam esse movimento, buscando estabelecer diretrizes mais claras e aplicáveis. Além dos novos marcos regulatórios, é importante considerar a aplicação de legislações existentes ao contexto da IA no Brasil, como a LGPD, Código de Defesa do Consumidor e Código Civil, inclusive já gerando decisões judiciais e administrativas
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	A confiança digital envolve mitigar os riscos da IA, especialmente diante de problemas com a falta de precisão, erros e alucinações; complexidade da explicabilidade; violação de propriedade intelectual; perigo da potencialização de vieses sociais discriminatórios; aumento na escala e sofisticação da desinformação; e proteção de dados pessoais e segurança cibernética. O Gartner projeta que, até 2026, organizações que adotarem práticas éticas e responsáveis em IA terão 50% mais resultados positivos em negócios e aceitação do usuário.

2) REGULAÇÃO E GOVERNANÇA DA INTELIGÊNCIA ARTIFICIAL

RESUMO EXECUTIVO

SUGESTÕES DO VLK

As organizações devem ponderar o melhor framework ou a combinação deles para a governança ética de IA e o consolidar mediante medidas, como:

- Prioridade Estratégica: tudo começa pelo board, pois é onde são definidas a estratégia, responsabilidade final e cultura ética da organização. Isso garante alinhamento estratégico, mitigação de riscos e credibilidade perante stakeholders e reguladores. Ou seja, alinhar IA aos objetivos corporativos, valores éticos e frameworks regulatórios.
- Literacia em IA: capacitar e aprimorar a cultura organizacional, do conselho, executivos e colaboradores em aspectos éticos, regulatórios e estratégicos da IA é fundamental. Ela permite que as pessoas compreendam os benefícios e as limitações das tecnologias de IA, identificando oportunidades de aplicação e avaliando riscos éticos e de conformidade;
- Mapeamento: mapear aplicações de IA desenvolvidas, implementadas ou utilizadas.
- Cadeia de Valor: identificar os papéis desempenhados como "agentes de IA" em cada aplicação. Enquadrar a organização para cada aplicação como desenvolvedor ou aplicador, por exemplo;
- Grau de risco: Classificar o grau de risco das aplicações de IA conforme o seu uso e finalidades;
- Gestão de IAs de terceiros: avaliar riscos no uso de sistemas de IA de terceiros, especialmente os de propósito geral;
- Definir medidas de governança adequadas, com base nos riscos, finalidades e papéis desempenhados;
- Estruturar programa de governança com comitês de ética, políticas e cláusulas contratuais claras;
- Realizar Avaliações de Impacto Algorítmico para aplicações de IA de alto risco;
- Monitorar continuamente o programa, estabelecendo métricas e responsáveis.

Ao combinar uma governança estruturada com reflexões sociotécnicas, as organizações podem mitigar riscos, fortalecer a confiança e se posicionar de forma estratégica em um mercado cada vez mais regulado e em transformação legal.

3) PROTEÇÃO DE DADOS PESSOAIS

TENDÊNCIAS PARA 2025

A economia e os negócios atuais são cada vez mais movidos a dados pessoais, que são a mola propulsora para de diversos mercados e grandes vetores de condições de mercado e transações econômicas, englobando prevenção a fraude, proteção ao crédito, marketing, comércio, e para o treinamento e desenvolvimento da inteligência artificial, por exemplo.

Justamente para nortear as empresas em como utilizar referidos dados de forma ética, segura responsável, a LGPD agora passa para uma nova fase, com a sua regulamentação e fiscalização pela ANPD, a futura Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD) e por meio de parâmetros que estão sendo estabelecidos em decisões judiciais, inclusive de superior instância, no Poder Judiciário.

POR QUE É TENDÊNCIA?

A Proteção de Dados seguirá como tema central na agenda regulatória brasileira para 2025, com destaque para: a PNPD; o fortalecimento da atuação da ANPD, já que há planos de aumento de contratações e de servidores de carreira**[1]**, Projeto de Lei para fortalecer sua autonomia**[2]** e ela pode ser a "autoridade competente" do novo marco legal de IA**[3];** Agenda Regulatória 25-26 da ANPD e temas que serão objeto de futuras regulamentações, como IA, direitos dos titulares, alto risco, dados biométricos, crianças e adolescentes, entre outros; fiscalizações e sanções administrativas; decisões judiciais de superior instância no Judiciário; e Códigos de Conduta e Autorregulação Regulada.

Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD)

A LGPD prevê que compete à ANPD elaborar diretrizes para a PNPD, assim como ao Conselho Nacional de Proteção de Dados e da Privacidade (CNPD) propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política. O CNPD se dividiu em 6 Grupos de Trabalho temáticos**[4]** e entregará para a ANPD em fevereiro de 2025 suas sugestões de diretrizes para avaliação da ANPD, que minutará a PNPD e entregará ao Executivo para análise e estabelecimento de decreto. Ou seja, em 2025, possivelmente teremos uma política de Estado que norteará as premissas de proteção de dados pessoais no Brasil.

Agenda Regulatória da ANPD

A ANPD já regulamentou o processo de fiscalização, agentes de tratamento de pequeno porte, dosimetria para sanções, comunicado de incidentes de segurança, encarregado pelo tratamento de dados pessoais e transferência internacional de dados. Emitiu guias e estudos técnicos sobre legítimo interesse, *cookies*, tratamento de dados pelo poder público, dados pessoais nas eleições, segurança da informação para agentes pequeno porte, *sandbox* regulatório para IA, crianças e adolescentes, anonimização, cidades inteligentes, biometria e reconhecimento Facial e IA Generativa.

Sobre a agenda regulatória 2025/2026, o CNPD também foi consultado e encaminhou seis sugestões para a ANPD**[5]**:

- Proteção de dados de crianças e adolescentes;
- Tratamento de dados pessoais na área da saúde;
- Definição de alto risco;
- Tratamento de dados pessoais por pessoas jurídicas de direito privado para fins de segurança pública;
- Critérios para reconhecimento e divulgação de regras de boas práticas e de governança, com o objetivo de regulamentar o art. 50 da LGPD; e
- Dados abertos, meio ambiente e proteção de dados.

Para 2025/2026, os temas que serão priorizados na agenda regulatória**[6]**, são:

- Direitos dos titulares;
- Relatório de Impacto;
- Medidas de Segurança da Informação;
- Crianças e adolescentes, incluindo aferição de idade;
- Dados biométricos;
- Alto risco;
- Anonimização e pseudonimização;
- Inteligência Artificial e Fraudes e proteção ao crédito;
- Decisões automatizadas (art. 20 e parágrafos)**[7]**; e
- Tratamento Poder público.

Sobre transferência internacional de dados, até julho de 2025, é provável que ocorra a decisão de adequação mútua entre Brasil e União Europeia, bem como, posteriormente, um olhar e tendência natural para outros países que já foram reconhecidos pela EU.

Com o fim do prazo de 12 meses para o estabelecimento do mecanismo de cláusulas-padrão contratuais (agosto de 2025), vale acompanhar os pedidos junto à ANPD de cláusulas-padrão equivalentes, cláusulas contratuais específica e normas corporativas globais**[8]**.

Além disso, espera-se que a ANPD fortaleça sua atuação em geral, diante da futura realização de concurso público, que poderá levar à Autoridade 213 novos servidores.

Fiscalização

Os processos de fiscalização em trâmite e sanções administrativas aplicadas pela ANPD demonstram a importância de: boa e atualizada avaliação de incidentes e transparência na comunicação, quando configurar risco ou dano relevante aos titulares afetados; boas práticas de cibersegurança (como manter evidências digitais para apurar os incidentes, incluindo guarda de logs); e um almejado nível de governança compatível com a legislação já em vigor há mais de 4 anos, incluindo registro das atividades de tratamento atualizado (RoPA), avaliação de legitimo interesse (LIA) e elaboração de relatório de impacto (RIPD), quando pertinentes.

O cenário também inclui o aumento da fiscalização em práticas relacionadas envolvendo o treinamento de modelos de IA generativa com dados pessoais, uso de reconhecimento facial para fins de segurança e prevenção à fraude e de dados de crianças e adolescentes, especialmente no ambiente digital.**[9]**

Ainda, o Regulamento de Fiscalização determina que a Coordenação-Geral de Fiscalização realizará o monitoramento das atividades de tratamento de dados pessoais, visando, dentre outras ações, planejar e subsidiar a atuação fiscalizatória com informações relevantes. O último relatório publicado, incluindo ações para 2025, contempla os seguintes temas: agregadores de dados; setor público, especialmente relacionado aos poderes executivo e judiciário; Telecomunicações; Financeiro; Plataformas Digitais, especialmente relacionado às intermediadoras de serviços; Direito dos titulares; e Ações Educativas.**[10]**

De outro lado, com os regulamentos publicados ao longo de 2024, especialmente, as Resoluções nº 15, 18 e 19, que tratam, respectivamente, Comunicação de Incidentes de Segurança, do Encarregado e das Transferências Internacionais de Dados, é possível que a fiscalização tenha atenção aos temas.

Da norma do Encarregado, por exemplo, após denúncias de titulares, empresas já estão sendo cobradas para apresentar: os dados de contato do encarregado pelo tratamento de dados pessoais; o canal de comunicação com os titulares de dados destinado ao exercício de seus direitos, com o detalhamento previsto nos artigos 8º e 9º e 13, do Regulamento do Encarregado (identidade do Encarregado; divulgação das informações de forma clara e objetiva, em local de destaque e fácil acesso; capacidade de se comunicar em língua portuguesa); o caminho exato a ser percorrido pelo titular no sítio eletrônico, ou por outros meios disponibilizados, para o exercício de seus direitos garantidos pela LGPD, descrevendo, de maneira clara, os passos necessários para que o titular acesse o canal de comunicação. A ANPD ressalta que será verificado se há obstáculos para o contato direto com o encarregado.

Sobre comunicado de incidentes, de acordo com a LGPD e a Resolução CD/ANPD 15/2024, a ANPD pode iniciar processos de fiscalização para verificar se os agentes regulados estão tratando dados pessoais em conformidade legal.

Desde que foi criada, a ANPD já analisou e concluiu 20 processos de fiscalização e atualmente está analisando outros 17. Os dados sobre processos de fiscalização são constantemente atualizados e mantidos em transparência ativa na página**[11]**.

Por fim, em termos de setores regulados e conforme previsto na LGPD, é relevante que a ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica coordenem suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento desses setores regulados, conforme legislação específica, e o tratamento de dados pessoais.

Judiciário

Desde a vigência da LGPD (agosto de 2020), o Judiciário tem sido provocado a resolver questões como a responsabilidade por dados vazados e as hipóteses de indenização por violação da LGPD em relação aos procedimentos de coleta, armazenamento, tratamento e compartilhamento de dados, sobretudo ao reforçar o direito de o cidadão saber como, quando e por que os seus dados são captados e tratados.

As decisões judiciais já atingiram a superior instância. Especialmente no STJ, vale apontar os seguintes precedentes**[12]**: devido processo informacional e direito de revisão em decisões automatizadas que afetem perfis profissionais; incidente envolvendo dados pessoais não geram, por si só, o direito à indenização por danos morais; instituição financeira responde pelo defeito na prestação do serviço quando informações bancárias são utilizadas por estelionatário para aplicar golpe contra o consumidor; e responsabilidade civil por vazamento de dados pelo fato da empresa não adotou medidas de segurança estabelecidas pela LGPD, que pudessem ser necessárias e suficientes à proteção dos dados pessoais**[13]**.

Assim, em 2025, além da agenda regulatória e dos procedimentos de fiscalização da ANPD, é de fundamental importância acompanhar o entendimento do Poder Judiciário ao interpretar a LGPD.

Códigos de Conduta e Autorregulação Regulada

A autorregulação, por meio de iniciativas como códigos de conduta privados e selos de conformidade, permite que setores econômicos criem padrões adaptados às suas especificidades, promovendo eficiência e maior adesão às normas de proteção de dados.

Os códigos de conduta, superando a fase dos códigos de boas práticas, assumem papel central nesse cenário, ao oferecerem diretrizes claras e práticas específicas que ajudam empresas a implementarem medidas de conformidade de maneira eficaz e demonstrável. A adesão e participação ativa no desenvolvimento desses códigos podem não apenas conferir maior segurança jurídica às organizações, mas também fortalecer sua reputação e a confiança dos titulares de dados, criando um diferencial estratégico em um mercado cada vez mais orientado pela ética e inovação.

Posteriormente, o modelo legal de autorregulação regulada prevista pela LGPD, em que a autoridade supervisora – como a ANPD – valida, monitora e incentiva essas iniciativas, tem se consolidado como uma possibilidade de abordagem equilibrada, unindo flexibilidade setorial à supervisão estatal.

COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?

O impacto dessas tendências nos negócios é muito significativo, considerando a íntima relação entre dados pessoais e a economia digital. Os regulamentos, possíveis atividades fiscalizatórias previstas da ANPD e processos judiciais, exigirão maior dedicação das empresas para se atentar (e conformar) às já existentes e novas obrigações. Ainda, o aumento das atividades de fiscalização expõe as empresas a riscos reputacionais e responsabilização, exigindo atenção redobrada à conformidade e prestação de contas.

Além disso, dados de alguns estudos chamam a atenção para a pauta:

Estudo da CISCO**[14]**, publicado em 2023, com 4.700 profissionais de 12 países, incluindo o Brasil, apurou:

- Retorno sobre o investimento de 1,8 vezes em privacidade nas organizações, sendo que 36% das organizações estão obtendo retorno de pelo menos o dobro de seus gastos, muitas de 3 a 5 vezes o seu investimento;
- Entre os entrevistados brasileiros, em 2022, o orçamento médio para privacidade foi de US$ 2,2 milhões. A média global foi de US$ 2,7 milhões;
- 95% consideram privacidade um imperativo comercial;
- 94% disseram que seus clientes não comprariam deles se seus dados não estivessem devidamente protegidos;
- 95% informaram que privacidade é parte integrante da cultura de suas organizações;
- A mesma pesquisa aponta ainda os benefícios potenciais da jornada de privacidade, que vão muito além dos riscos legais. Mais de 70% indicaram que estavam obtendo benefícios "significativos" ou "muito significativos" em cada um dos seguintes seguimentos:

1. Permitir a inovação;
2. Eficiência operacional;
3. Construir a confiança com os clientes e tornar a empresa mais atraente;
4. Redução de atrasos nas vendas; e
5. Mitigação de perdas por violação de dados.

Cisco 2024 *Data Privacy Benchmark Study***[15]**:

- 94% das organizações afirmam entender que seus clientes não adquirirão seus produtos e serviços se os dados não estiverem devidamente protegidos;
- Mais de 90% das organizações acreditam que precisam fazer mais para tranquilizar os clientes sobre o uso de seus dados com IA; e
- 98% das organizações estão relatando métricas de privacidade aos seus conselhos de administração.

IAPP-EY Privacy Governance Report 2023**[16]**:

- 33% das organizações relataram que suas equipes de privacidade cresceram no último ano e que o privacy by design foi identificado como estratégia prioritária;
- 70% das empresas que possuem um DPO estão confiantes em seu programa de privacidade, em comparação a 30% daqueles em organizações que não contam como um DPO; e
- 63% desses profissionais sentem a necessidade de mais recursos para atingir os objetivos de privacidade.

Na Europa, ação de fiscalização coordenada sobre a designação e cargo dos DPOs, de iniciativa do *European Data Protection Board* (EDPB)**[17]**, demonstrou que pode haver uma alocação insuficiente de recursos aos DPOs, sendo que alguns deles são contratados somente por meio período e outros se dividem entre demais funções, enquanto o EDPB indica que pode ser necessária inclusive a alocação de uma equipe dedicada ao DPO dependendo do tamanho da organização.

Ou seja, os dados apresentados mostram como pilares para uma maior valorização do tema e o aumento do orçamento destinado a proteção de dados dentro das organizações, trará retorno sobre o investimento, por meio da melhoria da confiança de clientes e parceiros de negócio e da necessidade de conformidade regulatória.

Acerca dos códigos de conduta, empresas ou entidades setoriais que lideram ou participam da sua criação têm a oportunidade de influenciar os parâmetros regulatórios do setor, ajustando-os às suas realidades operacionais, o que pode gerar eficiência e vantagens competitivas. Já os selos de conformidade, derivados desse tipo de iniciativa, podem funcionar como diferenciais comerciais, facilitando a entrada em novos mercados, especialmente internacionais, onde a demonstração de boas práticas em privacidade é cada vez mais exigida.

Por fim, a participação ativa em consultas públicas e tomadas de subsídios oferece uma oportunidade estratégica para que as empresas influenciem os rumos da regulamentação e adaptem as suas práticas antecipadamente, garantindo regulamentação proporcional que ao mesmo que tutela o indivíduo, permite o impulsionamento dos negócios.

SUGESTÕES DO VLK

É essencial que os agentes de tratamento acompanhem atentamente as iniciativas da ANPD e invistam no aprimoramento e na atualização de seus programas de Governança em Privacidade e Proteção de Dados, além de garantir a conformidade com a legislação já existente.

Além disso, pelas razões acima apontadas, a participação ativa em consultas públicas e interações com a ANPD é recomendável, tanto para se antecipar às exigências legais, quanto para exercer *advocacy* e influenciar, democraticamente, debates regulatórios em temas prioritários, a fim de garantir maior segurança jurídica às empresas e ao mercado como um todo.

