

DIREITO DA INTELIGÊNCIA ARTIFICIAL

*Regulação, Responsabilidade, Proteção de Dados
e Governança Empresarial no Brasil*

Jardel Vieira Alves

Direito da Inteligência Artificial — Regulação, Responsabilidade, Proteção de Dados e Governança Empresarial no Brasil

© 2026 Jardel Vieira Alves. Todos os direitos reservados.

Edição atualizada até 6 de agosto de 2026.

Esta obra tem finalidade educacional e informativa. Não substitui parecer jurídico, análise regulatória ou aconselhamento profissional aplicável a caso concreto.

O PL 2.338/2023 é tratado neste livro como proposta legislativa em tramitação, e não como lei vigente. O leitor deve conferir alterações legislativas e regulatórias posteriores à data de atualização desta edição.

FONTES PRINCIPAIS

Constituição Federal; LGPD; Marco Civil da Internet; Código de Defesa do Consumidor; Código Civil; Lei de Direitos Autorais; Lei de Software; Lei de Defesa da Concorrência; Lei 14.133/2021; Lei 15.211/2025; Lei 15.352/2026; regulamentações e publicações da ANPD; tramitação oficial do PL 2.338/2023 no Senado e na Câmara dos Deputados.

Sumário

Nota ao leitor	5
Como usar este livro	7
Parte I — Fundamentos e enquadramento jurídico	7
Cap. 1 — O que o Direito regula quando regula IA	7
Cap. 2 — O mosaico normativo brasileiro	12
Cap. 3 — O ciclo de vida jurídico de um sistema de IA	15
Parte II — Dados pessoais, decisões e modelos generativos	19
Cap. 4 — LGPD aplicada à inteligência artificial	19
Cap. 5 — Decisões automatizadas e revisão humana	22
Cap. 6 — IA generativa, prompts e dados corporativos	25
Cap. 7 — Treinamento, fine-tuning e dados de terceiros	28
Parte III — Responsabilidade, consumo e propriedade intelectual	31
Cap. 8 — Responsabilidade civil por sistemas de IA	31
Cap. 9 — IA nas relações de consumo	34
Cap. 10 — Direitos autorais, software e conteúdo gerado	37
Cap. 11 — Contratos de inteligência artificial	39
Parte IV — Pessoas, segurança e direitos fundamentais	42
Cap. 12 — IA nas relações de trabalho	42
Cap. 13 — Segurança da informação e ataques contra IA	45
Cap. 14 — Discriminação algorítmica e direitos fundamentais	47
Cap. 15 — Crianças, adolescentes e o ECA Digital	50
Parte V — Mercado, setores regulados e poder público	52
Cap. 16 — Concorrência, plataformas e poder econômico	52
Cap. 17 — IA em setores regulados	55
Cap. 18 — IA no setor público e empresas contratadas	57
Parte VI — Governança empresarial e preparação regulatória	60
Cap. 19 — Programa corporativo de governança de IA	60
Cap. 20 — Auditoria, evidências e futuro marco brasileiro	62
Parte VII — Manual de implementação empresarial	65
Cap. 21 — Implantação em 90 dias	65
Cap. 22 — Métricas e indicadores de governança	67
Parte VIII — Riscos especializados e operações avançadas	69
Cap. 23 — Biometria, visão computacional e reconhecimento	69
Cap. 24 — Deepfakes, voz sintética e personalidade	72
Cap. 25 — Transferências internacionais e fornecedores globais	74
Cap. 26 — Conselho, M&A e diligência corporativa	76
Cap. 27 — Model Risk Management aplicado à IA	79
Cap. 28 — Agentes de IA e automação autônoma	81
Cap. 29 — IA no jurídico, compliance e auditoria	83
Cap. 30 — Fiscalização, prova e litígios envolvendo IA	85

Parte IX — Estudos de caso empresariais.....	87
Apêndices A–L — Modelos, matrizes, checklists e evidências.....	94
Conclusão	116
Referências legislativas, institucionais e técnicas	117

Nota ao leitor

A inteligência artificial deixou de ser um tema reservado a laboratórios de pesquisa e passou a integrar decisões empresariais rotineiras: concessão de crédito, triagem de currículos, atendimento ao consumidor, detecção de fraude, análise documental, programação, marketing, precificação, auditoria, saúde, educação, logística e inúmeras outras atividades. O problema jurídico surge justamente porque a tecnologia atravessa várias áreas do direito ao mesmo tempo. Não existe, no Brasil, uma única lei capaz de responder isoladamente a todas as perguntas criadas por um sistema de IA.

Este livro adota uma abordagem funcional. Em vez de tratar o “Direito da Inteligência Artificial” como um ramo completamente autônomo, parte da ideia de que a empresa precisa combinar normas constitucionais, proteção de dados, responsabilidade civil, defesa do consumidor, propriedade intelectual, contratos, direito do trabalho, concorrência, segurança da informação e regulações setoriais. A governança de IA funciona, portanto, como uma camada de coordenação jurídica e técnica.

A obra foi escrita para juristas, profissionais de compliance, encarregados de dados, gestores de risco, auditores, responsáveis por segurança da informação, desenvolvedores que atuam próximos da área jurídica e executivos que precisam transformar princípios abstratos em controles verificáveis. O nível é intermediário: pressupõe familiaridade básica com conceitos jurídicos, mas explica os elementos técnicos necessários para avaliar modelos, dados, fornecedores e fluxos de decisão.

O marco legislativo brasileiro de IA permanece em construção. O PL 2.338/2023 foi aprovado pelo Senado em dezembro de 2024 e remetido à Câmara dos Deputados em março de 2025. Em 6 de agosto de 2026, a matéria permanecia em Comissão Especial na Câmara, aguardando parecer do relator, com diversos projetos apensados. Por isso, o livro distingue rigorosamente três camadas: direito vigente; orientações regulatórias e padrões técnicos; e propostas legislativas ainda sujeitas a alteração. Sempre que o PL 2.338/2023 for discutido, ele será tratado como horizonte regulatório e não como obrigação legal já vigente.

Em paralelo, o ambiente institucional mudou. A Lei 15.352/2026 transformou a Autoridade Nacional de Proteção de Dados em Agência Nacional de Proteção de Dados, autarquia especial e agência reguladora. A Agenda Regulatória 2025-2026 da ANPD inclui inteligência artificial, tratamento de dados de alto risco, direitos dos titulares, relatório de impacto, biometria, segurança, anonimização e governança. A Lei 15.211/2025, o Estatuto Digital da Criança e do Adolescente, entrou em vigor em 17 de março de 2026 e adicionou deveres relevantes para produtos e serviços digitais acessíveis a crianças e adolescentes.

Este texto é material de estudo e orientação geral. A aplicação a um caso concreto exige análise das circunstâncias, dos contratos, do setor regulado, da arquitetura tecnológica e da legislação vigente na data da decisão.

Como usar este livro

O leitor pode seguir a ordem dos capítulos ou utilizar a obra como manual de consulta. Os capítulos iniciais constroem o vocabulário e o mapa normativo. Em seguida, são tratados dados pessoais, decisões automatizadas, IA generativa, responsabilidade, consumo, propriedade intelectual, contratos, relações de trabalho, segurança, discriminação, crianças e adolescentes, concorrência e setores regulados. Os últimos capítulos concentram governança, auditoria, documentação e preparação para o provável amadurecimento regulatório brasileiro.

Uma regra aparece repetidamente: a empresa não deve começar perguntando “qual lei de IA se aplica?”, mas “qual é a função real do sistema, que dados entram, quem é afetado, que decisão sai, qual o potencial de dano e quem controla cada etapa?”. A classificação jurídica nasce desse inventário.

Parte I — Fundamentos e enquadramento jurídico

Capítulo 1 — O que o Direito regula quando regula inteligência artificial

1.1 IA como sistema sociotécnico

A expressão “inteligência artificial” é útil como rótulo, mas insuficiente para o trabalho jurídico. Para fins de governança, importa menos discutir se um software “pensa” e mais identificar quais funções ele desempenha. Um sistema pode classificar, recomendar, prever, gerar conteúdo, detectar padrões, priorizar pessoas, automatizar tarefas ou apoiar decisões humanas. Cada função cria riscos diferentes. Um classificador de spam e um modelo que ajuda a decidir quem receberá crédito podem utilizar técnicas semelhantes, mas não ocupam a mesma posição jurídica.

A análise empresarial deve enxergar a IA como sistema sociotécnico. O resultado não depende apenas do modelo matemático. Ele nasce da combinação entre dados, regras de negócio, interface, configuração, pessoas, fornecedores, infraestrutura, incentivos e procedimentos internos. Um modelo com boa métrica estatística pode produzir dano se for usado fora do contexto para o qual foi testado. Da mesma forma, um modelo imperfeito pode ser aceitável quando funciona apenas como ferramenta

auxiliar e sua saída é revisada por profissional qualificado com acesso a informações adicionais.

Essa visão altera a pergunta sobre responsabilidade. A investigação não deve procurar um único “culpado algorítmico”, mas reconstruir a cadeia de decisões: quem definiu a finalidade, quem selecionou os dados, quem treinou ou adquiriu o modelo, quem parametrizou limites, quem decidiu automatizar, quem deveria revisar a saída e quem tinha capacidade de interromper o uso. Em ambientes corporativos maduros, cada uma dessas funções precisa possuir responsável identificável.

Para o jurídico, o primeiro produto de qualquer projeto relevante de IA deve ser um mapa do sistema. O mapa registra finalidade, usuários, titulares afetados, categorias de dados, modelo utilizado, origem do modelo, integrações, fornecedores, decisões influenciadas, possibilidade de revisão humana e consequências de falha. Sem esse documento, a empresa tende a discutir princípios de forma abstrata e perde a capacidade de demonstrar diligência.

Aplicação empresarial. Antes de aprovar uma ferramenta, descreva em uma página: entrada, processamento, saída, decisão humana posterior e efeito sobre pessoas. Essa pequena descrição costuma revelar se o problema principal está em privacidade, consumo, trabalho, propriedade intelectual, segurança, contrato ou regulação setorial.

1.2 IA, automação e modelos generativos

Nem toda automação é inteligência artificial e nem toda inteligência artificial gera conteúdo. Essa distinção é juridicamente importante porque as obrigações dependem

da função e do risco. Sistemas determinísticos aplicam regras previamente definidas; modelos estatísticos estimam probabilidades; sistemas de aprendizado de máquina extraem padrões de dados; modelos generativos produzem novas sequências de texto, imagem, áudio, vídeo ou código a partir de padrões aprendidos.

Modelos generativos adicionam riscos próprios. A saída pode ser plausível e incorreta; informações confidenciais podem ser inseridas em prompts; conteúdos protegidos podem aparecer de forma indevida; a origem de uma afirmação pode ser difícil de reconstruir; e o fornecedor pode utilizar entradas para melhoria do serviço conforme sua configuração contratual. Por isso, a política de uso de IA generativa não deve ser mera extensão da política de software. Ela precisa definir classes de informação permitidas, atividades que exigem revisão, usos proibidos e requisitos de fornecedores.

Outro ponto essencial é distinguir modelo, sistema e aplicação. O modelo é o componente que produz inferências ou conteúdo. O sistema inclui componentes adicionais, como banco de dados, filtros, autenticação, logs e interface. A aplicação é o uso concreto do sistema em determinado processo de negócio. A mesma tecnologia pode ser de baixo risco em um chatbot interno para dúvidas administrativas e de alto impacto quando utilizada para recomendar desligamentos de empregados.

Essa separação é especialmente útil nos contratos. O fornecedor do modelo pode não conhecer a finalidade final escolhida pelo cliente. O integrador pode controlar os dados e a interface. A empresa usuária pode definir a decisão que será tomada. A responsabilidade jurídica

precisa acompanhar o controle efetivo de cada etapa, e não apenas a marca comercial da tecnologia.

Regra de bolso. Se a empresa não consegue explicar onde termina o modelo e começa a decisão de negócio, ela provavelmente ainda não consegue distribuir corretamente os deveres jurídicos do projeto.

1.3 Princípios jurídicos como requisitos de engenharia

Princípios como finalidade, necessidade, transparência, prevenção, não discriminação e responsabilização não devem permanecer apenas em pareceres. Em projetos de IA, eles precisam ser convertidos em requisitos verificáveis. “Transparência”, por exemplo, pode significar aviso ao usuário, documentação interna, registro da versão do modelo, explicação dos principais fatores de uma decisão, indicação de conteúdo sintético ou informação sobre limitações conhecidas. O requisito depende do contexto.

O princípio da necessidade pode resultar em minimização de campos usados para treinamento, redução do período de retenção ou exclusão de atributos sem ganho mensurável de desempenho. A prevenção pode exigir testes antes da implantação, monitoramento de deriva, limites de confiança, revisão humana e plano de rollback. A não discriminação pode demandar métricas separadas por grupos juridicamente relevantes, investigação de proxies e validação de impactos adversos. A responsabilização exige evidências: atas, relatórios, logs, versões, aprovações e controles.

O advogado que atua com IA precisa aprender a formular perguntas testáveis. Em vez de “o algoritmo é

justo?”, pergunte quais grupos foram avaliados, qual métrica foi escolhida, qual diferença foi considerada aceitável e qual decisão foi tomada quando a métrica excedeu o limite. Em vez de “o sistema é explicável?”, pergunte que informação pode ser fornecida ao usuário sem revelar segredo comercial e ainda assim permitir compreensão e contestação adequadas.

Essa tradução evita dois extremos. O primeiro é o formalismo, no qual a empresa produz políticas sofisticadas sem alterar a tecnologia. O segundo é o tecnicismo, no qual a equipe mede desempenho do modelo sem considerar direitos, contratos e consequências sociais. Governança de IA existe para conectar esses mundos.

Capítulo 2 — O mosaico normativo brasileiro

2.1 Constituição, direitos fundamentais e proteção de dados

A Constituição Federal é o ponto de partida da regulação de IA no Brasil, ainda que não mencione algoritmos. Igualdade, intimidade, vida privada, honra, imagem, liberdade de expressão, acesso à informação, devido processo e defesa do consumidor fornecem parâmetros para interpretar usos tecnológicos. A Emenda Constitucional 115/2022 acrescentou a proteção de dados pessoais ao catálogo de direitos e garantias fundamentais, inclusive nos meios digitais.

A constitucionalização da proteção de dados tem efeito prático. Tratamentos algorítmicos não são avaliados apenas como questões contratuais entre empresa e usuário. Determinadas práticas podem afetar direitos fundamentais e exigir justificativa proporcional. Em

sistemas de vigilância, biometria, classificação de pessoas ou decisões com grande impacto, a pergunta jurídica inclui adequação, necessidade e existência de alternativas menos intrusivas.

No setor privado, direitos fundamentais irradiam efeitos por meio da legislação civil, consumerista, trabalhista e de proteção de dados. Uma empresa não precisa exercer poder estatal para produzir assimetria relevante. Plataformas, empregadores, instituições financeiras e grandes provedores de serviços podem organizar oportunidades e restringir acessos de modo significativo. A governança corporativa deve reconhecer esse potencial e criar mecanismos de contestação compatíveis com a gravidade da decisão.

A consequência metodológica é simples: a ausência de uma “lei geral de IA” em vigor não cria vazio jurídico. O sistema continua submetido a normas existentes. O que muda é a dificuldade de encaixá-las em cadeias técnicas complexas. É justamente nessa interseção que surge o trabalho jurídico especializado.

2.2 LGPD, Marco Civil, CDC e Código Civil

A Lei Geral de Proteção de Dados é a norma mais frequentemente acionada em projetos de IA porque muitos sistemas dependem de dados pessoais durante treinamento, validação, inferência ou monitoramento. A LGPD define princípios, bases legais, direitos dos titulares, deveres de segurança, responsabilidades de controlador e operador e regras para transferência internacional. Seu art. 20 trata especificamente do direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem interesses do titular.

O Marco Civil da Internet incide quando o sistema se conecta a aplicações de internet, registros, comunicações e responsabilidades próprias do ambiente online. O Código de Defesa do Consumidor ganha centralidade quando a IA é incorporada a produtos, serviços, publicidade, atendimento, recomendação, precificação ou concessão de benefícios. Informação adequada, segurança, qualidade, boa-fé e responsabilidade do fornecedor continuam aplicáveis mesmo quando a decisão foi mediada por software.

O Código Civil fornece fundamentos para atos ilícitos, abuso de direito, boa-fé contratual, danos e responsabilidade civil. Em relações empresariais, também orienta interpretação de contratos, deveres anexos e alocação de riscos. Uma cláusula que transfere toda responsabilidade de um sistema crítico ao fornecedor pode não resolver o problema se a empresa contratante controlou finalidade, dados e decisão final.

O ponto central é a cumulação de regimes. Um incidente envolvendo um chatbot pode simultaneamente envolver LGPD, CDC, responsabilidade contratual, propriedade intelectual e regras setoriais. A avaliação não deve escolher uma lei e ignorar as demais; precisa construir uma matriz normativa por fluxo de risco.

2.3 Normas recentes: ANPD e ECA Digital

Em 2026, duas mudanças tornaram o cenário brasileiro mais concreto. A primeira foi institucional: a Lei 15.352/2026 transformou a ANPD em agência reguladora, com autonomia funcional, técnica, decisória, administrativa e financeira. Isso reforça sua capacidade regulatória e fiscalizatória e torna ainda mais relevante

acompanhar resoluções, guias, agendas e processos da Agência.

A Agenda Regulatória 2025-2026 inclui um projeto específico sobre inteligência artificial, com atenção ao art. 20 da LGPD, direitos dos titulares, princípios, hipóteses legais e boas práticas de governança. Também inclui tratamento de dados de alto risco, biometria, relatório de impacto, padrões mínimos de segurança, anonimização e governança. Para empresas, isso significa que a preparação não deve aguardar a aprovação do PL 2.338/2023. Muitos controles que provavelmente serão esperados já podem ser derivados da LGPD e da agenda regulatória.

A segunda mudança foi o Estatuto Digital da Criança e do Adolescente, Lei 15.211/2025, vigente desde 17 de março de 2026. A lei alcança produtos e serviços de tecnologia da informação direcionados a menores ou de acesso provável por eles e cria obrigações relacionadas a prevenção, segurança, supervisão parental, aferição de idade, publicidade e design de serviços. Em março de 2026, o Decreto 12.880 regulamentou aspectos relevantes e atribuiu à ANPD papel central de regulamentação e fiscalização.

Para empresas digitais, a consequência é clara: “não somos um aplicativo infantil” não basta como conclusão. É necessário avaliar acesso provável, atratividade, facilidade de acesso e grau de risco. Produtos generalistas podem entrar no campo de incidência se, na prática, forem utilizados por crianças ou adolescentes em condições relevantes.

Capítulo 3 — O ciclo de vida jurídico de um sistema de IA

3.1 Da ideia ao inventário

A governança começa antes da compra ou do desenvolvimento. O primeiro controle é o inventário de casos de uso. Cada projeto deve possuir identificação, unidade responsável, patrocinador executivo, finalidade, categoria de usuários, pessoas afetadas, dados envolvidos, fornecedor, modelo, integrações e criticidade preliminar. A ausência de inventário é um dos maiores obstáculos à conformidade porque ferramentas de IA podem ser contratadas diretamente por áreas de negócio e utilizadas sem conhecimento de jurídico, segurança ou privacidade.