Por fim, participar ativamente da elaboração e implementação de códigos de conduta setoriais, em parceria com associações representativas, é interessante sob a perspectiva de regulação privada, que depois pode ser reconhecida pelo Estado.

[1] A ANPD foi autorizada a realizar um processo seletivo simplificado para preencher 213 postos de trabalho. O órgão tem seis meses para soltar o edital com a abertura das inscrições. Atualmente, a ANPD conta com 141 servidores – quando foi criada em 2020, eram 50. Disponível em: https://www.telesintese.com.br/anpd-vai-preencher-213-vagas-com-servidores-temporarios/#google_vignette
[2] Em 6 de março de 2024, o senador Ângelo Coronel (PSD-BA) apresentou o Projeto de Lei nº 615/2024, que propõe alterações à Lei nº 13.848/2019 para fortalecer a autonomia da Autoridade Nacional de Proteção de Dados (ANPD). A iniciativa visa detalhar as prerrogativas da ANPD, equiparando-a às agências reguladoras e ao Conselho Administrativo de Defesa Econômica (Cade), assegurando-lhe autonomia funcional, decisória, administrativa e financeira, sem subordinação hierárquica. A ANPD, inicialmente vinculada à Presidência da República, foi transformada em autarquia de natureza especial em 2022. Contudo, essa mudança não especificou claramente o conceito de autarquia especial nem as prerrogativas administrativas necessárias para o pleno exercício de suas funções legais. O PL 615/2024 busca suprir essa lacuna, consolidando a autonomia da ANPD e alinhando-a às melhores práticas internacionais em proteção de dados. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/projeto-apresentado-no-senado-fortalece-autonomia-da-anpd#:~:text=O%20Senador%20%C3%82ngelo%20Coronel%20(PSD,Prote%C3%A7%C3%A3o%20de%20Dados%20(ANPD).
[3] Vide capítulo sobre IA deste E-book.
[4] Educação e capacitação em proteção de dados; Mecanismos, instâncias e práticas de conformidade de proteção de dados; Governança de dados (setor privado e setor público); Dados pessoais para o desenvolvimento econômico, tecnológico e a inovação; e dados abertos como infraestrutura crítica em conformidade com LGPD. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/grupos-de-trabalho/?_authenticator=b6eb3a05a4525642bd6ac568cc9f7fffa5566587
[5] CNPD envia contribuições para a Agenda Regulatória do biênio 2025-2026. Disponível em: https://www.gov.br/anpd/pt-br/cnpd-2/cnpd-envia-contribuicoes-para-a-agenda-regulatoria-do-bienio-2025-2026-1#:~:text=O%20CNPD%20encaminhou%20%C3%A0%20ANPD,a%20prote%C3%A7%C3%A3o%20integral%20de%20kidsinfluencers.

[6] Confira aqui a Agenda Regulatória 2025/2026 da ANPD: https://www.linkedin.com/posts/rony-vainzof-b456976_agenda-regulat%C3%B3ria-da-anpd-20252026-activity-7272563502114877440-WewU?utm_source=share&utm_medium=member_desktop
[7] Riscos e oportunidades da regulamentação de decisões automatizadas e IA pela ANPD. Disponível em: https://www.conjur.com.br/2024-nov-27/riscos-e-oportunidades-da-regulamentacao-de-decisoes-automatizadas-e-inteligencia-artificial-pela-anpd/
[8] Vide página da ANPD dedicada ao tema: https://www.gov.br/anpd/pt-br/assuntos/assuntos-internacionais/assuntos-internacionais-pt
[9] Processos de Fiscalização em Andamento. Disponível em: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao
[10] Relatório de Ciclo de Monitoramento (2023). Disponível em: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/2023-11-07-relatorio-do-ciclo-de-monitoramento-2023-versao-final-1-1.pdf
[11] Confira aqui: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340.
[12] Os precedentes do STJ nos primeiros quatro anos de vigência da Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/27102024-Os-precedentes-do-STJ-nos-primeiros-quatro-anos-de-vigencia-da-Lei-Geral-de-Protecao-de-Dados-Pessoais.aspx
[13] RECURSO ESPECIAL Nº 2147374 - SP (2022/0220922-8).
[14] Privacy's Growing Importance and Impact. CISCO 2023 DATA PRIVACY BENCHMARK STUDY. Disponível em: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2023.pdf?CCID=cc000160&DTID=esootr000875&OID=rptsc030828
[15] Cisco 2024 Data Privacy Benchmark Study. Disponível em: Por fim, a participação ativa em consultas públicas e tomadas de subsídios oferece uma oportunidade estratégica para que as empresas influenciem os rumos da regulamentação e adaptem as suas práticas antecipadamente, garantindo regulamentação proporcional que ao mesmo que tutela o indivíduo, permite o impulsionamento dos negócios.
[16] IAPP-EY Privacy Governance Report 2023. Disponível em: Por fim, a participação ativa em consultas públicas e tomadas de subsídios oferece uma oportunidade estratégica para que as empresas influenciem os rumos da regulamentação e adaptem as suas práticas antecipadamente, garantindo regulamentação proporcional que ao mesmo que tutela o indivíduo, permite o impulsionamento dos negócios.
[17] Launch of coordinated enforcement on role of data protection officers. Disponível em: https://www.edpb.europa.eu/news/news/2023/launch-coordinated-enforcement-role-data-protection-officers_en?utm_source=chatgpt.com

3) PROTEÇÃO DE DADOS PESSOAIS

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	A LGPD passará por novo momento, com a sua regulamentação e fiscalização pela ANPD, a futura Política Nacional de Proteção de Dados Pessoais e da Privacidade (PNPD) e por meio de parâmetros que estão sendo estabelecidos em decisões judiciais, inclusive de superior instância, no Poder Judiciário. Com isso, as empresas simplificarão sua governança para que seja realmente efetiva (e não apenas "de papel"), reforçando os processos de *privacy by design*. O tema de transferência internacional de dados também estará em foco e é provável que ocorra a decisão de adequação mútua entre Brasil e União Europeia (países sob o GDPR), até julho de 2025. Posteriormente há a tendência natural para reconhecimento de outros países que já foram reconhecidos pela EU. Ainda, vale acompanhar os pedidos junto à ANPD de cláusulas-padrão equivalentes, cláusulas contratuais específica e normas corporativas globais. Olhar atento para estas regulamentações e fiscalizações que devem ocorrer em 2025: Regulamentações: Direitos dos Titulares; Relatório de Impacto; Segurança da Informação; Decisões Automatizadas; Alto Risco; Crianças e Adolescentes; e Autorregulação Regulada. Fiscalizações: Publicização do Nome e Canais de Contato do Encarregado; Incidentes de Segurança; Decisões Automatizadas e Treinamento de IA; Raspagem de Dados; Agregadores de Dados; Crianças e Adolescentes; e Direitos dos Titulares.
POR QUE É TENDÊNCIA?	A Proteção de Dados seguirá como tema central na agenda regulatória brasileira para 2025, com destaque para: a PNPD; o fortalecimento da atuação da ANPD, já que há planos de aumento de contratações e de servidores de carreira , Projeto de Lei para fortalecer sua autonomia e ela pode ser a "autoridade competente" do novo marco legal de IA ; Agenda Regulatória 25-26 da ANPD e temas que serão objeto de futuras regulamentações, como IA, direitos dos titulares, alto risco, dados biométricos, crianças e adolescentes, entre outros; Fiscalizações e Sanções Administrativas; decisões judiciais de superior instância no Judiciário; e Códigos de Conduta e Autorregulação Regulada.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	A maior valorização do tema e o aumento do orçamento destinado a proteção de dados dentro das organizações, além de mitigar riscos regulatórios e reputacionais, trará retorno sobre o investimento, por meio da melhoria da confiança de clientes e parceiros de negócio.

3) PROTEÇÃO DE DADOS PESSOAIS

RESUMO EXECUTIVO

COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	Acerca dos códigos de conduta, empresas ou entidades setoriais que lideram ou participam da sua criação têm a oportunidade de influenciar os parâmetros regulatórios do setor, ajustando-os às suas realidades operacionais, o que pode gerar eficiência e vantagens competitivas. Já os selos de conformidade, derivados desse tipo de iniciativa, podem funcionar como diferenciais comerciais, facilitando a entrada em novos mercados, especialmente internacionais, onde a demonstração de boas práticas em privacidade é cada vez mais exigida.
SUGESTÕES DO VLK	É essencial que os agentes de tratamento acompanhem atentamente as iniciativas da ANPD e invistam no aprimoramento e atualização de seus programas de Governança em Privacidade e Proteção de Dados, além de garantir a conformidade com a legislação já existente. Além disso, a participação ativa em consultas públicas e interações com a ANPD é altamente recomendável também, tanto para se antecipar às exigências legais quanto para exercer *advocacy* e influenciar, democraticamente, nos debates regulatórios em temas prioritários, a fim de garantir maior segurança jurídica às empresas e ao mercado como um todo. Por fim, participar ativamente da elaboração e implementação de códigos de conduta setoriais, em parceria com associações representativas, é interessante sob a perspectiva de regulação privada, que depois pode ser reconhecida pelo Estado.

4) CIBERSEGURANÇA E RESPOSTA A INCIDENTES

TENDÊNCIAS PARA 2025

A pauta é complexa, densa e crítica, e vai muito além de fraudes e vazamento de dados, pois ataques cibernéticos podem travar organizações e países.

Relatório de Riscos Globais de 2024, do Fórum Econômico Mundial, elaborado para tomadores de decisão equilibrarem crises imediatas e desafios de longo prazo, aponta a insegurança cibernética como preocupação crítica nos dois cenários, no seguinte sentido: a rápida integração de novas tecnologias tem exposto parcela maior da população a exploração digital e física; os criminosos focam em indivíduos menos alfabetizados digitalmente e em infraestruturas menos seguras; o crime organizado adota modelos de negócios usando a tecnologia para expandir suas operações; os crimes cibernéticos oferecem receita de baixos risco e custo, sendo cada vez mais sofisticados, graças a tecnologias como a IA generativa, como nos ataques de *phishing*; há crescente preocupação de que ataques cibernéticos possam causar grandes interrupções em infraestruturas críticas, como redes de energia e sistemas de transporte.

Não por acaso, o custo global do cibercrime é projetado em USD 24 trilhões até 2027. Os pagamentos de *ransomware* atingiram USD 1,1 bilhão em 2023**[1]**. O mercado global de seguros cibernéticos tem crescido rapidamente, com prêmios brutos subscritos estimados em USD 14 bilhões em 2023 e projetados para chegar a USD 29 bilhões até 2027. Tendência preocupante observada é a falta de cobertura adequada para empresas de pequeno porte, que muitas vezes não têm recursos financeiros para investir em cibersegurança ou adquirir seguros cibernéticos. Ainda, 87% dos tomadores de decisão globais acredita que suas organizações estão inadequadamente protegidas contra ataques cibernéticos (MarshMcLennan e Zurich – 2024).

Estudo recente apoiado por B3, Abrasca e BCG**[2]**, envolvendo 181 empresas brasileiras, estimou que o impacto financeiro de ataques cibernéticos pode chegar a US$ 6,6 bilhões em média, com destaque para as grandes empresas de capital aberto.

Já o INCC, levantou os seguintes impactos na economia nacional**[3]**: cada ataque custa, em média, R$ 33.53 milhões à economia brasileira, com um custo estimado de R$ 1.545 por registro violado; a cada violação, cerca de 74 empregos são eliminados, refletindo a interrupção de atividades e a redução da capacidade operacional das empresas; cada ataque reduz, em média, R$ 26 milhões da renda brasileira, afetando diretamente o poder de compra dos trabalhadores. Este cenário gera uma redução de R$ 839 bilhões em massa salarial, ocasionando uma perda estimada de até 43%, além de 2,5 milhões de empregos,

representando 2,3% do total de empregos no Brasil. Considerando os impactos acima agregados, os prejuízos causados pelas violações de dados geram uma perda para a economia de até R$ 2,3 trilhões, o que representa 18% do PIB brasileiro.

Outro estudo, publicado pela Harvard Business Review em 2023, mostrou que quando empresa de capital aberto é alvo de ciberataque bem-sucedido, independentemente da tendência anterior do mercado, o preço das ações cai rapidamente, resultando em queda média de 7,5% no valor de mercado, juntamente com perda média de capitalização de mercado de aproximadamente US$ 5,4 bilhões.

Ainda, o Security Design Lab (SDL) mostrou que empresas que experimentam violações significativas de dados têm desempenho inferior ao índice NASDAQ em média 8,6% após um ano do incidente, podendo chegar a 11,9% após dois anos.

Ou seja, segurança cibernética é fundamental para a sobrevivência e competitividade das empresas e nações. É pauta organizacional e estratégica e não apenas técnica.

A cibersegurança tem se consolidado como uma das maiores prioridades para empresas em todo o mundo, especialmente no Brasil, onde a digitalização avança rapidamente. As discussões recentes de projetos de lei sobre Cibersegurança e a criação da Agência Nacional de Cibersegurança (ANCiber), demonstram o comprometimento do país com a criação de ambiente regulatório mais robusto para enfrentar as ameaças cibernéticas. Além disso, ganhou força a troca de informações com autoridades internacionais sobre incidentes cibernéticos, o que demonstra que o tema é realmente, sob diversas perspectivas, e uma tendência para o próximo ano.

POR QUE É TENDÊNCIA?

O Brasil, em termos normativos e de governança, vem se preparando para enfrentar referidos desafios, que reforçam a necessidade de uma abordagem proativa e sistemática para a proteção contra ameaças cibernéticas.

A Política Nacional de Cibersegurança (PNCiber)**[4]**, estabelece diretrizes para fortalecer a segurança cibernética no país, incluindo medidas como o desenvolvimento da educação, capacitação técnico-profissional e fomento à pesquisa científica em segurança cibernética; resiliência organizacional; desenvolvimento de produtos, serviços e tecnologias nacionais destinados à segurança cibernética; cooperação entre órgãos e entidades públicas e privadas em matéria de segurança cibernética; e adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, mitigar e neutralizar vulnerabilidades, incidentes e ataques cibernéticos.

Para implementar e acompanhar a PNCiber, foi criado o Comitê Nacional de Cibersegurança (CNCiber)**[5]**, responsável por orientar a atividade de cibersegurança no País, propor atualizações para a PNCiber, bem como avaliar e propor medidas para o

incremento da segurança cibernética no País, dentre outras competências. Em março de 2024, o CNCiber estabeleceu Grupos de Trabalho Temáticos (GTT), destacando-se:

- Atualização da Estratégia Nacional de Cibersegurança (e-Ciber): visa revisar e aprimorar a estratégia nacional vigente para alinhá-la às melhores práticas internacionais;

- Elaboração de Proposta de Projeto de Lei para Criação de Órgão de Governança da Cibersegurança Nacional: encarregado de desenvolver uma proposta legislativa para instituir um órgão dedicado à governança da cibersegurança no Brasil; e

- Definição de Parâmetros de Atuação Internacional do Brasil em Cibersegurança: Focado em estabelecer diretrizes para a participação do Brasil em questões internacionais de cibersegurança, este grupo busca fortalecer a cooperação técnica internacional.

A Resolução CD/ANPD nº 15/2024, aprovou o Regulamento de Comunicação de Incidente de Segurança, estabelecendo procedimentos para a notificação de incidentes que possam acarretar risco ou dano relevante aos titulares de dados pessoais, conforme o artigo 48 da LGPD.

A comunicação deverá ser feita por meio de formulário disponibilizado pela ANPD e deverá conter, no mínimo: descrição da natureza e categoria dos dados afetados; número de titulares afetados (especificando os vulneráveis); medidas técnicas de segurança utilizadas (antes, durante e após o incidente); riscos do incidente e possíveis impactos aos titulares; data da ocorrência; dados do Encarregado; identificação do controlador e do operador; descrição do incidente e causa principal; total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente; motivos da demora, caso a comunicação não tenha sido realizado no prazo previsto de três dias úteis; e medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares, quando cabíveis.

Para fins de transparência e prestação de contas, mesmo nos casos em que a comunicação não é necessária, o controlador deverá realizar e manter o registro do incidente de segurança, pelo prazo mínimo de 5 anos, contados a partir da data do registro, contendo, no mínimo: data de conhecimento do incidente; descrição geral das circunstâncias em que o incidente ocorreu; natureza e a categoria de dados afetados; número de titulares afetados; avaliação do risco e os possíveis danos aos titulares; medidas de correção e mitigação dos efeitos do incidente, quando aplicável; forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e motivos da ausência de comunicação, quando for o caso.

Sobre o tema, até o mês de setembro de 2024, a ANPD recebeu 1.063 comunicados de incidentes, os quais estão atualmente em processo de análise. Desse total, 250 incidentes

foram reportados apenas no ano de 2024, o que evidencia a contínua relevância e complexidade das questões envolvendo a segurança da informação e a proteção de dados pessoais no País. Com base nestas informações, a ANPD pode iniciar processos de fiscalização para verificar se os agentes regulados estão tratando dados pessoais em conformidade com a LGPD e a Resolução 15/24. Esse processo é caracterizado por um diálogo constante entre a ANPD e os agentes regulados, visando à adoção de medidas corretivas de forma cooperativa e eficaz.

A ANPD, inseriu como prioridade em sua agenda regulatória para 2025/2026, o tema Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança).