O inventário deve incluir ferramentas gratuitas e recursos de IA embutidos em softwares já contratados. Um editor de texto que recebe um novo assistente generativo pode alterar significativamente o fluxo de dados sem que a empresa assine novo contrato. Da mesma forma, uma API de terceiros pode trocar silenciosamente a versão do modelo, modificando desempenho, localização de processamento ou práticas de retenção.

Shadow AI é o nome frequentemente dado ao uso não autorizado ou não governado de ferramentas de IA. O problema não se resolve apenas com bloqueio tecnológico. Políticas excessivamente restritivas podem empurrar usuários para canais informais. A abordagem mais eficiente combina catálogo de ferramentas aprovadas, regras claras sobre dados permitidos, treinamento e um processo rápido para avaliar novas soluções.

O jurídico deve exigir que todo caso de uso relevante tenha um “dono”. Sem responsável pelo processo de negócio, não existe quem possa decidir se o benefício compensa o risco, validar os resultados ou suspender a operação. A área de tecnologia pode administrar o sistema, mas não deve assumir sozinha a responsabilidade pela finalidade empresarial.

3.2 Avaliação preliminar de risco

Nem todo uso precisa de um relatório extenso. A empresa pode adotar triagem em duas etapas. A primeira pergunta se o sistema envolve dados pessoais sensíveis, crianças, biometria, saúde, crédito, emprego, educação, segurança, decisões que afetam direitos, monitoramento em larga escala, conteúdo sintético persuasivo ou atuação em setor regulado. Se a resposta for positiva, o caso segue para avaliação aprofundada.

A triagem também deve analisar reversibilidade. Um erro em resumo de reunião pode ser corrigido facilmente; um erro que exclui candidato de processo seletivo pode impedir oportunidade; um falso positivo de fraude pode bloquear conta; uma recomendação clínica incorreta pode ter consequências graves. Quanto menos reversível o dano, maior deve ser a exigência de supervisão, teste e documentação.

Outro critério é a autonomia. Sistemas que apenas organizam informação apresentam risco diferente daqueles que executam ações automaticamente. A expressão “human in the loop” não deve ser aceita sem análise. Revisão humana real exige tempo, autoridade, acesso aos dados necessários, possibilidade de discordar do sistema e ausência de incentivos que transformem a revisão em mera confirmação automática.

A matriz de risco deve produzir consequências. Classificar um sistema como “alto” sem alterar controles é inútil. Cada nível pode determinar requisitos de aprovação, testes, monitoramento, frequência de revisão, documentação, cláusulas contratuais e participação de comitês.

3.3 Desativação e mudança de modelo

O ciclo jurídico não termina na implantação. Modelos mudam, dados mudam e o contexto de uso muda. Uma solução considerada adequada em determinado momento pode perder desempenho, adquirir novas funcionalidades ou passar a tratar informações adicionais. A empresa deve definir eventos que obrigam nova avaliação: troca de modelo, mudança substancial de finalidade, inclusão de nova categoria de dados, aumento de autonomia, expansão geográfica ou alteração relevante do fornecedor.

Desativar um sistema também exige governança. É necessário decidir o destino de dados, embeddings, logs, vetores, backups e credenciais. Contratos devem prever exportação ou eliminação, apoio de transição e comprovação quando necessário. Em sistemas críticos, a empresa precisa evitar dependência técnica que torne impossível migrar para outro fornecedor.

Um controle particularmente importante é o registro de versões. Quando um cliente contesta uma decisão tomada seis meses antes, a organização precisa saber qual modelo estava ativo, quais regras de negócio foram aplicadas e quais dados relevantes entraram no processo. Sem versionamento, a explicação posterior pode se tornar especulativa.

A documentação do ciclo de vida é, em última análise, prova de governança. Ela permite demonstrar que a organização identificou riscos, escolheu controles proporcionais e revisou o sistema quando houve mudanças materiais.

Parte II — Dados pessoais, decisões e modelos generativos

Capítulo 4 — LGPD aplicada à inteligência artificial

4.1 Papéis de controlador e operador

Em projetos de IA, a classificação entre controlador e operador não deve seguir automaticamente o contrato comercial. Controlador é quem toma as decisões referentes ao tratamento de dados pessoais; operador realiza o tratamento em nome do controlador. Um fornecedor de IA pode ser operador para determinada finalidade e controlador para outra. Por exemplo, pode processar prompts apenas para prestar o serviço ao cliente, mas decidir independentemente utilizar certos dados para segurança, prevenção de abuso ou melhoria de produto.

Essa multiplicidade de papéis exige mapear finalidades. Termos contratuais genéricos como “poderemos usar dados para melhorar nossos serviços” precisam ser examinados com atenção. Se a empresa envia dados pessoais de clientes a uma ferramenta, deve saber se esses dados serão utilizados no treinamento de modelos, por quanto tempo serão retidos, onde serão

processados, que suboperadores participam e quais mecanismos de exclusão existem.

A posição jurídica também afeta atendimento de direitos. Se um titular solicitar informação, correção ou eliminação, a empresa precisa conseguir acionar o fornecedor quando a operação estiver sob sua responsabilidade. Contratos devem estabelecer cooperação, prazos e formatos de resposta. A cláusula de proteção de dados não pode ser desconectada da arquitetura técnica.

Nos modelos contratados via API empresarial, é recomendável separar dados de entrada, dados de telemetria, dados de suporte e dados de treinamento. Cada categoria pode ter finalidade e prazo diferentes. Essa decomposição melhora tanto a análise de base legal quanto a negociação comercial.

4.2 Bases legais e finalidade

Não existe uma base legal chamada “inteligência artificial”. Cada tratamento precisa se apoiar em hipótese compatível com a LGPD. Consentimento pode ser adequado em alguns contextos, mas não deve ser escolhido por reflexo. Execução de contrato, legítimo interesse, obrigação legal, proteção do crédito e outras hipóteses podem ser mais coerentes conforme a finalidade e a categoria de dados.

O legítimo interesse exige especial cautela quando o tratamento surpreende o titular, envolve perfilamento intenso ou produz consequências relevantes. A avaliação deve documentar finalidade legítima, necessidade, balanceamento com direitos e salvaguardas. Em sistemas de IA, a tentação de coletar “o máximo possível porque

pode ser útil ao modelo” é incompatível com o princípio da necessidade.

Mudança de finalidade é outro risco recorrente. Dados coletados para prestar um serviço podem ser posteriormente considerados valiosos para treinar um modelo. O fato de a empresa possuir tecnicamente os dados não significa que qualquer reutilização seja juridicamente compatível. A análise deve considerar contexto original, expectativa do titular, natureza dos dados, impacto e possibilidade de adoção de técnicas menos invasivas.

Para dados sensíveis, o regime é mais restrito. Saúde, biometria e informações que revelem origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou vida sexual exigem hipótese específica do art. 11 da LGPD. Modelos capazes de inferir atributos sensíveis a partir de dados aparentemente comuns também merecem tratamento cuidadoso, porque o risco pode surgir da inferência e não apenas do campo explicitamente coletado.

4.3 Minimização, qualidade e retenção

Modelos de IA costumam incentivar a ideia de que mais dados sempre produzem melhores resultados. Na prática, dados adicionais podem aumentar custo, ruído, viés e exposição jurídica sem benefício proporcional. A minimização deve ser testada empiricamente: remover determinado atributo degrada de forma relevante a finalidade legítima do sistema? Se não, sua manutenção precisa ser questionada.

Qualidade de dados assume dimensão jurídica quando informações incorretas alimentam decisões sobre pessoas.

Bases históricas podem conter erros, padrões discriminatórios ou classificações desatualizadas. O processo de curadoria deve registrar origem, critérios de exclusão, atualização e limitações conhecidas. Para dados adquiridos de terceiros, a empresa deve investigar legitimidade de coleta e permissões de uso, e não apenas confiar em declarações comerciais.

Retenção também precisa ser separada por etapa. Dados brutos de treinamento, conjuntos de validação, prompts, respostas, logs e métricas podem ter prazos diferentes. A pergunta “por quanto tempo o sistema guarda meus dados?” raramente possui uma única resposta. O programa de retenção deve refletir essa complexidade e possibilitar eliminação quando aplicável.

Anonimização e pseudonimização são controles úteis, mas não mágicos. Dados pseudonimizados continuam pessoais quando a reidentificação é possível com informação adicional. Mesmo conjuntos declarados anônimos podem apresentar risco de reidentificação dependendo da granularidade e do contexto. A avaliação deve ser técnica e jurídica.

Capítulo 5 — Decisões automatizadas, perfilamento e revisão humana

5.1 O alcance do art. 20 da LGPD

O art. 20 da LGPD assegura ao titular o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive decisões destinadas a definir perfil pessoal, profissional, de consumo e de crédito ou aspectos de personalidade. A redação torna

duas perguntas essenciais: a decisão é unicamente automatizada? E ela afeta interesses do titular?

A presença nominal de um humano não necessariamente elimina a automatização. Se o operador apenas aceita a recomendação sem análise real, a organização deve ser cautelosa ao afirmar que há decisão humana. A revisão precisa ser substancial e deve poder mudar o resultado. Para processos de grande escala, isso também exige dimensionamento operacional; não adianta prometer revisão se a empresa não possui equipe ou informações para realizá-la.

A LGPD também prevê dever de fornecer informações claras e adequadas sobre critérios e procedimentos utilizados para a decisão automatizada, observados segredos comercial e industrial. Esse equilíbrio é importante: transparência não exige necessariamente divulgar código-fonte ou parâmetros proprietários. Exige, porém, informação útil para compreender a lógica relevante e exercer direitos.

A ANPD incluiu inteligência artificial em sua Agenda Regulatória 2025-2026 justamente com destaque para parâmetros interpretativos do art. 20. Empresas devem acompanhar essa evolução e adotar desde já mecanismos que sejam defensáveis: canal de contestação, registro da decisão, principais fatores, evidências de revisão e possibilidade de correção de dados.

5.2 Explicabilidade útil

Explicabilidade é um conceito técnico e jurídico com múltiplos níveis. Uma equipe de ciência de dados pode precisar entender variáveis e comportamento estatístico; o jurídico precisa reconstruir critérios e responsabilidades; o

titular necessita de explicação compreensível sobre uma decisão específica; o regulador pode exigir documentação mais detalhada. A mesma explicação não serve para todos.

Uma boa explicação ao usuário deve responder, quando aplicável: qual decisão foi tomada; que tipo de informação foi relevante; quais fatores principais pesaram; que limitações existem; como corrigir dados; e como contestar o resultado. Informações excessivamente técnicas podem ser tão pouco transparentes quanto silêncio.

Para sistemas complexos, a organização pode combinar explicações locais e globais. A explicação global descreve como o sistema normalmente funciona; a local trata do caso concreto. Nenhuma delas deve prometer causalidade quando a técnica apenas identifica correlação ou contribuição estatística.

O jurídico também deve proteger a integridade da explicação. Explicações pós-hoc não podem ser inventadas para justificar decisão já tomada. Se a organização não consegue reproduzir o resultado ou identificar fatores relevantes, esse é um risco de governança que precisa ser tratado antes da escala.

5.3 Perfilamento e inferências

Perfilamento combina dados para classificar ou prever características de uma pessoa. Pode ser utilizado para marketing, prevenção de fraude, crédito, segurança, recursos humanos e personalização. O risco aumenta quando atributos inferidos não foram fornecidos diretamente pelo titular ou quando o perfil produz consequências que a pessoa não consegue perceber.

Inferências podem ser erradas. Um sistema que associa comportamento de navegação a vulnerabilidade financeira ou intenção de compra pode gerar segmentações imprecisas. Quando a organização transforma inferência em fato, pode prejudicar o titular e comprometer a qualidade dos dados. É recomendável identificar claramente quais campos são observados e quais são inferidos.

Também é preciso avaliar proxies. Mesmo que o modelo não use diretamente raça, gênero ou condição de saúde, outras variáveis podem reproduzir essas informações. CEP, padrões de consumo, nome, escola, dispositivo e histórico podem atuar como substitutos estatísticos. A retirada do atributo sensível não garante neutralidade.

Em aplicações de alto impacto, a empresa deve testar resultados por grupos e investigar diferenças relevantes. O objetivo não é exigir igualdade matemática absoluta em todos os cenários, mas compreender se diferenças decorrem de finalidade legítima, qualidade dos dados ou discriminação indevida e se existem alternativas menos danosas.

Capítulo 6 — IA generativa, prompts e dados corporativos

6.1 O prompt como fluxo de dados

Em empresas, o prompt deve ser tratado como canal de informação. Funcionários podem inserir contratos, código-fonte, planilhas, dados de clientes, segredos comerciais e informações pessoais em ferramentas generativas. A interface conversacional cria uma falsa

sensação de informalidade, mas juridicamente o envio pode representar tratamento por terceiro, transferência internacional ou divulgação não autorizada.

A política interna precisa definir classes de informação. Dados públicos podem ter uso amplo; informações internas podem depender de ferramenta corporativa aprovada; dados confidenciais, pessoais sensíveis ou segredos estratégicos podem exigir ambiente privado ou ser proibidos. A regra precisa ser simples o bastante para uso cotidiano.

Além da política, controles técnicos ajudam. Single sign-on, desativação de treinamento quando disponível, retenção reduzida, filtros de dados sensíveis, gestão centralizada de contas e logs corporativos diminuem a dependência de comportamento individual. A empresa deve preferir versões empresariais com compromissos claros de segurança e tratamento de dados quando o caso exigir.

A orientação “não cole dados pessoais” é insuficiente quando o trabalho do empregado consiste justamente em analisar documentos contendo esses dados. O programa precisa oferecer alternativa segura; caso contrário, a pressão por produtividade tende a vencer a regra formal.

6.2 Alucinações, verificação e dever profissional

Modelos generativos produzem texto probabilístico. Podem apresentar fatos falsos com aparência convincente, inventar referências, misturar jurisdições ou reproduzir informação desatualizada. Em atividades jurídicas, contábeis, financeiras e técnicas, o risco decorre não apenas do erro, mas da confiança excessiva na forma persuasiva da resposta.

Uma política madura não proíbe genericamente o uso, mas define quando a saída exige verificação independente. Citações jurídicas, cálculos relevantes, dados financeiros, recomendações médicas, compromissos contratuais e comunicações regulatórias não devem ser aceitos sem revisão compatível com o risco. A pessoa responsável continua sendo responsável por seu trabalho profissional.

Empresas podem criar uma taxonomia de usos. Brainstorming, resumo preliminar e reescrita de texto de baixo risco podem exigir revisão simples. Decisões externas ou material que produz obrigação jurídica exigem verificação de fonte. Usos em que um erro possa causar dano grave devem ser limitados ou submetidos a procedimento específico.

A própria interface pode lembrar limitações. Avisos contextuais, exigência de confirmação para determinadas tarefas e ligação a fontes corporativas confiáveis reduzem erro. Governança eficiente é incorporada ao fluxo de trabalho, não apenas a documentos que ninguém consulta.

6.3 RAG, bases internas e confidencialidade

Retrieval-Augmented Generation, ou RAG, combina um modelo generativo com busca em bases internas. A técnica pode reduzir alucinações e tornar respostas mais úteis, mas cria novos riscos. O sistema precisa respeitar permissões de acesso: um funcionário não deve descobrir por meio do chatbot documentos que não poderia abrir diretamente.

O controle de acesso deve funcionar antes da recuperação. Também é necessário verificar o que entra no índice vetorial, como exclusões são propagadas, como

dados sensíveis são segregados e quanto tempo embeddings permanecem. Embeddings não devem ser tratados automaticamente como anônimos; podem preservar informação suficiente para gerar riscos de inferência ou reconstrução.

A empresa precisa decidir se respostas devem exibir fontes. Em aplicações internas, referências aos documentos de origem melhoram verificabilidade e permitem ao usuário distinguir conteúdo recuperado de formulação do modelo. Em alguns contextos, também é recomendável registrar quais documentos sustentaram determinada resposta.

RAG não substitui gestão documental. Se a base contém versões conflitantes ou documentos obsoletos, o modelo pode apenas acelerar a propagação da inconsistência. A qualidade jurídica da IA depende da qualidade da informação corporativa disponível.

Capítulo 7 — Treinamento, fine-tuning e dados de terceiros

7.1 Origem e legitimidade dos dados

Treinar ou ajustar um modelo exige responder de onde vieram os dados e com que permissões podem ser utilizados. Dados obtidos publicamente na internet não estão automaticamente livres de proteção jurídica. Podem envolver dados pessoais, direitos autorais, termos de uso, confidencialidade, segredos comerciais ou restrições contratuais.

Em projetos próprios, a organização deve manter documentação de proveniência. Para cada conjunto relevante: origem, data, método de obtenção, licença, base

legal quando houver dados pessoais, finalidade, restrições e responsável. Essa disciplina é especialmente importante quando conjuntos são combinados e depois se torna difícil reconstruir a cadeia de origem.

Fornecedores de dados devem passar por due diligence. Uma declaração genérica de que o conjunto é “legal” não elimina o risco. O contrato deve conter garantias sobre direitos de disponibilização, mecanismos de resposta a reclamações e, conforme o caso, indenização. A empresa também deve avaliar se consegue cumprir pedidos de exclusão ou correção que atinjam dados incorporados ao pipeline.

A legitimidade precisa ser reavaliada conforme o uso. Dados licenciados para análise podem não estar autorizados para treinamento comercial. Um dataset interno criado para pesquisa pode não permitir implantação em produto. Finalidade técnica e finalidade jurídica precisam caminhar juntas.

7.2 Fine-tuning e adaptação de modelos

Fine-tuning altera o comportamento do modelo por meio de exemplos adicionais. Do ponto de vista jurídico, pode aumentar o controle da empresa e, ao mesmo tempo, sua responsabilidade sobre o resultado. Se a organização seleciona dados, define respostas desejadas e calibra o modelo para um domínio, participa diretamente da construção do comportamento que será oferecido aos usuários.

O processo deve separar conjunto de treinamento, validação e teste. Isso não é apenas boa prática técnica; ajuda a demonstrar que o sistema foi avaliado antes da implantação. Conjuntos de teste devem incluir casos

difíceis, exceções e situações de possível dano. Testar apenas exemplos médios produz falsa segurança.

Quando o fine-tuning usa conversas de clientes ou documentos internos, bases legais, transparência e retenção precisam ser avaliadas. A empresa deve evitar usar automaticamente todo histórico disponível. Amostragem, anonimização quando efetiva, revisão e filtros podem reduzir exposição.

Também é necessário controlar “catastrophic forgetting”, mudanças inesperadas de comportamento e regressões. Toda atualização significativa deveria ser acompanhada de testes mínimos de segurança e desempenho antes de entrar em produção.

7.3 Dados sintéticos

Dados sintéticos podem reduzir dependência de dados reais, mas não eliminam automaticamente riscos. Se forem gerados a partir de conjunto original com alta capacidade de memorização, podem reproduzir padrões ou registros próximos de indivíduos reais. A empresa deve avaliar risco de reidentificação e memorization leakage.