Em caso envolvendo vazamento de dados, houve recente decisão do STJ relevante em termos de governança empresarial:**[6]**

- Obrigação de Governança e Segurança (art. 49 da LGPD): a decisão afirma que os sistemas utilizados para o tratamento de dados pessoais deveriam estar estruturados para atender aos requisitos de segurança, boas práticas e governança, além dos princípios gerais da LGPD e normas regulamentares. A falta de implementação de tais medidas configurou a irregularidade no tratamento de dados.

- Compliance e Governança (art. 50 da LGPD): é mencionado que a empresa deveria ter adotado procedimentos e normas de governança, ferramentas de supervisão e mecanismos de mitigação de riscos relacionados ao tratamento de dados. A ausência desses elementos contribuiu para a vulnerabilidade que resultou no incidente de segurança.

- Falha na Segurança Esperada (art. 44, III, da LGPD): o tratamento de dados foi considerado irregular porque a segurança fornecida não correspondeu à "expectativa de legítima proteção". Foram consideradas as técnicas disponíveis na época, e a empresa não demonstrou que suas práticas eram adequadas para prevenir incidentes.

- Responsabilidade por Não Adotar Medidas Adequadas (art. 46 da LGPD): a empresa foi responsabilizada por não implementar medidas técnicas e administrativas capazes de proteger os dados de acessos não autorizados e de situações ilícitas ou inadequadas, como destruição, perda, alteração ou comunicação de dados.

- Impossibilidade de Comprovação de Excludente de Responsabilidade (art. 43, III, da LGPD): a decisão destacou que a empresa não conseguiu provar que o vazamento foi exclusivamente decorrente de culpa de terceiro (ataque *hacker*). Essa ausência de comprovação reforçou a falta de governança e medidas preventivas adequadas.

Em termos setoriais, a Resolução Anatel nº 767/24, introduziu alterações significativas no Regulamento de Segurança Cibernética aplicada ao setor de telecomunicações,

inicialmente aprovado pela Resolução nº 740/2020, ampliando seu escopo de aplicação, avaliação de fornecedores e dever de notificação à ANATEL incidentes relevantes e aqueles notificados à ANPD. Ela se soma as normas já existentes em outros setores, como a Resolução CMN nº 4.893/2021, que estabelece diretrizes para a política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem por instituições financeiras, além da Circular Susep nº 638/2021, que dispõe sobre requisitos de segurança cibernética a serem observados por sociedades seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.

Já em âmbito internacional, destacam-se:

- A implementação das novas regras da Comissão de Valores Mobiliários dos Estados Unidos (SEC) para aprimorar a transparência e gestão de riscos cibernéticos por parte das empresas de capital aberto. Essas medidas visam fornecer aos investidores informações mais precisas e oportunas sobre incidentes de segurança cibernética e as práticas de governança das empresas nesse contexto, como a obrigação de relatar incidentes de segurança cibernética considerados materiais no Formulário 8-K, no prazo de quatro dias úteis após determinarem a materialidade do incidente**[7]**; e responsabilidade do conselho de administração e da alta administração na supervisão e gestão de riscos cibernéticos, destacando a necessidade de expertise nessa área; e

- Na União Europeia, a *Digital Operational Resilience Act* (DORA) é regulamento que estabelece requisitos obrigatórios para fortalecer a resiliência operacional digital de instituições financeiras, aplicável a partir de janeiro de 2025. O regulamento abrange bancos, seguradoras, gestores de ativos e fornecedores críticos de tecnologia, exigindo governança robusta de riscos de TI, monitoramento e resposta a incidentes, testes regulares de resiliência e supervisão de terceiros. A DORA visa proteger o setor financeiro contra interrupções e ciberataques, promovendo estabilidade, confiança e uma abordagem harmonizada em todos os Estados-Membros da UE.

COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?

A crescente ameaça de ataques cibernéticos impacta diretamente a continuidade dos negócios e a reputação das organizações. O fortalecimento das políticas públicas e o surgimento de leis específicas sobre cibersegurança exigem que as empresas invistam em governança e segurança digital. Organizações que não se adaptam a esse novo cenário correm o risco de sofrer danos financeiros e reputacionais irreparáveis.

A implementação de políticas de segurança da informação, treinamentos contínuos para colaboradores, simulações de incidentes, incluindo o preenchimento de formulário de comunicação à ANPD, e testes de vulnerabilidades são ações essenciais para garantir que as empresas possam responder de maneira rápida e eficiente a qualquer ataque**[8]**. Além disso, a necessidade de metodologia estruturada para análise de riscos, resposta a

incidentes e notificação às autoridades exige um planejamento e execução rigorosos. Empresas que não investem adequadamente em cibersegurança podem enfrentar consequências devastadoras, tanto financeiras quanto em termos de confiança do cliente.

Sob a perspectiva da LGPD, conforme a Resolução CD/ANPD 4/2023, que regulamenta a dosimetria das sanções administrativa, vale lembrar que prevenir é necessário também para atenuar eventuais sanções, pois:

- A definição do valor-base para multa simples deve considerar o faturamento do infrator no último exercício disponível anterior à aplicação da sanção, excluídos os tributos, relativo ao ramo de atividade empresarial em que ocorreu a infração. Ou seja, uma boa governança de dados pode impedir que o cálculo seja iniciado com base no grupo econômico;

- Um dos critérios para poder ser caracterizada infração grave é "o infrator auferir ou pretender auferir vantagem econômica em decorrência da infração cometida" e o valor mínimo para multa será o dobro da vantagem econômica decorrente da infração para os casos em que a vantagem auferida ou pretendida pelo infrator seja estimável. A vantagem auferia ou pretendida pode ser direta ou indireta. A vantagem direta é aquela em que o infrator obtém recursos financeiros em decorrência da infração, como, por exemplo, aqueles decorrentes da venda ilegal de dados pessoais. Já a vantagem indireta pode ser todo o custo ou investimento que o infrator deixou de fazer em decorrência da infração, como, por exemplo, o custo que um agente de tratamento não tem ao deixar de investir em uma ferramenta mais eficaz de segurança da informação.

- A adoção de política de boas práticas e governança pode atenuar em 20% as sanções;

- Identificar e cessar a infração pode reduzir as sanções em 75%, se previamente à instauração de procedimento preparatório pela ANPD; 50%, se após a instauração de procedimento preparatório e até a instauração de processo administrativo sancionador; ou 30%, se após a instauração de processo administrativo sancionador e até a prolação da decisão de primeira instância no âmbito do processo administrativo sancionador.

SUGESTÕES DO VLK

São diversas as estratégias e sugestões, incluindo:

- Desenvolvimento de capacidades nacionais de prevenção, monitoramento, análise e resposta para detectar e gerenciar incidentes;
- Diretrizes para que se avance a maturidade e a resiliência cibernética;
- Aumentar a conscientização e a educação sobre os riscos cibernéticos, tanto para empresas quanto para o público em geral, pois 98% dos ataques cibernéticos seriam

evitados com cuidados básicos (higiene digital), como usar antimalware, manter versões atualizadas dos sistemas, habilitar múltiplos fatores de autenticação, controle de acessos e governança de credenciais (2022 Microsoft Digital Defense Report);

- O Conselho de Administração das empresas assumirem papel de protagonista no desenvolvimento de cultura empresarial, transmitindo a visão de que segurança cibernética é um risco estratégico, mais do que tecnológico;
- Elevar o conhecimento e responsabilidades sobre o tema no próprio board, pois apesar de 77% dos membros do conselho acreditarem que segurança cibernética é uma das prioridades do conselho, pouco menos de 2% deles têm experiência relevante no tema (Microsoft Security, 2023);
- Troca de experiências e informações de inteligência sobre incidentes entre organizações para antever ameaças, impactos e adotar medidas preventivas;
- Incentivar parcerias público-privadas para melhorar a coleta e a análise de dados, além de promover políticas mais eficazes contra riscos cibernéticos;
- Ter um bom plano de resposta a incidentes com simulações periódicas. Empresas que simulam incidentes, avaliando o processo de resposta já existente, fortalecem significativamente sua capacidade de atuar de forma mais adequada em um cenário real. Um plano de resposta adequado e equipe treinada, traz, em média, US$ 2,66 milhões a menos de prejuízo no caso de ataques cibernéticos (IBM, 2022);
- Análise de riscos cibernéticos e resiliência na cadeia de suprimentos e terceirização, avaliando quais são os fornecedores mais críticos e como um ataque cibernético contra esses terceiros pode afetar seus negócios ou dados pessoais de seus clientes; e
- Criar incentivos e subsídios em cibersegurança, ajudando especialmente empresas de pequeno porte a adotarem boas práticas, de forma a estimular empresas medidas preventivas.

Fortalecer a cibersegurança da organização com abordagem proativa é o melhor caminho para enfrentar esses desafios. É preciso a conscientização das empresas sobre a importância em se investir numa estrutura de governança robusta, que inclua políticas de segurança da informação bem definidas, treinamentos periódicos e testes de resistência a ataques.

[1] Fechando a lacuna de proteção contra riscos cibernéticos. Disponível em: https://www.marshmclennan.com/insights/publications/2024/september/closing-the-cyber-protection-gap.html
[2] Em sua segunda edição, pesquisa de Cibersegurança do país indica leve aumento no nível de segurança das companhias. Disponível em: https://tiinside.com.br/02/12/2024/em-sua-segunda-edicao-pesquisa-de-ciberseguranca-do-pais-indica-leve-aumento-no-nivel-de-seguranca-das-companhias/?utm_source=chatgpt.com
[3] O impacto das Violações de dados na Economia brasileira com foco nas pequenas E médias empresas | 2024. Instituto Nacional de Combate ao Cibercrime.
[4] Instituída pelo Decreto nº 11.856, de 26 de dezembro de 2023

[5] Presidido pelo Gabinete de Segurança Institucional da Presidência da República, é composto por 16 membros permanentes dentre órgãos da Administração Pública Federal e por nove representantes da Sociedade Civil, sendo três de entidades relacionadas à cibersegurança ou à garantia de direitos fundamentais no ambiente digital, três de instituições acadêmicas relacionadas à área de cibersegurança e três de entidades representativas do setor empresarial ligado ao tema. Para mais informações: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber?utm_source=chatgpt.com

[6] BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2147374/SP. Recorrente: Eletropaulo Metropolitana Eletricidade de São Paulo S.A. Recorrido: Thayna Nayara da Silva Queiroz. Relator: Ministro Ricardo Villas Bôas Cueva. Decisão proferida em 04 de dezembro de 2024. Brasília: Diário de Justiça Eletrônico/STJ, 06 dez. 2024.

[7] A divulgação deve incluir detalhes sobre a natureza, escopo, timing do incidente e seu impacto material ou potencial impacto material nas condições financeiras e nos resultados operacionais da empresa.

[8] E-BOOK - Comunicação de Incidentes de Segurança. Infográficos interativos. Q&A - Resolução 15/2024 da ANPD. Visão da ANPD, conforme suas Notas Técnicas / Sanções Administrativas. Disponível em: https://vlklaw.com.br/wp-content/uploads/2024/06/Serie-Comunicacao-de-Incidentes-1_compressed.pdf

4) CIBERSEGURANÇA E RESPOSTA A INCIDENTES

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Os ataques cibernéticos ficarão ainda mais sofisticados, com o crescente uso de IA para personalizar as invasões, de todos os tipos – para obtenção de dados pessoais, segredos de negócios ou até mesmo para travar a operações de grandes organizações. As demandas na ANPD e no Judiciário também devem se avolumar, sendo importante acompanhar como será a estabilização da jurisprudência e sanções administrativas, havendo previsão de que os tribunais e a ANPD tenham interpretação mais focada na governança das corporações (preventiva e reativa) e transparência calibrada de acordo com o risco e contexto do incidente (para o mercado, clientes, titulares de dados e parceiros de negócio). A ANPD, inseriu como prioridade em sua agenda regulatória para 2025/2026, o tema Medidas de segurança, técnicas e administrativas (incluindo padrões técnicos mínimos de segurança). Baseado no contexto internacional (SEC – EUA), os Conselhos de Administração devem ter papel e responsabilidades mais ativas no tema. A Política Nacional de Proteção de Cibersegurança deve ganhar tração e é provável a criação de uma agência governamental com foco em segurança cibernética, no segundo semestre de 2025. Por fim, setores críticos poderão ter regulamentações específicas criadas ou atualizadas pelos seus respectivos reguladores.
POR QUE É TENDÊNCIA?	A Política Nacional de Cibersegurança (PNCiber), estabelece diretrizes para fortalecer a segurança cibernética no país, incluindo medidas como o desenvolvimento da educação, capacitação técnico-profissional e fomento à pesquisa científica em segurança cibernética; resiliência organizacional; desenvolvimento de produtos, serviços e tecnologias nacionais destinados à segurança cibernética; cooperação entre órgãos e entidades públicas e privadas em matéria de segurança cibernética; e adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, mitigar e neutralizar vulnerabilidades, incidentes e ataques cibernéticos. Para implementar e acompanhar a PNCiber, foi criado o Comitê Nacional de Cibersegurança (CNCiber), que está trabalhando na atualização da Estratégia Nacional de Cibersegurança (e-Ciber) e na elaboração de Proposta de Projeto de Lei para Criação de Órgão de Governança da Cibersegurança Nacional. A Resolução CD/ANPD nº 15/2024, aprovou o Regulamento de Comunicação de Incidente de Segurança, estabelecendo procedimentos para a notificação de incidentes que possam acarretar risco ou dano relevante aos titulares de dados pessoais, conforme o artigo 48 da LGPD. Sobre o tema, até o mês de setembro de 2024, a ANPD recebeu 1.063 comunicados de incidentes, os

4) CIBERSEGURANÇA E RESPOSTA A INCIDENTES

RESUMO EXECUTIVO

POR QUE É TENDÊNCIA?	quais estão atualmente em processo de análise. Desse total, 250 incidentes foram reportados apenas no ano de 2024, o que evidencia a contínua relevância e complexidade das questões envolvendo a segurança da informação e a proteção de dados pessoais no País. Com base nestas informações, a ANPD pode iniciar processos de fiscalização para verificar se os agentes regulados estão tratando dados pessoais em conformidade com a LGPD e a nova Resolução. Nos Tribunais, o STJ decidiu responsabilizar uma empresa por vazamento de dados em razão da impossibilidade de comprovação de excludente de responsabilidade (art. 43, III, da LGPD): a decisão destacou que a empresa não conseguiu provar que o vazamento foi exclusivamente decorrente de culpa de terceiro (ataque hacker). Essa ausência de comprovação reforçou a falta de governança e medidas preventivas adequadas. Em termos internacionais, destacam-se: (i) a implementação das novas regras da Comissão de Valores Mobiliários dos Estados Unidos (SEC) para aprimorar a transparência e a gestão de riscos cibernéticos por parte das empresas de capital aberto, especialmente a obrigação de relatar incidentes de segurança cibernética considerados materiais e responsabilidade do conselho de administração e da alta administração na supervisão e gestão de riscos cibernéticos, destacando a necessidade de expertise nessa área; e (ii) na União Europeia, a *Digital Operational Resilience Act* (DORA), um regulamento que estabelece requisitos obrigatórios para fortalecer a resiliência operacional digital de instituições financeiras, aplicável a partir de janeiro de 2025.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	A crescente ameaça de ataques cibernéticos impacta diretamente a continuidade dos negócios e a reputação das organizações. O fortalecimento das políticas públicas e o surgimento de leis específicas sobre cibersegurança exigem que as empresas invistam em governança e segurança digital. Organizações que não se adaptam a esse novo cenário correm o risco de sofrer danos financeiros e reputacionais irreparáveis.
SUGESTÕES DO VLK	Realizar simulações de resposta a incidentes e estratégias integradas de recuperação; • Desenvolvimento de capacidades nacionais de prevenção, monitoramento, análise e resposta para detectar e gerenciar incidentes; • Diretrizes para que se avance a maturidade e a resiliência cibernética; • Aumentar a conscientização e a educação sobre os riscos cibernéticos, tanto para empresas quanto para o público em geral, pois a grande maioria dos ataques cibernéticos seriam evitados com cuidados básicos (higiene digital); • O Conselho de Administração das empresas assumirem papel de protagonista no desenvolvimento de cultura empresarial, transmitindo a visão de que segurança cibernética é um risco estratégico, mais do que tecnológico;

4) CIBERSEGURANÇA E RESPOSTA A INCIDENTES

RESUMO EXECUTIVO

SUGESTÕES DO VLK	• Elevar o conhecimento e responsabilidades sobre o tema no próprio board; • Troca de experiências e informações de inteligência sobre incidentes entre organizações para antever ameaças, impactos e adotar medidas preventivas; • Incentivar parcerias público-privadas para melhorar a coleta e a análise de dados, além de promover políticas mais eficazes contra riscos cibernéticos; • Ter um bom plano de resposta a incidentes com simulações periódicas; • Análise de riscos cibernéticos e resiliência na cadeia de suprimentos e terceirização; e • Criar incentivos e subsídios em cibersegurança, ajudando especialmente empresas de pequeno porte a adotarem boas práticas, de forma a estimular empresas medidas preventivas.

5) GOVERNANÇA DIGITAL ESTRUTURADA

TENDÊNCIAS PARA 2025

Novas tecnologias, ferramentas, gerações e habilidades trazem natural atrito em um momento relevante da revolução tecnológica em que não há mais como separar o físico do digital.