Do ponto de vista jurídico, dados sintéticos são ferramenta de minimização quando realmente rompem o vínculo com pessoas identificáveis. Isso exige análise técnica. A simples etiqueta “synthetic” não transforma o conjunto em anônimo para fins da LGPD.

O uso é particularmente interessante para testes de software e cenários raros. Em vez de copiar base de produção para ambiente de desenvolvimento, a empresa pode gerar dados que preservem estrutura estatística sem

expor pessoas. Essa arquitetura reduz superfície de ataque e facilita controles de acesso.

O princípio geral é escolher a solução menos intrusiva que cumpra a finalidade. Se um processo pode ser desenvolvido e testado com dados sintéticos adequados, o uso de dados pessoais reais precisa de justificativa adicional.

Parte III — Responsabilidade, consumo e propriedade intelectual

Capítulo 8 — Responsabilidade civil por sistemas de IA

8.1 O dano não é causado “pela IA” em abstrato

Quando um sistema de IA causa ou contribui para um prejuízo, a primeira tarefa jurídica é reconstruir a cadeia causal. A expressão “foi o algoritmo” é insuficiente. Algoritmos não contratam fornecedores, não escolhem finalidades empresariais nem definem sozinhos procedimentos de revisão. É preciso identificar atos e omissões de desenvolvedores, integradores, operadores, administradores, usuários e responsáveis pela decisão de negócio.

O Código Civil estabelece a obrigação de reparar dano decorrente de ato ilícito e admite responsabilidade independentemente de culpa em hipóteses legais ou quando a atividade normalmente desenvolvida implicar risco para direitos de terceiros. A incidência concreta depende do caso, da relação jurídica e do regime especial

aplicável. Em relações de consumo, o CDC pode estabelecer responsabilidade objetiva do fornecedor. Em tratamento de dados, os arts. 42 a 45 da LGPD criam regime próprio de reparação e dialogam com a legislação consumerista.

A governança deve ser construída como sistema de prevenção e também como sistema probatório. Após um incidente, será relevante demonstrar quais riscos eram conhecidos, que testes foram realizados, quem aprovou a implantação, quais alertas foram configurados e como a empresa reagiu. A ausência de documentação pode dificultar a prova de diligência e transformar uma falha pontual em aparente falha sistêmica.

É útil separar três perguntas: houve defeito ou conduta inadequada? Esse defeito contribuiu causalmente para o dano? Qual agente tinha controle ou dever de evitar o resultado? Essa estrutura evita atribuir responsabilidade apenas com base na proximidade tecnológica.

8.2 Erro de modelo, erro de uso e erro organizacional

Um sistema pode falhar porque o modelo apresenta limitação estatística; porque foi usado fora da finalidade; porque dados de entrada estavam errados; porque um humano ignorou alerta; ou porque a organização não criou controle necessário. Essas categorias ajudam a distribuir responsabilidades.

Erro de modelo inclui desempenho insuficiente, viés, instabilidade ou vulnerabilidade conhecida. Erro de uso ocorre quando o sistema é aplicado em contexto não autorizado, por exemplo, utilizar ferramenta de resumo como fonte decisória sem verificação. Erro organizacional inclui ausência de treinamento, governança, segregação

de funções ou monitoramento. Em litígios, mais de uma categoria pode coexistir.

Contratos devem refletir essa taxonomia. O fornecedor pode garantir conformidade do serviço com documentação e níveis de disponibilidade; o cliente assume dever de utilizar dentro de finalidade; e ambos definem obrigações de comunicação de falhas. Cláusulas que simplesmente declaram “IA pode cometer erros” não afastam automaticamente deveres legais de qualidade e segurança.

A empresa também deve identificar riscos previsíveis de uso indevido. Se determinada funcionalidade facilita dano óbvio e recorrente, o argumento de que o usuário “não deveria ter feito isso” pode ser fraco sem controles razoáveis. Prevenção proporcional deve fazer parte do design.

8.3 Responsabilidade por terceiros e fornecedores

A terceirização não terceiriza integralmente o risco. Uma empresa que incorpora um modelo de terceiro ao próprio serviço pode responder perante clientes e titulares mesmo que a causa técnica esteja no fornecedor. O contrato servirá para regresso, cooperação e alocação econômica, mas não necessariamente impedirá a responsabilização externa.

Due diligence precisa avaliar estabilidade financeira do fornecedor, segurança, governança, localização de dados, subcontratados, histórico de incidentes, capacidade de auditoria e cobertura de seguro quando pertinente. Para sistemas críticos, é prudente avaliar continuidade de negócio e possibilidade de substituição.

Limitações de responsabilidade são comuns em contratos de tecnologia, especialmente serviços globais padronizados. O jurídico deve comparar o limite contratual com a exposição real. Um teto equivalente a poucos meses de mensalidade pode ser irrelevante diante de um incidente envolvendo milhares de titulares. Quando o poder de negociação é baixo, a empresa deve compensar por arquitetura, redução de dados e limitação de uso.

O melhor contrato não transforma fornecedor inadequado em fornecedor seguro. Governança começa na seleção e continua durante toda a relação.

Capítulo 9 — Inteligência artificial nas relações de consumo

9.1 Informação, transparência e confiança

O Código de Defesa do Consumidor exige informação adequada e clara sobre produtos e serviços. Quando IA afeta atendimento, recomendação, oferta ou decisão relevante, a empresa precisa avaliar se o consumidor deve ser informado sobre a automação e em que nível. Nem todo uso interno exige aviso destacado, mas ocultar característica material capaz de afetar decisão do consumidor pode ser problemático.

Chatbots são exemplo simples. O usuário deve saber quando está interagindo com sistema automatizado se essa informação for relevante à sua expectativa e aos canais de atendimento. Também deve existir mecanismo de escalonamento humano para situações que o sistema não consegue resolver, especialmente reclamações, cancelamentos, cobranças e disputas.

Transparência não autoriza inundar o consumidor com termos extensos. Informação essencial deve aparecer no momento adequado. A empresa pode adotar camadas: aviso curto na interface, explicação adicional e política detalhada. O desenho da experiência do usuário é parte do compliance.

Confiança é especialmente sensível em conteúdo generativo. Se a empresa utiliza avatar, voz sintética ou recomendação personalizada, deve evitar criar impressão enganosa de endosso humano, autoridade profissional ou autenticidade. O risco jurídico aumenta quando a técnica manipula vulnerabilidades ou dificulta percepção do caráter publicitário.

9.2 Oferta, publicidade e conteúdo sintético

Publicidade gerada por IA continua submetida às regras de publicidade. Afirmativas objetivas precisam ser verdadeiras e comprováveis. Um modelo que inventa benefício de produto não transfere a responsabilidade para a ferramenta. A empresa deve revisar material antes da publicação e controlar fontes de dados utilizadas para gerar campanhas.

Personalização algorítmica pode melhorar relevância, mas também explorar vulnerabilidades. Segmentações baseadas em condição financeira, saúde ou comportamento emocional exigem cautela adicional e podem envolver dados sensíveis. Para crianças e adolescentes, o ECA Digital proíbe técnicas de perfilamento para direcionamento de publicidade comercial e também veda o emprego de análise emocional, realidade aumentada, estendida e virtual para esse fim.

Deepfakes e representações sintéticas criam risco de fraude, violação de imagem e engano. Mesmo antes de eventual marco geral de IA, direitos da personalidade, CDC, propriedade intelectual e normas penais podem ser aplicáveis. Empresas devem exigir autorização para uso de imagem, voz e identidade e manter registro da origem de ativos sintéticos utilizados em campanha.

O processo de marketing deveria conter um checkpoint jurídico para conteúdos gerados ou modificados de modo substancial por IA quando envolvem pessoas, depoimentos, comparações, promessas de desempenho ou público vulnerável.

9.3 Precificação, recomendação e discriminação

Preços personalizados podem utilizar demanda, horário, localização, histórico e outros sinais. Nem toda variação é ilícita, mas critérios opacos podem gerar problemas de informação, discriminação ou abuso. O jurídico deve entender quais variáveis influenciam a oferta e se consumidores em situações equivalentes recebem tratamento significativamente diferente por fatores sem justificativa legítima.

Sistemas de recomendação também moldam escolhas. Em marketplaces e plataformas, a ordem de apresentação pode favorecer produtos próprios, patrocinados ou mais rentáveis. Transparência comercial e regras concorrenciais podem ser relevantes. A empresa deve diferenciar recomendação baseada em relevância de publicidade paga ou prioridade contratual.

Quando algoritmos detectam vulnerabilidade ou propensão individual, surgem questões éticas e jurídicas sobre exploração. Uma boa prática é limitar uso de

atributos sensíveis e estabelecer proibições internas de personalização que tenha como objetivo induzir comportamento prejudicial.

A pergunta empresarial não é apenas “o modelo aumenta conversão?”, mas “por que aumenta?”. Otimização cega de métricas pode premiar estratégias que seriam rejeitadas se descritas de forma explícita.

Capítulo 10 — Direitos autorais, software e conteúdo gerado por IA

10.1 Autoria e proteção do resultado

A Lei 9.610/1998 estrutura a proteção autoral brasileira a partir da criação intelectual humana. A discussão sobre obras produzidas com auxílio de IA exige separar ferramenta e criação. Quando a contribuição humana envolve escolhas criativas relevantes — seleção, organização, edição, combinação, direção e transformação — pode existir proteção sobre os elementos humanos, ainda que a máquina participe do processo. Conteúdo gerado de forma essencialmente autônoma traz maior incerteza quanto à autoria protegida.

Para empresas, a questão prática não é apenas “há copyright?”, mas “que direitos conseguimos explorar com segurança?”. Termos de fornecedores podem conceder ao usuário direitos sobre outputs, mas não garantem que o resultado seja exclusivo ou não infrinja direitos de terceiros. Modelos podem gerar conteúdos semelhantes para vários usuários.

Em branding, publicidade e produtos criativos, a empresa deve evitar depender de exclusividade sobre um ativo gerado automaticamente sem contribuição humana

significativa. Quando exclusividade é importante, convém incorporar trabalho humano documentado e realizar busca de conflitos conforme o tipo de ativo.

A política interna também deve esclarecer quem detém direitos sobre prompts, templates, fine-tunings, bases curadas e materiais produzidos por empregados. Contratos de trabalho e prestação de serviços devem ser coerentes com a estratégia de propriedade intelectual.

10.2 Treinamento com obras protegidas

O uso de obras protegidas no treinamento de modelos é uma das áreas mais debatidas. A legislação brasileira vigente não contém uma exceção geral e específica de text and data mining equivalente a alguns regimes estrangeiros. A análise depende da forma de acesso, reprodução, finalidade, licença, exceções existentes e circunstâncias do caso.

O texto aprovado pelo Senado no PL 2.338/2023 propôs regras específicas para conteúdos protegidos, mas, em agosto de 2026, o projeto ainda estava em análise na Câmara e pode ser alterado. Portanto, empresas não devem tratar essas regras como direito vigente.

Para projetos próprios, a abordagem conservadora é construir base documental de licenças e permissões. Obras em domínio público, materiais licenciados de forma compatível e conteúdo próprio reduzem risco. Quando grandes volumes de conteúdo de terceiros são essenciais, a estratégia jurídica deve ser definida antes do treinamento, e não depois da comercialização.

A rastreabilidade da fonte também permite responder a pedidos de titulares, negociar remuneração e investigar

outputs potencialmente infratores. Governança de dados e propriedade intelectual convergem nesse ponto.

10.3 Código-fonte gerado por IA e licenças

Assistentes de programação podem aumentar produtividade, mas introduzem questões de segurança e licenciamento. Trechos sugeridos podem se aproximar de código existente, e o desenvolvedor pode incorporar dependências sem perceber obrigações de licença. Por isso, código gerado deve passar pelos mesmos controles de revisão, testes e análise de composição de software aplicáveis ao código humano.

A empresa deve definir se repositórios confidenciais podem ser enviados ao fornecedor. Em ambientes regulados ou projetos estratégicos, pode ser necessário utilizar configuração empresarial que impeça treinamento com o conteúdo. Secrets, credenciais e chaves nunca devem ser compartilhados com modelos externos sem arquitetura especificamente desenhada para isso.

Ferramentas de Software Composition Analysis continuam relevantes. IA não elimina a necessidade de verificar bibliotecas, licenças e vulnerabilidades. O fato de um trecho ter sido “sugerido” por modelo não muda o risco operacional de introduzir uma dependência insegura.

No contrato com desenvolvedores e fornecedores, convém incluir declaração sobre uso de ferramentas generativas, dever de respeitar licenças, proteção de segredos e responsabilidade por revisão. O objetivo não é proibir inovação, mas preservar rastreabilidade.

Capítulo 11 — Contratos de inteligência artificial

11.1 O contrato deve refletir a arquitetura

Contratos de IA falham quando são escritos como contratos genéricos de SaaS. A primeira etapa da negociação deveria ser um diagrama simples do fluxo: que dados saem da empresa, quais componentes os recebem, onde são armazenados, quais suboperadores participam, que saída retorna e quem toma a decisão final. A partir desse desenho, cláusulas jurídicas ganham significado.

Escopo precisa identificar o caso de uso autorizado. Um mesmo modelo pode ser adequado para apoio interno e inadequado para decisões sobre pessoas. Limitar finalidade protege as partes e evita expansão silenciosa. Mudanças materiais de finalidade, modelo ou processamento devem acionar dever de notificação e, quando pertinente, nova avaliação.

O contrato deve distinguir dados do cliente, prompts, outputs, dados de telemetria, feedback e dados derivados. Cada categoria pode ter propriedade, licença e retenção diferentes. Termos amplos que concedem ao fornecedor licença perpétua sobre “conteúdo” precisam ser avaliados à luz de confidencialidade e proteção de dados.

Também é importante definir a hierarquia documental. Termos online podem mudar unilateralmente; contrato empresarial deve indicar quais documentos prevalecem e como atualizações serão comunicadas.

11.2 Cláusulas técnicas mínimas

Sistemas relevantes devem possuir compromissos sobre segurança, incidentes, disponibilidade, continuidade e suporte. Em IA, também são úteis cláusulas sobre versão do modelo, mudanças materiais, avaliação de desempenho, limites conhecidos e documentação técnica disponível.

Se a saída alimenta processo crítico, a empresa pode exigir direito de testar antes de atualizações significativas ou período de transição. APIs que trocam automaticamente de modelo podem produzir regressões. O fornecedor deve comunicar alterações capazes de afetar segurança, conformidade ou funcionalidade.

Logs e evidências precisam ser negociados. Após uma disputa, a empresa pode precisar reconstruir prompt, resposta, versão, horário e regra aplicada. O contrato deve garantir acesso compatível com retenção e privacidade.

Auditoria não significa necessariamente acesso irrestrito ao código. Pode incluir relatórios independentes, certificações, respostas a questionários, evidências de testes e auditoria direcionada em caso de incidente. O nível deve ser proporcional ao risco e ao poder de negociação.

11.3 Indenização, limites e seguro

Cláusulas de indenização devem separar categorias de risco: violação de propriedade intelectual, incidente de dados, descumprimento de confidencialidade, falha de segurança, uso fora do escopo e violação regulatória. Uma única cláusula genérica tende a produzir ambiguidade.

O limite de responsabilidade precisa ser comparado à exposição provável. Para uso de baixo risco, limite padrão

pode ser suficiente. Para sistema que processa dados sensíveis ou afeta milhares de clientes, o teto precisa ser analisado com mais rigor. Exclusões de danos indiretos também merecem atenção porque determinados prejuízos tecnológicos podem ser classificados contratualmente dessa forma.

Seguro cibernético e de responsabilidade tecnológica pode complementar, mas não substituir controles. A empresa deve verificar exclusões relacionadas a IA, privacidade e propriedade intelectual. Novos produtos securitários ainda estão amadurecendo e a cobertura deve ser lida de forma concreta.

A melhor alocação contratual é aquela alinhada ao controle. Quem escolhe dados responde por deveres relacionados a essa escolha; quem controla infraestrutura responde por sua segurança; quem define decisão empresarial assume deveres correspondentes. A redação deve seguir a realidade operacional.

Parte IV — Pessoas, segurança e direitos fundamentais

Capítulo 12 — Inteligência artificial nas relações de trabalho

12.1 Recrutamento e seleção

Sistemas de IA podem ordenar currículos, avaliar testes, analisar entrevistas e recomendar candidatos. O risco jurídico aumenta quando atributos aparentemente neutros funcionam como proxies de características

protegidas ou quando dados históricos reproduzem desigualdades. A empresa deve saber quais variáveis entram no modelo e quais candidatos são excluídos automaticamente.

A decisão de contratação afeta interesse relevante e envolve dados pessoais. A LGPD, princípios antidiscriminatórios e legislação trabalhista precisam ser considerados. A empresa deve evitar coleta de informação excessiva e avaliar se determinados sinais — expressão facial, voz, padrões comportamentais — realmente possuem validade para a finalidade pretendida.

Ferramentas que prometem inferir personalidade, emoção ou honestidade a partir de vídeo merecem ceticismo elevado. Além de questões científicas, podem envolver biometria e discriminação. O jurídico deve exigir evidência independente de validade e necessidade antes da contratação.

Candidatos devem ter canal para contestar erro material e, em processos altamente automatizados, mecanismos de revisão adequados. O objetivo não é permitir que cada candidato conheça segredo comercial, mas evitar decisões irreversíveis baseadas em dados incorretos ou inferências frágeis.

12.2 Monitoramento e produtividade

IA permite monitorar teclado, tela, localização, comunicação, tempo de atividade e padrões de desempenho. A facilidade técnica não significa proporcionalidade jurídica. Monitoramento invasivo pode violar privacidade, dignidade e proteção de dados, além de deteriorar relação de trabalho.

A empresa deve definir finalidade específica e escolher o método menos intrusivo. Segurança pode justificar determinados logs, mas não necessariamente vigilância constante de conteúdo. Produtividade pode ser medida por resultados em vez de presença digital contínua. Dados coletados para segurança não devem ser reutilizados automaticamente para avaliação disciplinar sem análise de compatibilidade.

Transparência é essencial. Empregados precisam conhecer tipos de monitoramento, finalidades e consequências relevantes. Políticas escondidas ou genéricas aumentam risco. Em ambientes com representação coletiva, também pode haver dimensão negocial e trabalhista específica.

Sistemas de pontuação devem ser auditados. Métricas mal desenhadas incentivam comportamento artificial e podem prejudicar trabalhadores que executam tarefas complexas não capturadas pelo indicador. Gestão algorítmica não elimina a obrigação humana de compreender contexto.

12.3 Uso de IA pelos empregados

A empresa precisa estabelecer regras para uso de ferramentas generativas por empregados, mas a política deve ser executável. Proibir tudo raramente funciona; liberar tudo aumenta exposição. O melhor caminho é classificar ferramentas e dados, oferecer opções aprovadas e ensinar exemplos reais.

A política deve dizer se IA pode produzir rascunhos de contratos, responder clientes, escrever código, avaliar candidatos, criar apresentações ou manipular dados pessoais. Para cada categoria, deve definir revisão

necessária. Funcionários também precisam saber que são responsáveis por conferir saída antes de uso profissional.