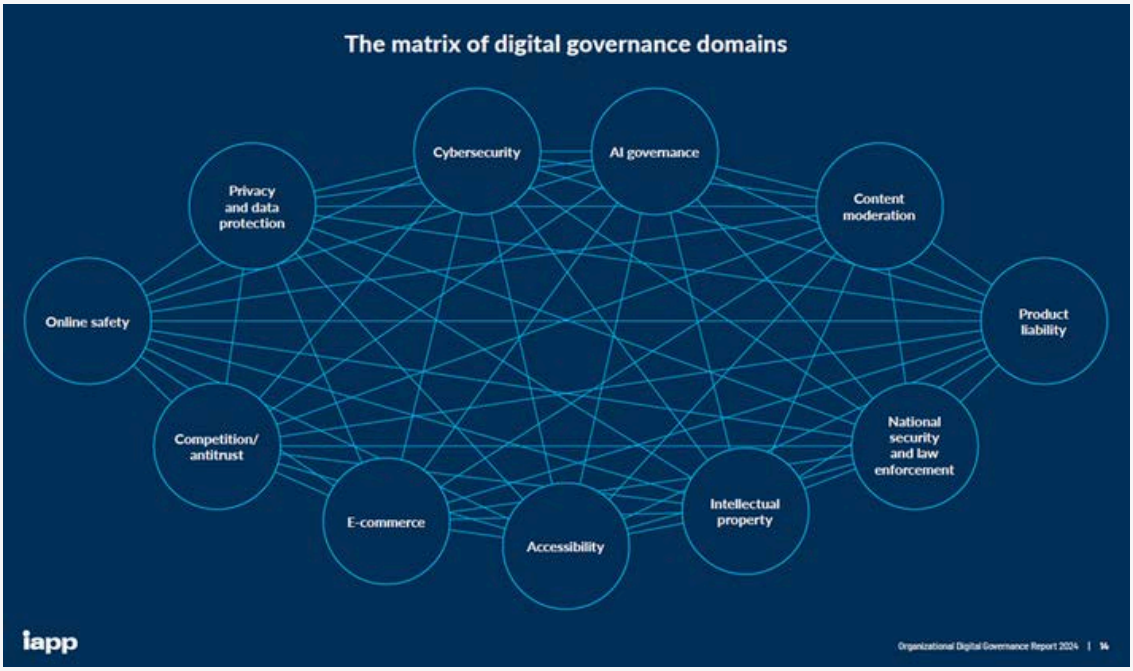
Empresas privadas e órgãos do Estado que não nasceram digitais, inevitavelmente estão em fase de digitalização e emprego de inovações. Elas são condicionantes para o desenvolvimento econômico e social no século 21.

Para a revolução tecnológica ser ainda mais potente, vibrante e melhorar a vida das pessoas, é preciso haver confiança digital, que se sustenta na estruturação de sólida governança do tripé segurança cibernética, proteção de dados pessoais e inteligência artificial ética e responsável, a chamada Governança Digital Estruturada (GDE).

POR QUE É TENDÊNCIA?

Nos últimos anos, as organizações têm se valido do conhecimento e expertise de governança de outras áreas, como compliance em anticorrupção, ambiental e cibersegurança, como legado estrutural para novas legislações da economia digital, como privacidade e ética em IA. Organizações mais maduras estão combinando comitês específicos para IA e privacidade com uma governança ampla, com o objetivo de apoiar decisões de ética digital e garantir a conformidade com as normas regulatórias em constante atualização, oferecendo assim uma base sólida para o crescimento empresarial responsável e sustentável.

A governança digital, que envolve desde proteção de dados, governança de IA e segurança cibernética, está se tornando prioridade nas empresas. Esse movimento é impulsionado por vários fatores, incluindo a aplicação mais intensa da LGPD, que já exige uma governança de privacidade mais madura, e pela crescente obrigações decorrentes dos riscos da IA e cibersegurança, seja por legislações já existentes ou novas regulamentações surgindo, com a expectativa de aprovação de novos marcos legais previstos para 2025. Esses fatores exigem que as empresas integrem essas diferentes camadas de governança em um modelo coeso e eficiente.



[1]

Ou seja, a governança digital não pode mais ser tratada de forma isolada. As estruturas existentes de governança de privacidade, que já possuem um bom nível de maturidade, estão sendo adaptadas para garantir a responsabilidade ética na aplicação de tecnologias emergentes, como a IA.

Em relatório recente do IAPP**[2]**, baseado em pesquisa qualitativa, utilizando entrevistas com mais de 20 líderes seniores de grandes empresas multinacionais, provavelmente mais maduras em suas abordagens à governança organizacional, revelou os seguintes dados sobre o papel do CPO (*Chief Privacy Officer*) e expansão de suas responsabilidades:

- 69% dos CPOs também são responsáveis pela governança de dados e ética de dados;
- 55% dos profissionais de privacidade trabalham em funções com responsabilidades de governança de IA;
- 37% dos CPOs respondem pela conformidade regulatória em cibersegurança;
- 32% dos profissionais de privacidade cobrem a conformidade regulatória em cibersegurança;
- Mais de 80% das equipes de privacidade assumiram responsabilidades além da privacidade; e
- 58% dos profissionais de privacidade também se ocupam da governança de dados e ética de dados.

Acerca de IA Generativa, apesar de 65% das organizações a utilizarem regularmente, apenas 18% têm um conselho ou diretoria empresarial com autoridade para tomar decisões envolvendo governança de IA responsável (McKinsey – 2024**[3]**).

Já a pesquisa realizada pela ABRASCA**[4]**, explorando a governança de IA nas empresas de capital aberto no Brasil, revela números que ilustram o estágio inicial da adoção e os desafios enfrentados:

Pesquisa Quantitativa:

- 40% das empresas não possuem uma estratégia de IA definida;
- 55% das empresas afirmam que a IA é pauta do Conselho de Administração;
- 61% reconhecem a sua relevância estratégica para a sustentabilidade;
- 72% dos Conselhos e C-Level demonstram pouca atenção aos processos de governança e gestão de riscos de IA;
- 41% das empresas possuem estratégias de gestão de riscos voltadas para a IA;
- 79% das empresas se preocupam com a segurança e privacidade dos dados;
- 10% se preocupam com as questões éticas;
- 42% das empresas declaram ter instâncias para avaliar questões éticas relacionadas à IA;
- 64% admitem que essas estruturas não estão preparadas para a função;
- 77% das empresas demonstram baixa incorporação dos impactos da IA na agenda ESG e em seus relatórios de sustentabilidade; e
- 76% das empresas não possuem programas de sensibilização em governança de IA para seus colaboradores.

Pesquisa qualitativa (entrevistas com membros do Conselho de Administração, CEOs, e responsáveis pela área de tecnologia):

- Nível de maturidade da governança de IA: a maioria das empresas ainda está em estágio inicial de estruturação da governança de IA, com poucas diretrizes formalizadas e estruturas de gestão de riscos;
- Percepções sobre os riscos da IA: evidenciou a preocupação das empresas com os riscos relacionados à segurança e privacidade dos dados, mas também a falta de conscientização sobre os desafios éticos e os impactos da IA na sociedade; e
- Papel da liderança na governança da IA: destacou a importância do engajamento do Conselho de Administração e do C-Level na definição da estratégia de IA e na promoção de uma cultura de uso responsável da tecnologia.

COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?

A convergência da rápida inovação tecnológica, regulamentações em expansão, importância da confiança e conscientização sobre os riscos digitais impulsiona a Governança Digital Estruturada (GDE). As organizações que não priorizarem a governança digital enfrentarão desafios crescentes em termos de conformidade, gerenciamento de riscos, reputação e competitividade.

A adoção de uma GDE traz diversos impactos positivos para os negócios. A definição clara de funções, responsabilidades e fluxos de decisão entre os comitês de IA e privacidade garante coerência e conformidade, além de mitigar riscos legais e reputacionais. Empresas que adotam esse modelo estão mais preparadas para enfrentar desafios relacionados à

proteção de dados, à ética de IA e à segurança cibernética, além de estarem mais alinhadas com as regulamentações locais e globais.

De acordo com pesquisas da *International Association of Privacy Professionals* (IAPP), 50% das organizações que estão desenvolvendo governança de IA fazem isso sobre a base de programas de privacidade maduros. Essa abordagem pode gerar processo mais eficiente e coeso, além de reduzir a necessidade de novos frameworks de governança do zero.

A integração de governança de IA com privacidade e ética cria um ambiente corporativo mais estruturado, que gera maior confiança por parte dos consumidores, investidores e demais stakeholders. Organizações que demonstram responsabilidade e transparência em suas práticas de governança têm mais chances de se destacar em um mercado cada vez mais competitivo e regulado.

SUGESTÕES DO VLK

Abordagem mais madura e eficaz deve focar na coordenação, coesão e consolidação entre os diferentes domínios da governança digital, visando superar os desafios da fragmentação e complexidade inerentes à era digital, conforme os seguintes elementos-chave:

- Definição Clara e Estruturada: é crucial definir o que a governança digital significa para a organização, estabelecendo um framework que delineia os domínios, responsabilidades e linhas de reporte.
- Coordenação Interdisciplinar: a governança digital não deve ser responsabilidade de um único departamento ou indivíduo. É essencial promover a colaboração entre áreas como privacidade, segurança da informação, tecnologia, jurídico, governança de dados e ética.
- Comitês de Governança: comitês específicos para cada domínio, com a participação de representantes das áreas relevantes, facilitam a tomada de decisões e a coordenação de atividades.
- Conscientização e Responsabilização: a primeira linha de defesa, que inclui as equipes operacionais, precisa estar ciente dos riscos digitais e assumir responsabilidades pela sua gestão.
- Funções de Monitoramento e Auditoria: a segunda linha, composta por funções como gerenciamento de riscos e conformidade, deve monitorar e testar os controles implementados pela primeira linha. a auditoria interna, de terceira linha, deve ter uma visão abrangente dos riscos digitais, incluindo aspectos financeiros e não financeiros.
- Automação e Tecnologia: a automação de controles, a utilização de IA e a análise de dados contribuem para a eficiência da governança digital.
- Políticas Claras e Integradas: as políticas relacionadas a dados e tecnologias digitais devem ser consolidadas e simplificadas, com controles que abrangem múltiplas áreas.
- Cultura de Governança: a governança digital deve ser incorporada à cultura da organização, com ênfase na ética, na transparência e na responsabilização.

Sugestão prática para as empresas é o melhor aproveitamento da estrutura de governança de privacidade já estabelecida, combinando-a com as novas demandas relacionadas à IA e cibersegurança. O encarregado de proteção de dados pode expandir seu papel para incluir questões relacionadas à ética digital, desde que isso não implique em conflitos de interesse.

A coordenação, coesão e consolidação entre e os papéis do CPO (*Chief Privacy Officer*), *Chief Security Officer* (CSO) e do CAIO (*Chief AI Governance Officer*) são cruciais nesse processo, pois essa tendência reflete a crescente interconexão entre os diferentes domínios da governança digital e a necessidade de uma abordagem integrada.

Assim, as organizações podem não apenas mitigar riscos, mas também fomentar a confiança e alcançar um crescimento sustentável, aproveitando a convergência entre privacidade e ética digital para transformar desafios em oportunidades.

[1] Organizational Digital Governance Report 2024. IAPP.
[2] Organizational Digital Governance Report 2024. IAPP.
[3] A pesquisa global da McKinsey sobre inteligência artificial (IA) em 2024 entrevistou 1.684 participantes de diversas regiões e setores.
[4] GOVERNANÇA E ÉTICA. Da Inteligência Artificial nas Companhias Abertas. Disponível em: https://s3-sa-east-1.amazonaws.com/abrasca/GovernancaEtica/8862-Relatorio-Final-Governanca-e-Etica-da-IA-nas-Cias-Abertas-Abrasca-Kaufman-e-Zavaglia.pdf

5) GOVERNANÇA DIGITAL ESTRUTURADA

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Solidificação do tripé segurança cibernética, proteção de dados pessoais e inteligência artificial ética e responsável, a chamada Governança Digital Estruturada (GDE), com empresas adotando estruturas mais eficazes e harmonizadas de governança e Conselhos e Conselheiros(as) especificamente designados para o tema, dentro do contexto de inovação responsável. Acreditamos que haverá a busca por harmonização de frameworks globais, como já há movimentos em proteção de dados, visando maior fluidez de tecnologias, dados, produtos e serviços entre as diversas nações. Por fim, deverá se consolidar a integração da governança digital às métricas ambientais, sociais e de governança (ESG), havendo forte apelo do mercado sobre o assunto.
POR QUE É TENDÊNCIA?	A governança digital não pode mais ser tratada de forma isolada. Organizações mais maduras estão combinando comitês específicos para IA e privacidade com uma governança ampla, com o objetivo de apoiar decisões de ética digital e garantir a conformidade com as normas regulatórias em constante atualização, oferecendo assim uma base sólida para o crescimento empresarial responsável e sustentável. Esse movimento é impulsionado por vários fatores, incluindo a aplicação mais intensa da LGPD, que já exige uma governança de privacidade mais madura, e pela crescente obrigações decorrentes dos riscos da IA e cibersegurança, seja por legislações já existentes ou novas regulamentações surgindo, com a expectativa de aprovação de novos marcos legais previstos para 2025. Esses fatores exigem que as empresas integrem essas diferentes camadas de governança em um modelo coeso e eficiente.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	As organizações que não priorizarem a governança digital estruturada enfrentarão desafios crescentes em termos de conformidade, gerenciamento de riscos, reputação e competitividade. A adoção de uma GDE traz diversos impactos positivos para os negócios. A definição clara de funções, responsabilidades e fluxos de decisão entre os comitês de IA e privacidade garante coerência e conformidade, além de mitigar riscos legais e reputacionais. Empresas que adotam esse modelo estão mais preparadas para enfrentar desafios relacionados à proteção de dados, à ética de IA e à segurança cibernética, além de estarem mais alinhadas com as regulamentações locais e globais.
SUGESTÕES DO VLK	• Definir o que a governança digital significa para a organização, estabelecendo um framework que delineia os domínios, responsabilidades e linhas de reporte. • A governança digital não deve ser responsabilidade de um único departamento ou indivíduo. É essencial promover a colaboração entre áreas como privacidade, segurança da informação, tecnologia, jurídico, governança de dados e ética.

5) GOVERNANÇA DIGITAL ESTRUTURADA

RESUMO EXECUTIVO

SUGESTÕES DO VLK	• Comitês específicos para cada domínio, com a participação de representantes das áreas relevantes, facilitam a tomada de decisões e a coordenação de atividades. • A primeira linha de defesa, que inclui as equipes operacionais, precisa estar ciente dos riscos digitais e assumir responsabilidades pela sua gestão. • A segunda linha, composta por funções como gerenciamento de riscos e conformidade, deve monitorar e testar os controles implementados pela primeira linha. A auditoria interna, de terceira linha, deve ter uma visão abrangente dos riscos digitais, incluindo aspectos financeiros e não financeiros. • A automação de controles, a utilização de IA e a análise de dados contribuem para a eficiência da governança digital. • As políticas relacionadas a dados e tecnologias digitais devem ser consolidadas e simplificadas, com controles que abrangem múltiplas áreas. • A governança digital deve ser incorporada à cultura da organização, com ênfase na ética, na transparência e na responsabilização. Sugestão prática para as empresas é o melhor aproveitamento da estrutura de governança de privacidade já estabelecida, combinando-a com as novas demandas relacionadas à IA e cibersegurança, excluindo as hipóteses de conflito de interesse.

6) SOBERANIA DIGITAL COMPETITIVA

TENDÊNCIAS PARA 2025

A soberania digital pode ser analisada a partir de diferentes perspectivas, incluindo a jurídica, tecnológica, cibersegurança e econômica. Trata-se de tema relevante em mundo cada vez mais conectado, em que o controle e o acesso a dados, tecnologias e infraestruturas têm implicações estratégicas e éticas.

Jurídica: refere-se à capacidade de um Estado de criar, implementar e fazer cumprir leis e regulamentos.

Tecnológica: diz respeito ao domínio de um país sobre sua infraestrutura digital (servidores, redes, data centers) e tecnologias críticas, como inteligência artificial, semicondutores e criptografia.

Cibersegurança: inclui medidas contra ciberataques, espionagem digital e manipulação de dados; desenvolvimento de políticas nacionais e cooperação internacional para garantir resiliência cibernética; e proteção de infraestruturas críticas e sistemas estratégicos contra ameaças externas;

Econômica: refere-se à capacidade de uma nação de proteger suas indústrias e promover inovação local, sem depender excessivamente de fornecedores ou plataformas globais.

Mas a soberania digital deve ser competitiva, equilibrada e estratégica, sem cair em ufanismo digital que priorize isolamento ou protecionismo extremo. Essa abordagem pragmática permite que países e organizações alcancem autonomia tecnológica e segurança, mas sem comprometer os benefícios da colaboração global, da inovação e do comércio internacional.

POR QUE É TENDÊNCIA?

O Brasil ocupa papel crucial no cenário global como potência emergente, mas enfrenta desafios significativos relacionados à dependência tecnológica**[1].** Ante este cenário, há diversas iniciativas do Legislativo, Judiciário e Executivo a fim de mitigar esse risco.