Treinamento deve incluir propriedade intelectual, confidencialidade, alucinações, segurança e proteção de dados. Exercícios práticos são mais eficazes que textos abstratos. Por exemplo: mostrar por que não se deve colar contrato sigiloso em conta pessoal e qual alternativa corporativa deve ser usada.

O programa deve prever reporte de incidentes sem criar medo excessivo. Se um empregado inserir por engano informação sensível em ferramenta não autorizada, a resposta rápida permite avaliar exposição e reduzir dano. Cultura punitiva pode estimular ocultação.

Capítulo 13 — Segurança da informação e ataques contra IA

13.1 Segurança tradicional continua essencial

Sistemas de IA dependem de infraestrutura, identidades, redes, bancos de dados e APIs. Portanto, os controles clássicos continuam fundamentais: autenticação forte, menor privilégio, segregação, criptografia, gestão de vulnerabilidades, backups e monitoramento. A novidade é que modelos e pipelines adicionam novas superfícies.

Dados de treinamento podem ser adulterados; prompts podem induzir comportamento indevido; modelos podem vaziar informações; integrações podem executar ações com privilégios excessivos. A empresa deve incluir componentes de IA no processo de threat modeling e não tratá-los como caixa-preta externa.

A LGPD exige medidas técnicas e administrativas aptas a proteger dados pessoais. A Resolução CD/ANPD 15/2024 disciplina comunicação de incidentes de segurança que possam ocasionar risco ou dano relevante e prevê registro dos incidentes. Em sistemas de IA, o plano de resposta deve conseguir identificar se prompts, logs, embeddings ou datasets foram expostos.

Segurança também deve entrar na aquisição. O fornecedor precisa explicar criptografia, isolamento de clientes, retenção, controles de acesso, suboperadores, resposta a incidentes e testes independentes. Certificações ajudam, mas não substituem análise do caso de uso.

13.2 Prompt injection e uso de ferramentas

Prompt injection ocorre quando instruções maliciosas inseridas na entrada tentam alterar o comportamento do modelo. O risco é maior em agentes capazes de acessar e-mail, arquivos, bancos de dados ou executar ações. Um texto externo pode conter instruções projetadas para induzir o agente a revelar dados ou realizar operação indevida.

A defesa não pode depender apenas de dizer ao modelo “ignore instruções maliciosas”. Sistemas críticos devem restringir ferramentas, validar parâmetros, aplicar allowlists, exigir confirmação para ações sensíveis e separar dados não confiáveis de instruções privilegiadas. O princípio do menor privilégio deve ser aplicado ao agente como seria aplicado a um usuário ou serviço.

Do ponto de vista jurídico, autonomia aumenta dever de controle. Se um agente pode contratar, pagar, alterar registros ou enviar comunicações externas, a empresa

deve definir limites claros e trilhas de auditoria. Ações de alto impacto podem exigir aprovação humana obrigatória.

Teste de segurança deve incluir entradas adversariais. Avaliar apenas prompts normais não revela comportamento sob ataque. Red teaming controlado pode identificar caminhos de vazamento e abuso antes da produção.

13.3 Incidentes e comunicação

Um incidente de IA deve ser classificado conforme seu efeito: confidencialidade, integridade, disponibilidade, violação de direitos, fraude, conteúdo indevido ou decisão incorreta em massa. Nem todo erro de modelo é incidente de segurança, mas alguns erros podem revelar comprometimento de dados ou manipulação externa.

O playbook precisa registrar quem decide interromper o modelo, como preservar evidências, como acionar fornecedor e como avaliar necessidade de comunicação à ANPD e titulares. A Resolução 15/2024 estabelece critérios e prazos específicos; por isso, o contrato com fornecedores precisa assegurar comunicação rápida, não apenas dentro de prazos comerciais longos.

Também é necessário distinguir incidente do fornecedor e incidente do cliente. Se uma API externa sofre exposição, a empresa deve compreender quais dados próprios estavam presentes. Inventário e logs tornam essa avaliação possível.

Após o evento, a organização deve realizar análise de causa raiz e revisão de controles. Em IA, isso pode envolver atualização de prompt de sistema, filtro, dataset, modelo, regra de negócio ou procedimento humano. A correção deve atingir a causa, não apenas o sintoma.

Capítulo 14 — Discriminação algorítmica e direitos fundamentais

14.1 Viés não é uma única coisa

“Viés” pode significar erro estatístico, distorção de amostragem, preconceito social ou diferença de desempenho entre grupos. Misturar conceitos dificulta a análise. O jurídico deve perguntar que diferença foi observada, qual grupo é afetado, qual consequência ocorre e se existe justificativa legítima.

Dados históricos refletem decisões humanas e estruturas sociais. Um modelo treinado para reproduzir “quem foi contratado no passado” pode aprender critérios que perpetuam padrões anteriores. Remover atributos protegidos não garante neutralidade porque proxies permanecem.

A análise deve ocorrer antes e depois da implantação. Antes, examina-se representatividade, variáveis, objetivo e métricas. Depois, monitora-se resultado real, porque o comportamento em produção pode diferir do teste. Grupos pequenos ou pouco representados merecem atenção especial.

Governança antidiscriminatória não exige que advogados programem modelos, mas exige colaboração com ciência de dados. O jurídico define quais impactos são relevantes e quais diferenças demandam investigação; a equipe técnica mede e testa alternativas.

14.2 Métricas de equidade e escolhas normativas

Existem várias métricas de fairness e elas podem ser incompatíveis entre si. Igualar taxa de aprovação, taxa de erro ou valor preditivo produz resultados diferentes. A

escolha não é puramente matemática; depende da finalidade e do tipo de dano que se deseja evitar.

Em prevenção de fraude, por exemplo, falso positivo pode bloquear usuário legítimo; falso negativo permite fraude. A empresa precisa decidir qual erro é mais grave e como distribuí-lo. Se um grupo recebe falsos positivos muito superiores, a consequência jurídica pode ser relevante mesmo que a acurácia global seja alta.

A documentação deve registrar por que determinada métrica foi escolhida e que alternativas foram avaliadas. Isso demonstra que a organização reconheceu trade-offs em vez de esconder decisões normativas dentro da tecnologia.

Também é importante evitar “fairness washing”: publicar declaração genérica de ética sem medir resultados. Evidência objetiva é mais valiosa do que promessa de neutralidade.

14.3 Contestação e remediação

Quando um sistema produz decisão adversa, a pessoa afetada deve ter caminho proporcional para contestar. O mecanismo precisa permitir corrigir dados, apresentar informação contextual e receber resposta. Em ambientes de alto volume, automação pode ajudar a organizar pedidos, mas a revisão não pode ser totalmente circular — outro algoritmo apenas reafirmando o primeiro sem análise adequada.

Remediação também inclui revisar decisões anteriores quando falha sistêmica é descoberta. Se um modelo foi configurado incorretamente por meses, corrigir apenas resultados futuros pode ser insuficiente. A empresa deve avaliar universo afetado e possibilidade de reparação.

Métricas de reclamação são sinais de risco. Aumento de contestações, reversões frequentes ou concentração em determinado grupo pode indicar problema do modelo. O jurídico deve receber esses indicadores em dashboards de governança.

A capacidade de suspender um sistema é parte da responsabilidade. Organizações que não definem kill switch, autoridade de interrupção e plano alternativo podem manter processo defeituoso por inércia operacional.

Capítulo 15 — Crianças, adolescentes e o ECA Digital

15.1 A mudança regulatória de 2026

A Lei 15.211/2025 criou o Estatuto Digital da Criança e do Adolescente e entrou em vigor em 17 de março de 2026. Trata-se de uma das mudanças mais relevantes do ambiente regulatório digital brasileiro recente. A norma alcança produtos e serviços de tecnologia da informação direcionados a crianças e adolescentes no País ou de acesso provável por eles, independentemente do local de desenvolvimento, oferta ou operação.

O conceito de acesso provável impede uma leitura baseada apenas na classificação comercial do produto. A organização deve considerar probabilidade de uso, atratividade, facilidade de acesso e grau de risco à privacidade, segurança ou desenvolvimento. Plataformas generalistas, jogos, redes sociais, aplicativos de conteúdo e serviços com assistentes generativos precisam realizar análise documentada.

O Decreto 12.880/2026 regulamentou a lei e atribuiu à ANPD competências de regulamentação e fiscalização, consolidando a convergência entre proteção de dados e proteção de menores no ambiente digital. Para empresas, isso significa que governança de IA direcionada a menores não pode ficar separada de privacy by design e safety by design.

A avaliação deve ocorrer desde a concepção. Configurações-padrão, publicidade, recomendação, mecanismos de contato, conteúdo gerado, coleta de dados e aferição de idade precisam ser avaliados como conjunto. A proteção não é uma tela de consentimento adicionada ao final do projeto.

15.2 Perfilamento, publicidade e design

O ECA Digital contém regras específicas para publicidade. É vedada a utilização de técnicas de perfilamento para direcionamento de publicidade comercial a crianças e adolescentes, assim como o emprego de análise emocional, realidade aumentada, estendida e virtual para esse objetivo. Para sistemas de recomendação e IA generativa, essas proibições devem ser incorporadas às regras de produto.

A empresa precisa distinguir personalização funcional de publicidade comportamental. Recomendar conteúdo educacional com base no progresso pode ter finalidade diferente de explorar perfil para venda. A documentação de finalidade e arquitetura de anúncios é essencial.

Dark patterns também merecem atenção. Interfaces não devem induzir menores a compartilhar mais dados, permanecer conectados de forma compulsiva ou realizar compra por mecanismos manipulativos. Modelos de IA

que otimizam engajamento podem amplificar tais padrões se a função objetivo não incluir limites de segurança.

Quando a plataforma utiliza influenciadores virtuais, avatares ou personagens gerados por IA, deve avaliar se a apresentação explora confiança infantil ou disfarça publicidade. Transparência precisa ser adaptada à capacidade de compreensão do público.