Por exemplo, no Brasil, não importa o local em que dados são armazenados ou se a empresa tem sede no Brasil. Se há exploração do mercado brasileiro ou alguma parte do tratamento dessas informações ocorrer em nosso país, deverá obrigatoriamente ser

respeitada a legislação nacional, como expressamente consta no Marco Civil da Internet (MCI) e na LGPD. Nessa linha, a discussão sobre a obrigação de os data centers terem sede no Brasil já foi ultrapassada (foi rechaçada depois de amplo debate público durante o MCI), pois onera a operação, não contribui para a segurança dos dados e limita o uso de novas soluções tecnológicas. Fato é que mesmo que os servidores tenham suas sedes nos Estados Unidos ou na Europa, por exemplo, poderão ficar sujeitos às regras e decisões judiciais brasileiras.

Em termos de IA, a soberania digital competitiva emerge como uma prioridade estratégica no Brasil, impulsionada pelo PBIA (Plano Brasileiro de Inteligência Artificial), divulgado elo Governo Federal no segundo semestre de 2024. Com um investimento projetado de R$ 23 bilhões entre 2024 e 2028, o Governo Federal busca fortalecer a infraestrutura tecnológica, incluindo uma "nuvem soberana" para armazenamento e tratamento de dados exclusivamente em território nacional. Essa iniciativa também visa reduzir a dependência de *big techs* estrangeiras e estimular o desenvolvimento de soluções tecnológicas adaptadas às necessidades locais, como IA para setores-chave, incluindo biodiversidade, saúde e logística**[2].**

Porém, apesar dos avanços, é preciso fortalecer a colaboração internacional com líderes globais, priorizar áreas estratégicas para maximizar o impacto dos recursos e detalhar medidas práticas para viabilizar a execução do plano. Questões como acesso à tecnologia, migração de talentos e alinhamento de prioridades econômicas são cruciais para transformar o PBIA em uma estratégia factível e competitiva**[3].**

Além disso, o conceito de soberania digital ganha relevância global, com países como os Estados Unidos e China investindo massivamente em IA e semicondutores para fortalecer sua autonomia tecnológica. A implementação de uma nuvem soberana no Brasil, liderada pelo Serpro, promete proteger dados estratégicos de setores como SUS e Embrapa, reforçando a privacidade e segurança cibernética no país**[4]**.

Ou seja, dados, algoritmos, capacidade computacional, conectividade, energia elétrica, talentos, cibersegurança e regulamentação de riscos, no contexto brasileiro, permitem traçar um panorama abrangente da soberania em IA do país,**[5]** no seguinte sentido:

Pontos Fortes do Brasil:

- Energia Elétrica Confiável: o Brasil possui grande vantagem em termos de energia elétrica, sendo um dos poucos países com independência energética e alta participação de fontes renováveis, como a energia hidrelétrica. Essa base sólida de energia confiável e sustentável é crucial para suportar a infraestrutura de IA, que demanda alto consumo energético.

- Governança de Dados: o Brasil tem demonstrado progressos significativos na área de

governança de dados, especialmente com a implementação da Lei Geral de Proteção de Dados (LGPD) e a criação de uma política de dados abertos. Esses avanços colocam o país em uma posição favorável para garantir a coleta, o armazenamento e o tratamento de dados de forma ética e responsável.

Áreas de Aperfeiçoamento:

- Concentração de Dados: apesar dos avanços na governança de dados, a coleta de dados (pessoais) no Brasil pode estar demasiadamente concentrada em poucas empresas. Essa concentração de dados pode limitar a capacidade do país de desenvolver seus próprios sistemas de IA e fortalecer sua soberania em dados.

- Capacidade Computacional: o Brasil ainda enfrenta desafios para garantir a disponibilidade de capacidade computacional suficiente para atender às demandas da IA.

- Desenvolvimento de Algoritmos: o apoio ao desenvolvimento de software nacional, especialmente de código aberto, é crucial para fortalecer a soberania em IA.

- Formação e Retenção de Talentos: investir na educação digital e na formação de talentos em IA é fundamental para que o Brasil se posicione como um ator relevante no cenário global. A falta de investimento em educação digital para todas as faixas etárias e o fenômeno da "fuga de cérebros" representam desafios a serem superados.

- Cibersegurança: a ausência de uma Lei Geral de Cibersegurança e de uma Agência Nacional de Cibersegurança, juntamente com a fragmentação da governança da cibersegurança no país, representam vulnerabilidades que precisam ser endereçadas. A criação de uma estrutura de governança sólida e abrangente é fundamental para garantir a segurança da infraestrutura crítica de IA e proteger os sistemas de IA contra ciberataques.

- Regulamentação de IA: a elaboração de um Marco Regulatório de IA no Brasil é um passo importante, mas ainda existem incertezas sobre a sua efetividade. A falta de clareza sobre os mecanismos de fiscalização, *enforcement* e padronização técnica, bem como a ausência de definição de uma autoridade competente, podem comprometer a implementação da futura lei.

- Estratégia Brasileira de IA (EBIA): a EBIA de 2021 foi criticada por sua falta de abrangência e por não adotar uma abordagem integrada. A revisão da EBIA e o PBIA são oportunidades para fortalecer a estratégia brasileira de IA.

Em termos de cibersegurança, a recente reforma tributária brasileira introduziu uma redução de 60% nas alíquotas do Imposto sobre Bens e Serviços (IBS) e da Contribuição

Social sobre Bens e Serviços (CBS) para serviços e bens relacionados à soberania e segurança nacional, incluindo segurança da informação e cibersegurança, quando fornecidos à administração pública direta, autarquias e fundações públicas. Contudo, essa disposição gerou preocupações no setor de tecnologia. Entidades representativas argumentam que a redução tributária beneficia desproporcionalmente empresas com pelo menos 20% de capital nacional, criando possível reserva de mercado e assimetria concorrencial, especialmente em setor dominado por multinacionais.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO?

Empresas brasileiras, especialmente aquelas que dependem de dados para inovação, enfrentam dois cenários principais:

- **Competitividade Global:** a integração das cadeias globais de valor digital exige conformidade com legislações internacionais e acesso a tecnologias disruptivas, como IA e computação em nuvem. Barreiras, como custos elevados de tratamento de dados ou restrições ao uso de plataformas globais, podem dificultar a inserção de empresas brasileiras no mercado global. Empresas que dependem de fornecedores globais podem ter que reavaliar contratos e parcerias para garantir conformidade com leis de soberania digital, o que pode impactar cronogramas e custos de projetos internacionais; e

- **Inovação Local:** A soberania digital promove o desenvolvimento de tecnologias adaptadas às necessidades do Brasil, como modelos de IA em língua portuguesa ou para setores estratégicos, abrindo novas oportunidades para empresas locais. Setores como agronegócio, logística, saúde e cibersegurança podem se beneficiar de soluções tecnológicas mais eficientes e acessíveis.

SUGESTÕES DO VLK

A construção de uma estratégia de soberania digital competitiva é indispensável para que o Brasil se destaque em um cenário global cada vez mais digitalizado. Essa estratégia deve garantir o acesso livre e facilitado às tecnologias mais inovadoras, independentemente de sua origem, evitando barreiras que prejudiquem a competitividade das empresas brasileiras.

Ao mesmo tempo, é crucial promover a integração das organizações nacionais às cadeias globais de valor, por meio de convergências regulatórias que abranjam transferência de dados, segurança cibernética, inteligência artificial e comércio eletrônico.

Além disso, a redução dos custos de processamento de dados e a ampliação da infraestrutura tecnológica no país devem ser priorizadas para impulsionar a pesquisa e o desenvolvimento de modelos computacionais avançados, fundamentais. Essa visão deve

ser complementada pelo incentivo ao desenvolvimento de tecnologias que reflitam a identidade e as necessidades brasileiras, com destaque para áreas estratégicas como biodiversidade, agropecuária, saúde e educação.

Com políticas públicas robustas e coordenadas, o Brasil terá condições de fomentar um ecossistema de inovação competitivo e sustentável, fortalecendo sua economia, promovendo inclusão digital e garantindo protagonismo no cenário global da transformação digital. O investimento nessa visão estratégica é o caminho para consolidar o país como um líder em tecnologia, inovação e desenvolvimento socioeconômico.

Para as empresas, é fundamental adotar uma abordagem estratégica para que se posicionem frente à Soberania Digital Competitiva, através da adoção das seguintes medidas: **(i) Avaliação Estratégica de Infraestruturas** dos níveis de dependência tecnológica para identificar vulnerabilidades relacionadas à governança de dados, cibersegurança e tecnologia; **(ii) Planejamento de Conformidade** para alinhar sua operação às regulamentações locais e internacionais, assegurando conformidade e reduzindo riscos legais e financeiros (investir em mecanismos de governança e auditoria de algoritmos, para mitigar os riscos de discriminação, vieses e violações de direitos); **(iii) Proteção de Ativos Digitais:** implementação de soluções jurídicas e contratuais que garantam maior controle sobre os ativos digitais e protejam dados contra acessos indevidos; **(iv) Incentivo à Inovação Local:** parcerias com empresas tecnológicas nacionais e estratégias de P&D (Pesquisa e Desenvolvimento) que utilizem tecnologias locais, promovendo competitividade e alinhamento com políticas públicas.

[1] Segundo especialistas como Sérgio Amadeu da Silveira, grande parte da infraestrutura tecnológica nacional está subordinada a empresas estrangeiras, que extraem valor dos dados locais para gerar produtos vendidos de volta ao mercado brasileiro. AGÊNCIA BRASIL. Brasil tem estrutura digital colonizada, alerta sociólogo. Agência Brasil, 29 set. 2024. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2024-09/brasil-tem-estrutura-digital-colonizada-alerta-sociologo. Acesso em: 29 nov. 2024.
[2] BRASIL. Gestão assina acordos com Serpro e Dataprev para criação de nuvem de governo. Portal do Governo, 29 nov. 2024. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2024/novembro/gestao-assina-acordos-com-serpro-e-dataprev-para-criacao-de-nuvem-de-governo. Acesso em: 29 nov. 2024.
[3] Plano Brasileiro de Inteligência Artificial é positivo, mas precisa ser aprimorado para que execução seja factível. Disponível em: https://www.fecomercio.com.br/noticia/plano-brasileiro-de-inteligencia-artificial-e-positivo-mas-precisa-ser-aprimorado-para-que-execucao-seja-factivel
[4] SERPRO. Brasil será única nação com nuvem 100% soberana no hemisfério sul. Disponível em: https://www.serpro.gov.br/menu/noticias/noticias-2024/serpro-nuvem-soberana. Acesso em: 29 nov. 2024.
[5] BELLI, Luca. Soberania em Inteligência Artificial: O que é e o quais facilitadores essenciais podem tornar o Brasil um país soberano em IA? In: CUEVA, Ricardo Villas Bôas; MENDES, Laura Schertel; BIONI, Bruno Ricardo; ALVES, Fabricio da Mota (Org.).

6) SOBERANIA DIGITAL COMPETITIVA

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Acreditamos que crescerá a exigência por infraestrutura local de data center, especialmente para dados e informações governamentais. Ao mesmo tempo, países buscarão diversificar fornecedores de tecnologia para reduzir riscos de dependência de uma nação em específico. Nessa linha, poderá haver incentivos para empresas locais (ou com pelo menos 20% do seu quadro societário compostos por brasileiros natos) e as regulações na área digital priorizarão o mercado interno, mas garantindo o acesso livre e facilitado às tecnologias mais inovadoras, independentemente de sua origem, desde que seja cumprida a legislação nacional.
POR QUE É TENDÊNCIA?	O Brasil ocupa papel crucial no cenário global como potência emergente, mas enfrenta desafios significativos relacionados à dependência tecnológica. Ante este cenário, há diversas iniciativas do Legislativo, Judiciário e Executivo a fim de mitigar esse risco.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	Empresas brasileiras, especialmente aquelas que dependem de dados para inovação, enfrentam dois cenários principais: competitividade global e inovação local.
SUGESTÕES DO VLK	A construção de estratégia de soberania digital competitiva é indispensável para que o Brasil se destaque em cenário global cada vez mais digitalizado. Essa estratégia deve garantir o acesso livre e facilitado às tecnologias mais inovadoras, independentemente de sua origem, evitando barreiras que prejudiquem a competitividade das empresas brasileiras. Ao mesmo tempo, é crucial promover a integração das organizações nacionais às cadeias globais de valor, por meio de convergências regulatórias que abranjam transferência de dados, segurança cibernética, inteligência artificial e comércio eletrônico.

7) *LEGAL DESIGN* E CENTRALIDADE DO USUÁRIO

TENDÊNCIAS PARA 2025

O Legal Design foi criado em 2001 por Colette Brunschwig e difundido por Margaret Hagan, uma professora e pesquisadora da Universidade de Stanford, nos Estados Unidos, na década de 2010. A proposta surgiu a partir da percepção de que o direito, tradicionalmente inacessível e complexo, poderia se beneficiar de princípios do design para se tornar mais centrado nas pessoas, acessível e eficaz.

Enfim, o direito passa por um momento de disrupção, em que ganha relevância a multidisciplinariedade, mediante a interlocução com outras ciências como o Design, através de ferramentas de empatia, prototipagem e testes. Esse movimento embarca a ciência jurídica em frameworks consolidados, como o foco na centralidade do cliente e do usuário final.

POR QUE É TENDÊNCIA?

Considerando o papel relevante do legal design ao conferir compreensão ao conteúdo jurídico, especialmente por meio de métodos como o visual law, nota-se que essa é forte tendência, impulsionada inclusive por entidades fiscalizadoras, como a Autoridade Nacional de Proteção de Dados (ANPD) ao perseguir o cumprimento legal de transparência, tal como consta na Lei Geral de Proteção de Dados (art. 6º, inc. VI).

Neste contexto, vale mencionar a decisão de suspensão cautelar pela ANPD da Política de Privacidade do Meta que previa o tratamento de dados pessoais para treinamento do seu sistema de IA, em julho de 2024 – posteriormente suspensa em agosto deste ano. Dentre os pontos suscitados, destacam-se as interfaces de difícil navegação e a complexidade de acesso às informações correspondentes, configurando-se em verdadeiras barreiras que limitavam o exercício dos direitos dos titulares.

Quando os padrões de design dificultam ou impõem obstáculos às informações e à utilização dos mecanismos de exercício de direitos dos titulares, há um claro descumprimento dos princípios do livre acesso e da transparência constantes na LGPD.

Adicionalmente, foram mapeadas barreiras comunicacionais na Política de Privacidade do Meta com termos pouco claros ou assertivos, desencadeando posteriormente em esforços de pesquisa com usuários para endereçar aplicação de linguagem mais acessível.

Outra temática extremamente importante que tem sido acompanhada de maneira muito próxima pela ANPD é o tratamento de dados de crianças e adolescentes em ambiente online, como ocorreu no caso supracitado do Meta e no processo sancionador contra o TikTok, em novembro de 2024.

Segundo a pesquisa Tic Kids Online Brasil 2023, 88% das crianças e adolescentes entre 9 e 17 anos possuem perfil nas redes sociais. Essa presença online de menores de idade tem chamado a atenção e despertado preocupação de especialistas e autoridades. Quanto mais tempo gastam conectados, mais expostos ficam à coleta de seus rastros digitais. Considerando as limitações cognitivas, incluindo aí aspectos psicomotores e intelectuais, é comum que, especialmente as crianças, não tenham consciência da utilização dos seus dados pessoais para finalidades mercadológicas.

Considerando o desafio de dar transparência para o tratamento de dados pessoais para esse público, a aplicação de técnicas de *visual law* pode ser uma importante aliada no cumprimento legal.

Aliás, esse é movimento que tem ganhado cada vez mais consistência mundialmente, a exemplo do *Children's Code Design Guidance do Information Commissioner's Office* (ICO), autoridade de proteção de dados do Reino Unido. Esse material traz orientações práticas de design para serviços e plataformas online considerando cada estágio de desenvolvimento das crianças e adolescentes, de maneira a cumprir com a legislação de proteção de dados local, tendo como um dos principais pilares a transparência.

Além disso, aqui no Brasil, identifica-se forte tendência legal e regulatória no sentido de destacar um regime protetivo específico para crianças e adolescentes, tal como consta na Seção III da LGPD, ou então em projetos de Lei como o do Marco Legal Regulatório de Inteligência Artificial (PL 2338/23) em seu Capítulo II que dedica ao uso de produtos/serviços de tecnologia da informação por criança e adolescentes e o PL 2628/22 que estabelece regras específicas para proteger esse público no ambiente online.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO?

É perceptível o quanto o *legal design,* com foco na linguagem simples e *visual law,* é ferramenta que cada vez mais vem ganhando espaço e fazendo sentido para os mais diversos stakeholders tal como clientes, colaboradores, advogados e servidores da Justiça. Não é apenas tendência passageira, mas evolução necessária em um mundo em que a experiência do cliente é cada vez mais central e valorizada.

A partir da utilização de ferramentas, como o mapa de empatia, é possível identificar as principais dores e gargalos durante a experiência do público-alvo a quem se direciona o documento jurídico e, a partir desse ponto, desenvolver linguagem mais adequada e aplicar recursos visuais para romper com barreiras de resistência e favorecer a compreensão da mensagem.

Sob a perspectiva da Justiça, em pesquisa realizada pela *VisuLaw***[1]** em 17 estados brasileiros no ano de 2020, verificou-se que 77% dos magistrados entrevistados afirmaram que o uso de elementos visuais facilita a análise de uma petição. Assim, esse recurso pode ser relevante especialmente em causas que envolvam temas muito técnicos e específicos, viabilizando o entendimento dos magistrados e podendo impactar positivamente nas decisões judiciais, levando, em última análise, a eficiência de custo e tempo.

Ainda, o uso de técnicas de legal design em interfaces diretas com o consumidor como em termos de uso e aviso de privacidade em sites, ou então em contratos, além de gerar encantamento e estabelecer relação de confiança com esse público, pode resultar na redução de custos operacionais em atendimento (SAC), em apoio jurídico e consequentemente em redução de exposição legal e regulatória.

SUGESTÕES DO VLK

Mais do que uma estratégia, o legal design representa mudança cultural, em que o direito se torna ferramenta de empoderamento e acessibilidade. Seu impacto vai além da estética: transforma a maneira como nos relacionamos com o universo jurídico, tornando-o mais humano, eficiente e alinhado às expectativas de uma sociedade em constante evolução. As empresas que adotarem essa abordagem estarão à frente em inovação e credibilidade, pois demonstram transparência e compromisso com a experiência do cliente – seja interno ou externo, fatores que são altamente valorizados em um mercado competitivo.

Neste contexto, destacamos a importância da utilização deste tipo de recurso em documentos com conteúdo jurídico, tais como: (i) contratos, (ii) políticas de privacidade, (iii) termos de uso de sites e plataformas, (iv) documentos de governança e (v) peças jurídicas.

A transparência comunicacional gerada pelo legal design rompe barreiras de desconfiança e resistência e engaja o interlocutor, sendo importante ferramenta para aderência legal e regulatória.

[1] *https://www.conjur.com.br/dl/vi/visulaw-pesquisa.pdf*

7) LEGAL DESIGN E CENTRALIDADE DO USUÁRIO

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Aplicação do legal design para a criação de soluções jurídicas mais acessíveis, eficientes e compreensíveis, com linguagem simplificada e uso de elementos visuais, mantendo-se como foco a centralidade do destinatário da mensagem. Com isso, políticas e documentos jurídicos interativos e visuais deixarão de ser apenas uma prática desejável e passarão a se tornar uma realidade necessária no cotidianos das organizações.
POR QUE É TENDÊNCIA?	O direito é tradicionalmente marcado por linguagem técnica, rebuscada e que resulta em documentos complexos. O *legal desing* tem se mostrado muito eficiente para garantir transparência e acessibilidade, auxiliando para o cumprimento legal e regulatório, tal como exigido pela LGPD. Casos na ANPD como o do Meta e do TikTok destacam a necessidade de interfaces claras e em design amigável, especialmente para proteger públicos vulneráveis como crianças e adolescentes no ambiente digital.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	Ao aplicar métodos de design, como linguagem simples e *visual law,* é facilitada a compreensão de documentos jurídicos com impactos positivos na experiência do usuário, aumentando a confiança no público-alvo e reduzindo custos operacionais.
SUGESTÕES DO VLK	Aplicação do legal design em documentos com conteúdo jurídico, tais como: (i) contratos, (ii) políticas de privacidade, (iii) termos de uso de sites e plataformas, (iv) documentos de governança e (v) peças jurídicas.

8) *LEGAL MARKETING*

TENDÊNCIAS PARA 2025

Com a transformação digital da sociedade, o mercado publicitário vive numa era de hipersegmentação, isto é, a *clusterização* do público-alvo em grupos menores e com características específicas comportamentais, sociais, demográficas.

De acordo com pesquisa realizada pela McKinsey**[1]** há forte expectativa dos consumidores em serem impactados por interações personalizadas das marcas: 71% dos respondentes, sendo que 76% afirmaram que ficam frustrados quando isso não acontece.

Neste contexto, identifica-se forte tendência para os próximos anos de criação de conteúdos publicitários com personalização em massa alavancados pelo uso de IA.

O que antigamente parecia contraditório, atualmente a tecnologia se encarregou de endereçar, permitindo entregar conteúdos customizados para determinado público com características específicas, de forma ampla.

POR QUE É TENDÊNCIA?

Com essa demanda de mercado em que os consumidores esperam das marcas comunicação mais direcionada e assertiva quanto a seus interesses, nota-se verdadeira corrida das áreas de marketing das empresas e agências de comunicação para se apoiar em ferramentas de inteligência artificial.

Pesquisas de mercado apontam para iniciativas que envolvem o uso de IA como uma das prioridades no setor de comunicação em 2025 visando eficiência de custo e de tempo, com assertividade.

Em recente pesquisa realizada na Europa para mapear as principais preocupações dos CMOs para o ano de 2025**[2]**, identificou-se como foco destes executivos a priorização do investimento para uso da IA nos processos de marketing (81% dos respondentes), seguido do gerenciamento e personalização da jornada do consumidor (80%).

O setor de publicidade entendeu que a IA pode ser aliada importante, se não fundamental, para possibilitar a hipersegmentação de conteúdo de forma rápida, eficiente e acessível. Atualmente, há soluções de IA que auxiliam em vários momentos desta jornada como para (i) análise de grande volume de dados para clusterização por meio de padrões comuns; (ii) análises preditivas de comportamentos de consumidores, (iii) criação de conteúdos personalizados a partir da interação com o público.

A partir desse panorama de hipersegmentação, identificamos que as seguintes discussões de Legal Marketing estarão em evidência no próximo ano:

- ***Microtargeting:*** utilização de dados pessoais para segmentar grupos específicos de consumidores com mensagens altamente personalizadas. Apesar de sua eficácia em alcançar o público certo, essa prática levanta questões jurídicas relevantes, especialmente no que se refere à proteção de dados pessoais.

- **Influenciadores Virtuais**: são personagens digitais gerenciados por empresas ou profissionais, que podem representar alguma celebridade/personalidade humana ou ser totalmente fictícios como Aitana (gerada com IA), Imma Gram e Lil Miquela. Esta tem sido uma forte tendência no marketing, tornando-se importante canal para a hipersegmentação, pois representa eficiência em (i) **custos**, permitindo a facilidade de adaptação do material para diferentes perfis de consumidores, inclusive com idiomas diferentes, (ii) **tempo**, uma vez que a criação de conteúdo é praticamente sintética, realizada por soluções de IA, as entregas são realizadas numa velocidade muito maior do que produções que demandam casting, equipe de produção, de edição, de finalização e (iii) assertividade, já que as empresas/marcas possuem total controle editorial da mensagem publicitária que será comunicada.

- **Microinfluenciadores:** eles têm desempenhado papel relevante no contexto de hipersegmentação, podendo ser pessoas ou avatares digitais e vêm ganhando cada vez mais destaque como estratégia de marketing, por sua conexão genuína com nichos altamente específicos de audiência, oferecendo maior credibilidade e engajamento. Contudo, o uso desse recurso requer atenção especial às responsabilidades legais. Especialmente se o perfil na rede social for gerido por pessoa física, esses influenciadores nem sempre possuem conhecimento aprofundado das normas de autorregulamentação publicitária e demais legislação aplicável, o que pode levar a práticas irregulares, como a ausência de identificação clara de conteúdo patrocinado e violação de direitos de Propriedade Intelectual.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO?

Quanto ao uso de sistemas de IA para a hipersegmentação, vale mencionar que o cenário regulatório de IA está em plena ebulição, tanto no Brasil com o PL 2338/23, como internacionalmente, como por exemplo, com a implementação do *AI Act* na União Europeia, os impactos da *Executive Order* assinada pelo Presidente Biden nos Estados Unidos e a *policy paper* apresentada pela Secretaria de Estado de Ciência, Inovação e Tecnologia (SECIT) no Reino Unido.

Além disso, entidades de autorregulamentação publicitária ao redor do mundo têm acompanhado o tema de perto.

No Brasil, o CONAR decidiu, em caso paradigmático, pela possibilidade de uso de IA Generativa que recriou a imagem da cantora Elis Regina em anúncio da Volkswagen. No caso em referência, a personalidade falecida figurava ao lado de sua filha, Maria Rita e, embora não houvesse sinalização expressa de que parte do conteúdo tinha sido criado com IA, entendeu-se pela transparência contextual e observância aos preceitos éticos do Código de Autorregulamentação Publicitária.

Adicionalmente, em julho deste ano de 2024, foi divulgado que o CONAR iniciaria testes de monitoramento de peças publicitárias nas redes sociais, com o apoio de sistemas de IA trazendo eficiência de fiscalização e de custos.

Em movimento similar, o *Advertising Standards Authority* (ASA) do Reino Unido divulgou em novembro/2024**[3]** o resultado de monitoramento com IA que detectou 16.000 anúncios online no período de 3 meses para avaliar a regularidade de alegações ("claims") de uso de IA e evitar anúncios enganosos neste sentido.

Se por um lado há encantamento pelos benefícios que o uso da IA pode desencadear nos processos de uma campanha publicitária, de outro, verifica-se um interesse regulatório crescente nesta temática considerando eventuais riscos relacionados à ética publicitária, direitos de consumidor, privacidade e proteção de dados pessoais e direitos de propriedade intelectual, apenas para citar alguns.

Assim, há desafio relevante em embarcar IA nos conteúdos e rotinas das áreas de marketing de maneira segura e ética.

Especificamente com relação às estratégias de marketing para alcançar a hipersegmentação, ressaltamos as seguintes cautelas:

- **Microtargeting:**

Com a vigência da Lei 13.709/18 (LGPD) no Brasil, as empresas devem garantir que a coleta e o tratamento de dados pessoais para *microtargeting* sejam realizados com base legal adequada, como o consentimento do titular ou a execução de contratos.

Outro aspecto relevante é o impacto do *microtargeting* na transparência das campanhas publicitárias. É essencial que os consumidores saibam como e por que estão recebendo determinadas mensagens, evitando práticas manipuladoras ou que limitem a liberdade de escolha. O uso de algoritmos para filtrar conteúdos também pode ser visto como forma de discriminação, caso haja exclusão ou direcionamento injusto de anúncios com base em critérios sensíveis, como etnia, gênero ou orientação sexual.

Por fim, as regulamentações internacionais, como o Regulamento Geral de Proteção de Dados (RGPD) na Europa, exercem influência significativa sobre o uso de microtargeting por empresas globais. Campanhas que utilizam essa estratégia devem estar alinhadas não

apenas com as normas brasileiras, mas também com exigências internacionais, especialmente empresas multinacionais.

- **Influenciadores digitais virtuais:**

Um dos principais pontos de atenção é a transparência quanto ao controle por trás desses influenciadores e especialmente com relação à natureza do conteúdo, quando houver caráter publicitário. A ausência de clareza pode ser considerada prática enganosa, violando tanto o Código de Defesa do Consumidor (art. 36), quanto o Código Brasileiro de Autorregulamentação Publicitário (art. 28).

Do ponto de vista ético, também surge a preocupação quanto ao impacto no público, especialmente em crianças e adolescentes, que podem não perceber a artificialidade desses influenciadores. Por serem vistos como figuras autênticas, sua influência pode ser ainda mais persuasiva, tornando fundamental que campanhas utilizem tais personagens com responsabilidade e em conformidade com as normas vigentes.

- **Microinfluenciadores:**

Para evitar sanções, as marcas devem investir em treinamentos e fornecer orientações claras sobre a necessidade de usar hashtags como #publi ou #parceria. A ausência de transparência em campanhas pode configurar infrações ao CDC e ao Código de Autorregulamentação Publicitária, prejudicando a reputação da empresa e do influenciador.

Outro ponto relevante é a formalização das relações contratuais. Garantir que todos os detalhes da parceria, como responsabilidades, pagamentos e cláusulas de exclusividade, estejam formalizados por escrito é essencial para mitigar riscos jurídicos e assegurar o alinhamento das expectativas entre ambas as partes.

SUGESTÕES DO VLK

Já é possível antecipar cautelas, em relação ao uso ético e responsável de IA no marketing, com foco em elevar o nível de governança corporativa: (i) fortalecer a literacia dos times de marketing e jurídico sobre o tema por meio de *workshops* e cartilhas, (ii) mapear e avaliar os riscos das ferramentas utilizadas especialmente na produção de conteúdo publicitário e interação com o consumidor, e (iii) utilizar cláusulas contratuais específicas de IA com fornecedores.

Importante mencionar que as estratégias de marketing também demandam cuidados específicos para a conformidade legal e regulatória:

- **Microtargeting:** (a) garantir que o tratamento de dados pessoais seja realizado com base em fundamentos legais, como o consentimento expresso (art. 7º da LGPD); (b) verificar se políticas de privacidade das plataformas utilizadas estão em conformidade

com a LGPD; (c) assegurar que as práticas de segmentação não tenham viés discriminatório; (d) utilizar recursos de transparência (como políticas de privacidade, pop-ups) com os consumidores sobre como os dados são tratados e possibilitar que eles optem por não participar de campanhas direcionadas.

- **Influenciadores Virtuais:** (a) identificar claramente o caráter publicitário de conteúdos feitos por influenciadores virtuais, em conformidade com o Código Brasileiro de Autorregulamentação Publicitária, (b) informar de maneira explícita que o influenciador é uma criação digital e que suas interações são controladas por uma equipe ou marca; (c) evitar campanhas voltadas a públicos vulneráveis, como crianças, que podem não distinguir entre personagens reais e virtuais; (d) inserir cláusulas específicas sobre propriedade intelectual e uso do avatar digital nos Contratos entre a marca e o estúdio que desenvolveu a imagem; (e) monitorar continuamente as mensagens emitidas para garantir que estejam alinhadas com as normas éticas e legais.

- **Microinfluenciadores:** (a) formalizar parcerias com microinfluenciadores mediante contratos que detalhem responsabilidades, valores e obrigações, incluindo cláusulas sobre a transparência do conteúdo publicitário; (b) elaborar guias orientativos e realizar workshops para os microinfluenciadores sobre os cuidados necessário para elaboração de conteúdo de maneira a evitar infrações; (c) realizar auditorias periódicas nas campanhas realizadas por microinfluenciadores para assegurar conformidade legal.

[1] https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying

[2] https://www.meioemensagem.com.br/marketing/quais-sao-os-desafios-e-prioridades-dos-cmos-para-2025
[3] https://www.asa.org.uk/static/eb77bee0-a147-49b8-81856c3c83586bf2/AI-as-a-Marketing-Term-Report.pdf

8) LEGAL MARKETING

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Campanhas publicitárias com personalização em massa alavancados pelo uso de IA visando a hipersegmentação, trazendo conteúdo genuíno e ético, alinhado a valores ESG. O poder das comunidades estará ainda em maior evidência com o reposicionamento das marcas com relação ao marketing de influência para públicos altamente específicos. Ferramentas de realidade aumentada passarão a ser mais usadas para engajar clientes, especialmente o público mais jovem.
POR QUE É TENDÊNCIA?	Pesquisas de mercado apontam para iniciativas que envolvem o uso de IA como uma das prioridades no setor de comunicação em 2025 com foco na eficiência de custo e de tempo, com assertividade. A IA será uma ferramenta determinante para possibilitar a hipersegmentação do conteúdo publicitário, especialmente mediante as estratégias de (i) microtargeting; (ii) utilização de influenciadores digitais virtuais; e (iii) microinfluência.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	Sob o viés de uso de sistemas de IA para a hipersegmentação do conteúdo publicitário, temos um cenário regulatório em plena ebulição, tanto no Brasil com o PL 2338/23 como internacionalmente. Além disso, entidades de autorregulamentação publicitária ao redor do mundo têm acompanhado o tema de perto, a exemplo do CONAR e do ASA (Reino Unido). Assim, há um desafio relevante em embarcar IA nos conteúdos e rotinas das áreas de marketing de maneira segura e ética. Adicionalmente, as estratégias de marketing supramencionadas para permitir a hipersegmentação demandam cuidados específicos como a observância da LGPD, Leis de Propriedade Intelectual e Normas de Autorregulamentação Publicitária.
SUGESTÕES DO VLK	Tanto para uso de sistemas de IA, quanto para a implementação das estratégias de hipersegmentação, destacamos: (i) o fortalecimento da literacia dos públicos afetados como times de marketing e jurídico das empresas, agências de marketing e influenciadores, (ii) aplicação de cláusulas contratuais robustas e (iii) monitoramento dos conteúdos publicitários para verificar a conformidade com a legislação e autorregulamentação publicitária.

9) EDUCAÇÃO MIDIÁTICA E LITERACIA DIGITAL

TENDÊNCIAS PARA 2025

A educação midiática e a literacia digital são fundamentais para capacitar indivíduos a navegar de forma crítica e segura no ambiente digital. Essas competências englobam a habilidade de acessar, analisar e criar conteúdo digital de maneira ética e responsável, além de compreender os riscos associados ao uso da tecnologia, como desinformação e ameaças cibernéticas. No Brasil, a crescente digitalização e o aumento do acesso à internet tornam urgente a promoção dessas habilidades, especialmente entre crianças, adolescentes e idosos, que são potencialmente mais vulneráveis aos perigos online. Iniciativas governamentais e legislativas buscam integrar a educação digital nos currículos escolares e promover a inclusão digital, reconhecendo a importância de preparar os cidadãos para os desafios do mundo digital.

POR QUE É TENDÊNCIA?

Em razão do seu impacto social e econômico, inúmeras iniciativas regulatórias e políticas públicas recentes demonstram a relevância crescente da educação midiática e da literacia digital. São exemplos:

- **Política Nacional de Educação Digital (Lei nº 14.533/2023):** instituída em janeiro de 2023, ela visa promover a inclusão digital, capacitação e especialização em tecnologias digitais, além de incentivar a pesquisa e a educação digital nas escolas.

- **Estratégia Brasileira de Educação Midiática (SECOM, 2023):** desenvolvida pela Secretaria de Comunicação Social, ela reforça a capacitação de cidadãos para análise crítica e engajamento ético no ambiente digital, enfrentando desafios como desinformação, discursos de ódio e exclusão digital.

- **Proteção de Crianças e Adolescentes em Ambientes Digitais (PL 2.628/2022):** aprovado em novembro pelo Senado Federal, o PL estabelece medidas para proteger o público jovem no ambiente digital, incluindo a educação e proibição de criação de contas em redes sociais por menores de 12 anos e restrições à publicidade digital voltada para crianças.

- **Inclusão Digital dos Idosos (PL 3.167/2023):** também aprovado no Senado, propõe a capacitação digital de idosos como prioridade da Política Nacional de Educação Digital, abrangendo habilidades para criar conteúdo, usar ferramentas tecnológicas com segurança, promovendo inclusão e autonomia dessa população.

- **Regulamentação da Inteligência Artificial (PL 2.338/2023):** atualmente em tramitação avançada no Senado Federal, o projeto reflete a crescente importância da capacitação profissional e da educação digital no contexto da inteligência artificial.

- **Política Nacional de Cibersegurança (Decreto nº 11.856/2023):** 24% dos brasileiros relataram ter perdido dinheiro em crimes cibernéticos no último ano, segundo o Instituto de Pesquisa do DataSenado2. Aprovada em 2023, a PNCiber reforça a centralidade da educação e capacitação em segurança cibernética como eixo estratégico para o fortalecimento da proteção digital no país.

- **Lei de Apostas Eletrônicas (Lei nº 14.790/2023):** regulamenta o setor de apostas online no Brasil, estabelecendo critérios para a operação de plataformas de apostas eletrônicas e medidas de proteção ao consumidor. A literacia digital permite que os usuários compreendam os riscos associados a essas plataformas e tomem decisões informadas.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO?

A literacia digital e educação midiática desempenham papel estratégico para o setor privado ao fornecer as habilidades e o conhecimento necessários para que as empresas aproveitem as oportunidades da transformação digital. Seguem os principais impactos positivos:

- **Melhoria da produtividade e eficiência operacional**

Funcionários com alta literacia digital utilizam ferramentas tecnológicas de maneira mais eficaz, reduzindo o tempo de execução de tarefas e aumentando a precisão. Isso melhora os processos internos, reduz custos e elimina redundâncias.

- **Redução de riscos cibernéticos**

Ao compreender conceitos básicos de segurança digital, como proteção de dados, autenticação segura e detecção de *phishing*, os colaboradores contribuem para postura de segurança cibernética mais robusta. Isso diminui a probabilidade de violações e incidentes de segurança.

- **Inovação nos modelos de negócios**

Com maior domínio das tecnologias digitais, as empresas podem explorar novos canais de venda, adaptar-se ao comportamento do consumidor e criar produtos ou serviços mais inovadores, como marketplaces online, serviços baseados em IA e automação de processos.

- **Aumento da competitividade**

Empresas com equipes bem preparadas digitalmente conseguem se adaptar mais rapidamente às mudanças tecnológicas e regulatórias, mantendo-se competitivas em mercados dinâmicos.

- **Conformidade legal e ética**

A literacia digital permite que os funcionários reconheçam a importância da conformidade e sigam as práticas recomendadas. Compreender os aspectos regulatórios, como a LGPD, é essencial para evitar multas e litígios.

De outro lado, a literacia em IA, por exemplo, é fundamental para o uso ético da tecnologia, pois permite compreender seus funcionamentos, identificar e mitigar riscos como vieses e violações de privacidade, e garantir decisões responsáveis. Por exemplo, ao implementar IA em processos de recrutamento, equipe com literacia em IA consegue identificar e corrigir vieses nos dados que poderiam discriminar candidatos. Além disso, saber avaliar os limites e impactos da tecnologia ajuda a evitar decisões automatizadas injustas e a comunicar de forma clara como a IA está sendo utilizada, fortalecendo a confiança do público e garantindo conformidade com leis, como a LGPD.

- **Habilidades críticas no uso da tecnologia e da informação**

A educação midiática ensina a analisar, interpretar e avaliar criticamente o conteúdo consumido, como notícias, publicidade e postagens em redes sociais.

- **Combate à desinformação**

Empresas dependem de informações precisas para tomadas de decisão estratégicas. A educação midiática fortalece a capacidade dos colaboradores de identificar e evitar a disseminação de *fake news*, que podem impactar negativamente a reputação ou decisões do negócio.

- **Fomento à cultura de inovação**

Colaboradores que compreendem o valor e funcionamento das tecnologias digitais se sentem mais capacitados a propor soluções criativas e disruptivas. Isso fortalece a cultura de aprendizado contínuo e inovação organizacional.

- **Sustentabilidade**

O domínio de ferramentas digitais pode ajudar a otimizar recursos, reduzir desperdícios e implementar iniciativas mais sustentáveis, como a digitalização de documentos e o uso de tecnologias para monitoramento ambiental.

Ou seja, a implementação de programas de educação midiática e literacia digital entre os colaboradores fortalece a segurança da informação, proteção de dados e reduz o impacto de *fake news*, diminuindo a vulnerabilidade a ataques cibernéticos e vazamentos de dados. Além disso, a capacitação em práticas digitais responsáveis garante a conformidade com as leis e regulamentações, prevenindo penalidades e danos à reputação da empresa. Empresas que investem em literacia digital estão mais preparadas para adotar novas tecnologias e manter sua competitividade no mercado global. Essa iniciativa também contribui para a formação de uma sociedade mais consciente e preparada para os desafios do mundo digital, melhorando a imagem institucional da empresa.

SUGESTÕES DO VLK

Para atender à tendência de combinar literacia digital e educação midiática, as empresas podem adotar medidas práticas que desenvolvam competências nos colaboradores e fortaleçam a cultura organizacional. Isso começa com programas de capacitação contínua em todos os níveis hierárquicos, garantindo que os colaboradores estejam atualizados sobre melhores práticas, regulamentações e tecnologias emergentes. A nomeação de líderes, como *"data champions"* ou embaixadores digitais, também é essencial para promover uma cultura de inovação responsável, que concilie novas tecnologias, segurança e uso ético.

Além disso, políticas corporativas claras podem orientar o consumo e compartilhamento responsável de informações, alinhadas à estratégia de *compliance* e ESG. Paralelamente, a participação ativa em fóruns e debates sobre políticas públicas permite à empresa influenciar regulamentações com insights práticos e experiências do mercado.

Essas ações, quando integradas à operação, transformam o ambiente corporativo, aumentando a produtividade, protegendo a reputação da marca e promovendo inovação com ética. A combinação de literacia digital e educação midiática não é apenas tendência, mas estratégia essencial para empresas que desejam prosperar em mercados digitais de maneira ética e eficaz.

9) EDUCAÇÃO MIDIÁTICA E LITERACIA DIGITAL

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	A educação midiática e a literacia digital comporão políticas públicas e programas corporativos, capacitando indivíduos a navegarem de forma ética e segura no ambiente digital, englobando a habilidade de acessar, analisar e criar conteúdo digital de maneira crítica e responsável, além de compreender os riscos associados ao uso da tecnologia, como desinformação e ameaças cibernéticas. Os governos também terão papel fundamental na criação e disseminação desse tipo de programa de conscientização.
POR QUE É TENDÊNCIA?	Em razão do seu impacto social e econômico, inúmeras iniciativas regulatórias e políticas públicas recentes demonstram a relevância crescente da educação midiática e da literacia digital.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	Melhoria da produtividade e eficiência operacional, redução de riscos cibernéticos, inovação nos modelos de negócios, aumento da competitividade e conformidade legal e ética.
SUGESTÕES DO VLK	Programas de capacitação contínua em todos os níveis hierárquicos, garantindo que os colaboradores estejam atualizados sobre melhores práticas, regulamentações e tecnologias emergentes, somada a nomeação de líderes, como embaixadores digitais, para promover a cultura de inovação responsável, que concilie novas tecnologias, segurança e uso ético. Tudo isso alinhada à estratégia de *compliance* e ESG da empresa.

10) INTEGRIDADE DA INFORMAÇÃO E DEVIDO PROCESSO INFORMACIONAL

TENDÊNCIAS PARA 2025

A integridade informacional surge como conceito essencial para lidar com os desafios impostos pela desinformação, conteúdos enganosos, manipulações no ambiente digital e decisões automatizadas. Esse tema, intensamente debatido no G20 Brasil e consolidado nas Nações Unidas em 2023**[1]**, é fundamental para mitigar os impactos da disseminação de notícias falsas sobre processos democráticos, relações sociais e a economia global. Além disso, decisões jurídicas recentes no Brasil, como as discussões sobre o artigo 19 do Marco Civil da Internet, o PL de IA, o PL 2630/2000 e o Projeto de Lei 3.024/2024, reforçam o papel estratégico da governança informacional na construção de um ambiente digital mais seguro, transparente e responsável.

Essas questões impulsionam a discussão sobre as plataformas digitais moderarem de forma mais diligente o conteúdo e comportamento de seus usuários, por meio do devido processo informacional.

POR QUE É TENDÊNCIA?

O avanço das tecnologias digitais e o crescimento do comércio eletrônico têm exposto novos desafios relacionados à integridade informacional. A proliferação de desinformação e de produtos falsificados online são exemplos práticos desse fenômeno. As discussões travadas no STF a respeito do artigo 19 do Marco Civil da Internet**[2]**, que buscam analisar o grau de responsabilidade das plataformas por conteúdo de terceiros, têm implicações importantes para o equilíbrio entre liberdade de expressão e segurança jurídica, afetando o modo como as empresas gerenciam e moderam conteúdo**[3]**.

Iniciativas legislativas, como o PL 2630/2020 (que busca combater a desinformação na internet) e o PL 3.024/2024 (que responsabiliza solidariamente plataformas pela venda de produtos falsificados) destacam a crescente pressão regulatória sobre a integridade da informação disponível online. Essa regulação busca proteger os indivíduos, os consumidores e a propriedade intelectual, ao mesmo tempo em que incentiva práticas empresariais mais éticas e seguras**[4]**.

São diversas as normas e decisões internacionais impondo às plataformas a necessidade de adotarem o devido processo informacional na moderação de conteúdo, como o Digital

Millennium Copyright Act (EUA), Direito ao Esquecimento (União Europeia), NetzDG (Alemanha) e o Digital Service Act (União Europeia).

Por fim, o debate sobre o projeto de lei que busca regulamentar o desenvolvimento e uso de sistemas baseados em inteligência artificial reforça a preocupação com o impacto dessas tecnologias na propagação da desinformação, sublinhando a urgência de medidas que promovam um ambiente digital mais seguro e transparente**[5]**.

O cenário internacional também reforça a relevância da integridade informacional. A *Global Initiative for Information Integrity on Climate Change*, lançada durante o G20**[6]**, exemplifica como a desinformação em áreas críticas, como mudanças climáticas, pode comprometer decisões estratégicas globais. Tais esforços enfatizam a necessidade de políticas coordenadas para enfrentar crises informacionais em escala global.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO?

A integridade informacional afeta diretamente o ambiente de negócios ao influenciar a confiança dos consumidores e a reputação das empresas. No comércio eletrônico, a presença de produtos falsificados não apenas prejudica a credibilidade das plataformas, mas também implica possíveis penalidades regulatórias. Para empresas de tecnologia, e-commerce e publicidade digital, decisões como as que envolvem o artigo 19 do Marco Civil da Internet trazem segurança jurídica ao definir limites claros para a responsabilização de conteúdos de terceiros. Contudo, o monitoramento contínuo e adoção de políticas internas robustas para evitar ilegalidades e danos reputacionais são medidas para se manter um ambiente saudável de negócios e debates, independentemente da discussão de responsabilidade civil.

SUGESTÃO SUGESTÕES DO VLK

Desenvolver melhor o conceito de devido processo informacional na moderação de conteúdo online, que busca garantir que os direitos dos usuários sejam respeitados e que os processos de decisão sejam justos, transparentes e fundamentados em critérios objetivos, no seguinte sentido:

Transparência: as plataformas devem divulgar de forma clara suas políticas de uso, incluindo os critérios e procedimentos utilizados para moderação de conteúdo.

Justificativa e Motivação: sempre que conteúdo for removido, limitado ou sinalizado, as plataformas devem informar ao usuário o motivo, com explicações claras e baseadas em normas previamente definidas.

Direito de Contestação: assegurar ao usuário a possibilidade de recorrer das decisões, por meio de processos internos eficazes e acessíveis.

Proporcionalidade e necessidade: as ações de moderação devem ser proporcionais ao impacto do conteúdo e à violação das políticas, considerando as implicações nos direitos dos usuários. As medidas podem incluir a limitação de alcance do conteúdo e calibragem de algoritmos; vedação de utilização de contas inautênticas para práticas nocivas; avisos sobre a sensibilidade de determinados conteúdos; desestímulo financeiro, impedindo a monetização, suspendendo ou cancelando contas que servem para atividades ilícitas, entre outras medidas.

Inclusão de Revisão Humana de forma proporcional: decisões automatizadas devem ser revisadas por humanos em casos complexos, para evitar erros decorrentes de algoritmos que possam afetar significativamente direitos.

Accountability **(Responsabilidade):** as plataformas devem estar sujeitas a auditorias, pesquisas acadêmicas e fiscalização de desempenho acerca das suas práticas de moderação, pois há interesse público na transparência sobre os critérios de decisão.

Adotar o devido processo informacional pode gerar a confiança do usuário, redução de riscos legais e melhoria da reputação.

[1] INSIGHTS do G20 sobre a integridade da informação e a era das fake news. JOTA, 27 mai. 2024. Disponível em: https://www.jota.info/artigos/insights-do-g20-sobre-a-integridade-da-informacao-e-a-era-das-fake-news. Acesso em: 2 dez. 2024.
[2] Atualmente, o Supremo Tribunal Federal (STF) possui dois casos paradigmáticos com repercussão geral envolvendo o tema – os Recursos Extraordinários 1057258 (Tema 533) e 1037396 (Tema 987). O Tema 533, considera o dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário. Já o Tema 987, discute a necessidade de prévia e específica ordem judicial de exclusão de conteúdo para a responsabilização civil de provedor de internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros.
[3] CARVALHO, Luísa. Julgamento do artigo 19 impacta conteúdo comercial, incitação à violência e desinformação. JOTA, 28 nov. 2024. Disponível em: https://www.jota.info/stf/do-supremo/julgamento-do-artigo-19-impacta-conteudo-comercial-incitacao-a-violencia-e-desinformacao. Acesso em: 29 nov. 2024.
[4] BRASIL. Projeto pretende coibir venda de produtos falsificados em plataformas on-line. Agência Senado, 02 ago. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/08/02/projeto-pretende-coibir-venda-de-produtos-falsificados-em-plataformas-on-line. Acesso em: 29 nov. 2024.
[5] SOARES, Matheus. Novo do PL de IA é "pró-inovação", mas mantém direitos e integridade da informação. Desinformante, 28 nov. 2024. Disponível em: https://desinformante.com.br/novo-pl-ia-inovacao-direitos/. Acesso em: 2 dez. 2024.
[6] WORLD METEOROLOGICAL ORGANIZATION. WMO joins Global Initiative for Information Integrity to fight climate disinformation. 20 nov. 2024. Disponível em: https://wmo.int/media/news/wmo-joins-global-initiative-information-integrity-fight-climate-disinformation. Acesso em: 2 dez. 2024.

10) INTEGRIDADE DA INFORMAÇÃO E DEVIDO PROCESSO INFORMACIONAL

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Regulações que obriguem às plataformas digitais adotarem medidas mais robustas de moderação de conteúdo e comportamento contra a prática e disseminação de conteúdo e atividades nocivas de seus usuários, por meio do instituto do devido processo informacional. Há alta probabilidade de regulamentação e responsabilização das aplicações de internet de acordo com as suas atividades, nos termos do Marco Civil da Internet.
POR QUE É TENDÊNCIA?	Tema intensamente debatido no G20 Brasil (2024) e já consolidado nas Nações Unidas em 2023, é fundamental para mitigar os impactos da disseminação de notícias falsas sobre processos democráticos, relações sociais e a economia global. Além disso, decisões jurídicas recentes no Brasil, como as discussões sobre o artigo 19 do Marco Civil da Internet, PL de IA, PL 2630/2000 e o Projeto de Lei 3.024/2024, reforçam o papel estratégico da governança informacional na construção de um ambiente digital mais seguro, transparente e responsável.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	A integridade informacional afeta diretamente o ambiente de negócios ao influenciar a confiança dos consumidores e a reputação das empresas. No comércio eletrônico, a presença de produtos falsificados não apenas prejudica a credibilidade das plataformas, mas também implica possíveis penalidades regulatórias. Para empresas de tecnologia, e-commerce e publicidade digital, decisões como as que envolvem o artigo 19 do Marco Civil da Internet trazem segurança jurídica ao definir limites claros para a responsabilização de conteúdos de terceiros.
SUGESTÕES DO VLK	Desenvolver melhor o conceito de devido processo informacional na moderação de conteúdo online, que busca garantir que os direitos dos usuários sejam respeitados e que os processos de decisão sejam justos, transparentes e fundamentados em critérios objetivos.

11) SUSTENTABILIDADE DIGITAL E GREEN TECH

TENDÊNCIAS PARA 2025

A Sustentabilidade Digital e Green Tech emerge como um pilar essencial em um cenário atual onde o consumo energético global por data centers deve crescer 160% até 2030, segundo relatório da *Goldman Sachs Research***[1]**. À medida que a inteligência artificial (IA) é amplamente adotada, sua integração com tecnologias verdes tem potencial para transformar o setor, com exemplos de sucesso em empresas como Google, Microsoft e Equinix. No Brasil, o Plano Brasileiro de Inteligência Artificial (PBIA) alinha o desenvolvimento de infraestruturas de alta capacidade à eficiência energética, fortalecendo o papel das energias renováveis e da inovação tecnológica no setor**[2]**.

POR QUE É TENDÊNCIA?

O crescimento acelerado de tecnologias digitais e a explosão de dados impulsionaram a expansão dos data centers, que atualmente consomem entre 1% e 2% da energia global, podendo alcançar 4% até o final da década. Soluções baseadas em IA são indispensáveis para mitigar os impactos ambientais desse crescimento, com destaque para:

- **Eficiência Energética:** A IA ajusta dinamicamente a distribuição de cargas e controla sistemas de resfriamento, reduzindo o consumo de energia em até 40% como demonstrado pela Google DeepMind;

- **Redução de Emissões:** A Equinix e outras líderes do setor têm implementado práticas de otimização energética, alinhando suas operações aos Objetivos de Desenvolvimento Sustentável (ODS) da ONU, especialmente o ODS 7, que visa dobrar a eficiência energética global até 2030; e

- **Impactos Locais:** No Brasil, iniciativas como o PBIA destinam R$ 5,79 bilhões à infraestrutura e desenvolvimento de IA, incentivando a criação de data centers energeticamente eficientes que utilizam energias renováveis.

Ainda, o texto atual do Marco Regulatório de IA, prevê o fomento da pesquisa e o desenvolvimento de programas de certificação para redução do impacto ambiental de sistemas de IA**[3]**.

COMO A TENDÊNCIA IMPACTA O SEU NEGÓCIO

A sustentabilidade digital afeta diretamente o ambiente empresarial, principalmente em

setores que dependem intensamente de tecnologias de alto desempenho e grandes volumes de dados, incluindo:

- **Custos Operacionais:** empresas que utilizam data centers podem reduzir significativamente seus custos por meio da otimização de recursos e da redução do consumo energético.

- **Conformidade Regulatória:** com regulamentações globais cada vez mais rígidas em relação à sustentabilidade, a adequação às novas normas será essencial para evitar penalidades e garantir competitividade no mercado internacional.

- **Reputação e ESG**: a adoção de práticas digitais sustentáveis fortalece indicadores ambientais, sociais e de governança (ESG), atraindo investidores e consumidores preocupados com impacto ambiental.

No Brasil, apesar dos desafios, o país apresenta vantagem estratégica praticamente única: disponibilidade de terreno, matriz energética limpa, que inclui fontes renováveis como hidrelétricas, energia solar e eólica, bem como disponibilidade de água para refrigeração dos equipamentos. Com políticas públicas e investimentos adequados, o Brasil pode se tornar polo de data centers verdes**[4]**. Inclusive, o Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC) e o Ministério da Ciência e Tecnologia e Inovação (MCTI) tentam avançar com políticas de fomento à construção de centros de dados, incluindo a cadeia produtiva do setor "entre as prioridades" do programa Nova Indústria Brasil (NIB), no tema de transformação digital**[5]**.

SUGESTÕES DO VLK

As empresas devem se preparar para as exigências e oportunidades relacionadas à Sustentabilidade Digital e Green Tech por meio de: (i) Auditorias de Sustentabilidade para identificar gargalos de eficiência energética e oportunidades de melhoria nas operações de TI; (ii) Planejamento Regulatório para se anteciparem às mudanças legislativas, especialmente nas áreas de eficiência energética e uso de IA; (iii) Incentivos Fiscais e Financiamentos com o aproveitamento de programas governamentais e internacionais de incentivo à implementação de tecnologias verdes e (iv) Estratégias ESG, já que o desenvolvimento de políticas robustas de sustentabilidade digital além de proteger o meio ambiente, reforçam a reputação das empresas no mercado.

O futuro digital e a emergência climática devem ser encarados como oportunidades para transformar desafios em avanços, especialmente para o Brasil.

[1] GOLDMAN SACHS. AI poised to drive 160% increase in power demand. Goldman Sachs, 2024. Disponível em: https://www.goldmansachs.com/insights/articles/AI-poised-to-drive-160-increase-in-power-demand. Acesso em: 29 nov. 2024.
[2] TELESÍNTESE. Freire: data centers e inteligência artificial. TeleSíntese, 2024. Disponível em: https://telesintese.com.br/freire-data-centers-e-inteligencia-artificial/. Acesso em: 29 nov. 2024.
[3] Texto da Comissão Temporária de IA do Senado, de 27.11.24.
[4] GOVERNO FEDERAL (Brasil). Agência Nacional de Telecomunicações. Conselheiro Alexandre Freire publica artigo sobre data centers e inteligência artificial. Brasília, DF, 9 set. 2024. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/noticias/conselheiro-alexandre-freire-publica-artigo-sobre-data-centers-e-inteligencia-artificial. Acesso em: 14 nov. 2024.
[5] Governo prepara uma política nacional para 'data centers'. Disponível em https://valor.globo.com/empresas/noticia/2024/11/11/governo-prepara-uma-politica-nacional-para-data-centers.ghtml. Acesso em: 14 nov. 2024.

11) SUSTENTABILIDADE DIGITAL E GREEN TECH

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Acreditamos que a IA será grande aliada para alcançar melhor eficiência energética e redução de resíduos e que esse tipo de solução tecnológica ganhará incentivos fiscais. Nessa linha, a pegada de carbono de atividades de tecnologia (inclusive de IA) deve ser medida e regulada. Por fim, devem surgir políticas públicas incentivando o reuso e a reciclagem de dispositivos eletrônicos.
POR QUE É TENDÊNCIA?	O crescimento acelerado de tecnologias digitais e a explosão de dados impulsionaram a expansão dos data centers e do desenvolvimento da IA, trazendo discussões sobre mitigar riscos ao meio ambiente derivadas do consumo energético.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	A sustentabilidade digital afeta diretamente o ambiente empresarial, principalmente em setores que dependem intensamente de tecnologias de alto desempenho e grandes volumes de dados, com custos operacionais, conformidade regulatória, reputação e ESG.
SUGESTÕES DO VLK	As empresas devem se preparar para as exigências e oportunidades relacionadas à Sustentabilidade Digital e *Green Tech* por meio de Auditorias de Sustentabilidade, Planejamento Regulatório, Incentivos Fiscais e Financiamentos e Estratégias de ESG.

12) NEURODIREITOS

TENDÊNCIAS PARA 2025

A regulação dos dados neurais é tendência crescente para 2025, devido ao avanço acelerado das neurotecnologias, que permitem a coleta e análise de informações relacionadas à atividade cerebral, como emoções, reações, intenções e níveis de atenção. Esses dados possuem potencial significativo para fins médicos, educacionais e comerciais, mas também levantam preocupações éticas e de privacidade, devido ao risco de manipulação, discriminação e exploração psicológica.

POR QUE É TENDÊNCIA?

Na América do Sul, o Chile lidera a iniciativa global**[1]**, sendo o primeiro país a incorporar os "neurodireitos" em sua Constituição, protegendo a integridade psíquica**[2]**. No Brasil, propostas regulatórias buscam incluir a proteção da integridade mental como direito fundamental previsto no artigo 5º da Constituição Federal**[3]**, bem como inserir expressamente a tutela dos dados neurais na Lei Geral de Proteção de Dados Pessoais (LGPD), abordando questões como transparência algorítmica e integridade mental. O Rio Grande do Sul foi o primeiro estado brasileiro que incorporou a tutela dos neurodireitos em sua Constituição Estadual como uma das bases da política de pesquisa científica e tecnológica promovidas pelo governo.

Nos EUA, estados como Califórnia e Colorado já aprovaram leis para classificar dados neurais como "dados pessoais sensíveis", protegendo os usuários contra coleta e uso sem consentimento, e ampliando o escopo da tutela da privacidade. Além disso, organizações como a *NeuroRights Foundation***[4]** e a UNESCO**[5]** defendem a necessidade de diretrizes claras para o uso ético dessas tecnologias, sugerindo a proteção da privacidade mental em escala internacional.

COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?

A regulação dos dados neurais acaba por impactar os agentes de tratamento de dados pessoais que fazem uso desses dados, assim como os agentes de IA que utilizam esses dados pessoais em sistemas de IA. Tais agentes deverão fortalecer suas práticas de *compliance*, previstas na LGPD (como indicação de base legal, mapeamento e registro desses tipos de dados, medidas de transparência, elaboração de relatórios de impacto à proteção de dados pessoais, dentre outras) e as que serão exigidas na futura legislação brasileira de IA.

Na medida em que envolvem dados do cérebro, tendem a ser considerados dados de saúde e, portanto, sensíveis, exigindo o fortalecimento da adoção de princípios éticos nas decisões corporativas para assegurar que o uso de tecnologias baseadas nesses tipos de dados não promova manipulação ou discriminação.

Esse cenário aumenta os custos de conformidade, especialmente para startups e pequenos negócios, mas também incentiva a inovação responsável.

SUGESTÕES DO VLK

É fundamental a participação na construção regulatória, de modo que os desafios sejam enfrentados de forma proporcional aos riscos que podem gerar, não se esquecendo do grande potencial das neurotecnologias de promover melhores condições de vida aos seres humanos. As empresas que priorizam práticas éticas podem se diferenciar no mercado, ganhando a confiança de consumidores e investidores preocupados com a privacidade e a integridade mental, no seguinte sentido:

- **Respeito à Autonomia Cognitiva:** assegurar que tecnologias neurotecnológicas respeitem a autonomia dos indivíduos sobre seus pensamentos, emoções e decisões.

- **Privacidade Mental e Compliance com Marcos Regulatórios Emergentes:** dados neurais são intrinsecamente sensíveis e demandam proteções rigorosas, nos termos da LGPD, incluindo anonimização, criptografia e controle de acesso. Ainda, empresas precisam se antecipar a regulações como a Ley de Neuroderechos no Chile e debates na UE e na ONU. Devem estruturar suas operações de maneira a atender princípios como a proteção da integridade mental e da identidade pessoal.

- **Avaliação de Impacto de Riscos Neuroéticos:** tal como as avaliações de impacto à privacidade, as empresas deveriam adotar avaliações de impacto neuroético, antecipando possíveis danos ao usuário e demonstrando proatividade em seu gerenciamento.

- **Não-Discriminação e Inclusão:** o uso de neurotecnologias não pode reforçar vieses ou discriminações. Projetos éticos devem priorizar a inclusão, garantindo que inovações sejam acessíveis e não exacerbem desigualdades sociais.

- **Accountability no Desenvolvimento Tecnológico:** transparência nos processos de desenvolvimento e a possibilidade de auditar decisões tomadas por algoritmos neurotecnológicos devem ser princípios fundamentais.

- **Criação de Comitês de Ética e Neurodireitos:** formar grupos internos para revisar e guiar decisões sobre neurotecnologias, envolvendo especialistas multidisciplinares.

- **Capacitação Interna:** treinar colaboradores sobre neurodireitos e implicações éticas para promover uma cultura de conformidade e inovação responsável.

[1] Disponível em: https://somosiberoamerica.org/pt-br/tribunas/neurodireitos-no-chile-consagracao-constitucional-e-regulacao-das-neurotecnologias/
[2] CONSTITUCIÓN POLÍTICA DE LA REPÚBLICA DE CHILE. Disponível em: https://www.camara.cl/camara/doc/leyes_normas/constitucion.pdf
[3] Art. 1º O art. 5º da Constituição Federal para a vigorar acrescido do inciso LXXX: "Art. 5º (...) LXXX – o desenvolvimento científico e tecnológico assegurará a integridade mental e a transparência algorítmica, nos termos da lei." Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9386704&ts=1689276688763&disposition=inline&_gl=1*17lzve*_ga*NzI2ODMyMzQuMTcwNzE2NDI1Ng..*_ga_CW3ZH25XMK*MTcwNzE2NDI1NS4xLjAuMTcwNzE2NDI4Ny4wLjAuMA
[4] https://neurorightsfoundation.org/
[5] https://www.unesco.org/en/node/86248

12) NEURODIREITOS

RESUMO EXECUTIVO

TENDÊNCIAS PARA 2025	Países, como o Chile, servirão de exemplo sobre como deve ser protegida a “privacidade mental”, tema que tem ganhado cada vez mais destaque com a disseminação da IA. Além disso, devem começar a surgir regulamentações sobre tecnologias de monitoramento neural, com organismos multilaterais (como ONU e OCDE) redigindo diretrizes globais para salvaguardar essas questões.
POR QUE É TENDÊNCIA?	Na América do Sul, o Chile lidera a iniciativa global, sendo o primeiro país a incorporar os "neurodireitos" em sua Constituição. No Brasil, propostas regulatórias buscam incluir a proteção da integridade mental como direito fundamental previsto no artigo 5º da Constituição Federal. Nos EUA, estados como Califórnia e Colorado já aprovaram leis para classificar dados neurais como "dados pessoais sensíveis". Além disso, organizações como a NeuroRights Foundation e a UNESCO defendem a necessidade de diretrizes claras para o uso ético dessas tecnologias, sugerindo a proteção da privacidade mental em escala internacional.
COMO A TENDÊNCIA IMPACTA SEU NEGÓCIO?	A regulação dos dados neurais acaba por impactar os agentes de tratamento de dados pessoais que fazem uso desses dados, assim como os agentes de IA que utilizam esses dados pessoais em sistemas de IA. Tais agentes deverão fortalecer suas práticas de compliance, previstas na LGPD - como indicação de base legal, mapeamento e registro desses tipos de dados, medidas de transparência, elaboração de relatórios de impacto à proteção de dados pessoais, dentre outras, - bem como as que serão exigidas na futura legislação brasileira de IA.
SUGESTÕES DO VLK	Acompanhar os principais projetos de lei sobre o tema e buscar entender como eles poderão impactar as atividades da organização, antecipando-se nos ajustes de governança sempre quando possível. Além disso, deve ser estimulada a adoção de práticas éticas e de governança, como: Respeito à Autonomia Cognitiva; Privacidade Mental e Compliance com Marcos Regulatórios Emergentes; Avaliação de Impacto de Riscos Neuroéticos; Não-Discriminação e Inclusão; *Accountability* no Desenvolvimento Tecnológico; Criação de Comitês de Ética e Neurodireitos; e Capacitação Interna.

CONCLUSÕES

Em 2025, o uso ético, seguro, responsável e lícito de dados e algoritmos será central nas estratégias corporativas. Esse investimento deixará de ser apenas em resposta a riscos legais ou incidentes, tornando-se estratégico para a revolução tecnológica, a transformação digital, a proteção de direitos fundamentais e a integração da agenda ESG.

A legitimidade no uso de dados trará benefícios como eficiência operacional, reputação corporativa fortalecida e maior confiança de stakeholders – clientes, parceiros, investidores e reguladores. Nesse cenário, a ética no uso de dados será diferencial competitivo para empresas que buscam inovar de forma responsável e sustentável.

A governança digital estruturada será essencial, permitindo às empresas alinhar inovação, segurança e conformidade por meio de frameworks sólidos e integrados. A confiança digital, sustentada pela cibersegurança, proteção de dados e inteligência artificial ética, impulsionará a transformação tecnológica com segurança e sustentabilidade.

Ferramentas como legal design e visual law ganharão destaque ao traduzir questões jurídicas complexas em soluções acessíveis e centradas no usuário, promovendo transparência e decisões informadas.

O contexto de 2025 também exigirá respostas inovadoras a desafios, como a fragmentação regulatória, com a harmonização normativa e a colaboração entre reguladores sendo essenciais. Além disso, combater o analfabetismo digital será crucial, por meio de investimentos em educação e capacitação para promover inclusão digital e reduzir desigualdades.

Cibersegurança, proteção de dados, inteligência artificial ética e governança digital estruturada consolidam-se como pilares para um progresso sustentável. O equilíbrio entre inovação tecnológica e responsabilidade ética será a base para construir confiança digital, promovendo competitividade, segurança e inclusão de forma integrada.

AUTORES

Rony Vainzof
rony@vlklaw.com.br

Caio Lima
caio@vlklaw.com.br

Gisele Karassawa
gisele@vlklaw.com.br

Alexandra Krastins
alexandra.lopes@vlklaw.com.br

Bruna Bigas
bruna.bigas@vlklaw.com.br

Giovanna Milanese
giovanna.milanese@vlklaw.com.br

Jean Santana
jean.santana@vlklaw.com.br

Mateus Lamonica
mateus.lamonica@vlklaw.com.br

Nuria Baxauli
nuria.baxauli@vlklaw.com.br

Paulo Sarmento
paulo.sarmento@vlklaw.com.br

Verônica Barros
veronica.barros@vlklaw.com.br

FICHA TÉCNICA:

E-book Tendências do Direito Digital, IA, Proteção de Dados e Ciber para 2025, de 12 de dezembro de 2024.

Para mais informações ou para questões relacionadas à publicação, entre em contato conosco através do e-mail contato@vlklaw.com.br.

Produção Gráfica:
Jennifer Santos

VLK ADV