15.3 Aferição de idade e minimização

Aferir idade cria um paradoxo: para proteger crianças, a plataforma pode acabar coletando mais dados de todos os usuários. A solução deve observar proporcionalidade. Nem todo serviço precisa exigir documento de identidade; diferentes níveis de risco podem justificar mecanismos distintos.

A ANPD tem produzido estudos técnicos sobre mecanismos de aferição de idade e a matéria está inserida no contexto de suas novas atribuições. A empresa deve avaliar precisão, possibilidade de erro, vieses, retenção e segurança da técnica escolhida.

Biometria para estimativa de idade pode aumentar risco e deve ser tratada com cautela. Quando possível, a arquitetura deve separar a confirmação de faixa etária da identidade civil completa. O serviço muitas vezes precisa saber que o usuário está acima de determinado limite, e não necessariamente conhecer sua data de nascimento ou documento.

A governança deve registrar por que determinado mecanismo foi escolhido, que alternativas menos intrusivas foram consideradas e como usuários podem contestar classificação incorreta.

Parte V — Mercado, setores regulados e poder público

Capítulo 16 — Concorrência, plataformas e poder econômico

16.1 Dados, modelos e barreiras à entrada

Sistemas de IA podem ampliar vantagens de empresas que já possuem dados, infraestrutura, distribuição e capital computacional. A Lei 12.529/2011 continua sendo o marco brasileiro de defesa da concorrência e pode incidir quando práticas envolvendo IA produzem abuso de posição dominante, discriminação anticompetitiva, acordos ou fechamento de mercado.

O simples fato de uma empresa possuir modelo superior não é ilícito. A análise concorrencial observa conduta e efeitos. Questões podem surgir quando acesso essencial a dados ou infraestrutura é condicionado de forma abusiva, quando plataformas favorecem produtos próprios ou quando contratos impedem migração e interoperabilidade sem justificativa.

Vendor lock-in é simultaneamente risco comercial e de governança. Se uma organização depende de um único provedor de modelo, pode perder poder de negociação e capacidade de responder a mudanças regulatórias. Arquiteturas com camadas de abstração, exportação de dados e padrões abertos podem reduzir dependência.

Para empresas que fornecem IA, práticas de exclusividade e descontos precisam ser analisadas no contexto de participação de mercado e efeito competitivo.

O jurídico concorrencial deve participar quando a estratégia passa de produto para ecossistema.

16.2 Precificação algorítmica e coordenação

Algoritmos de precificação podem reagir rapidamente ao mercado. O risco concorrencial surge quando sistemas facilitam coordenação entre concorrentes, utilizam sinais comuns para estabilizar preços ou implementam acordo anticompetitivo. Automação não torna lícita uma conduta que seria ilícita se executada manualmente.

Empresas devem evitar troca indevida de informações competitivamente sensíveis por meio de fornecedores comuns. Se uma plataforma de otimização utiliza dados de vários concorrentes, governança de segregação é fundamental. O contrato deve esclarecer que dados de um cliente não serão utilizados para recomendar estratégia baseada em informações confidenciais de outro.

Modelos também podem aprender padrões de resposta de mercado sem acordo explícito. A análise jurídica de cenários autônomos é mais complexa, mas a organização deve monitorar comportamentos anômalos e manter limites de negócio.

A regra prática é não permitir que “o algoritmo decidiu” substitua política concorrencial. Parâmetros, fontes de dados e objetivos de otimização continuam sujeitos a supervisão.

16.3 Ecossistemas de IA e interoperabilidade

Empresas que controlam infraestrutura, marketplace, modelo e distribuição podem criar integrações eficientes e também conflitos de interesse. Interoperabilidade,

portabilidade e acesso a APIs tornam-se temas estratégicos.

Para clientes empresariais, contratos devem prever exportação de prompts, configurações, bases vetoriais e metadados necessários à migração quando tecnicamente possível. A ausência de portabilidade pode transformar uma decisão de curto prazo em dependência de longo prazo.

Em aquisições e parcerias, a due diligence concorrencial deve considerar não apenas participação atual, mas acesso a dados e capacidade de controlar gargalos futuros. IA pode deslocar poder econômico rapidamente.

O Direito da IA, nesse ponto, encontra o Direito Concorrencial: governança não protege apenas indivíduos; também preserva mercados contestáveis e inovação distribuída.

Capítulo 17 — IA em setores regulados

17.1 Serviços financeiros e crédito

Instituições financeiras já operam sob intenso regime de governança, risco operacional, segurança e proteção do consumidor. IA utilizada em crédito, fraude, atendimento ou investimentos precisa ser integrada aos controles existentes. O erro de tratar IA como projeto experimental paralelo pode gerar lacunas de responsabilidade.

Em crédito, a LGPD menciona expressamente decisões destinadas a definir perfil de crédito no contexto do art. 20. Modelos devem ter qualidade de dados, critérios documentados e mecanismos de correção. Variáveis

alternativas podem ampliar inclusão, mas também introduzir proxies e opacidade.

Prevenção de fraude exige equilíbrio. Sistemas muito agressivos bloqueiam clientes legítimos; sistemas permissivos aumentam perdas. Métricas de falso positivo e falso negativo precisam ser acompanhadas e segmentadas. Canais de desbloqueio devem ser rápidos quando o impacto sobre o consumidor é alto.

Empresas fornecedoras de IA a bancos precisam estar preparadas para auditorias, requisitos de continuidade, segurança e subcontratação mais rigorosos. O contrato deve refletir exigências do setor e não apenas práticas gerais de SaaS.

17.2 Saúde e seguros

IA em saúde pode apoiar triagem, imagem, documentação clínica, pesquisa e gestão. O grau de risco depende da função. Ferramenta que resume prontuário não é equivalente a sistema que recomenda diagnóstico ou dose. Dados de saúde são sensíveis e exigem regime reforçado da LGPD.

Validação clínica e supervisão profissional são centrais. Métrica estatística global não garante desempenho para todos os grupos ou hospitais. Mudança de população pode degradar resultado. Sistemas devem ser testados no contexto de uso e monitorados após implantação.

Em seguros, modelos podem influenciar subscrição, preço e investigação de sinistros. Critérios precisam ser consistentes com legislação setorial, proteção de dados e não discriminação. Inferências de saúde a partir de comportamento digital merecem cautela elevada.

Fornecedores devem evitar afirmações de desempenho que ultrapassem evidência. Em setores regulados, marketing técnico impreciso pode criar responsabilidade além da própria tecnologia.

17.3 Educação e avaliação

IA educacional pode personalizar conteúdo, corrigir atividades, detectar dificuldades e apoiar professores. Quando influencia avaliação, admissão ou progressão, a exigência de transparência e revisão aumenta. Crianças e adolescentes adicionam as obrigações do ECA Digital e regras específicas de proteção de dados.

Sistemas de detecção de texto gerado por IA merecem cuidado porque apresentam falsos positivos. Punir estudante apenas com base em detector probabilístico pode gerar injustiça. A ferramenta deve ser indício, não prova automática, salvo quando houver validação muito robusta e procedimento de contestação.

Plataformas educacionais precisam avaliar coleta de comportamento, publicidade e compartilhamento com terceiros. Dados escolares não devem virar insumo comercial sem análise jurídica compatível com a finalidade original.

A empresa que vende IA para escolas deve fornecer documentação inteligível para instituições, professores e responsáveis, especialmente quando o sistema produz recomendações sobre alunos.

Capítulo 18 — IA no setor público e empresas contratadas pelo Estado

18.1 Legalidade, motivação e controle

A Administração Pública está vinculada a legalidade, impessoalidade, moralidade, publicidade e eficiência. IA pode aumentar eficiência, mas decisões públicas exigem motivação e controle. Sistemas que selecionam beneficiários, fiscalizam, classificam risco ou apoiam sanções devem ser projetados com capacidade de auditoria e contestação.

Para empresas fornecedoras ao Estado, isso implica requisitos que podem superar os de contratos privados. O sistema precisa permitir registros, explicações, gestão de versões e preservação de evidências. Segredo comercial deve ser protegido, mas não pode transformar decisão pública em caixa-preta absoluta.

A LGPD possui regras específicas para tratamento pelo poder público. Fornecedores devem compreender se atuam como operadores e quais instruções recebem. Uso posterior de dados públicos para fins próprios precisa ser cuidadosamente limitado.

O princípio de impessoalidade também exige vigilância sobre discriminação. Modelos treinados em dados históricos de fiscalização ou concessão podem reproduzir padrões seletivos e afetar grupos de maneira desigual.

18.2 Contratações públicas de IA

A Lei 14.133/2021 disciplina licitações e contratos administrativos. Na aquisição de IA, o desafio é traduzir desempenho em critérios verificáveis. Editais que exigem

apenas “solução com inteligência artificial” favorecem marketing e dificultam comparação.

Requisitos deveriam descrever finalidade, métricas mínimas, segurança, interoperabilidade, propriedade de dados, documentação, atualização, suporte e testes. Em casos de alto impacto, provas de conceito controladas podem reduzir risco antes da implantação completa.

A Administração deve evitar dependência excessiva de fornecedor. Portabilidade, padrões de integração e acesso a documentação são relevantes. O contrato também precisa definir o que ocorre com dados e modelos ao término da relação.

Empresas participantes devem preparar evidências objetivas e não apenas apresentações comerciais. Certificações, relatórios de teste, matriz de responsabilidades e plano de segurança fortalecem propostas e reduzem disputas futuras.

18.3 Transparência pública e segredo comercial

Contratos públicos podem exigir transparência, enquanto fornecedores possuem propriedade intelectual e segredos. O equilíbrio deve ser planejado desde o início. Separar documentação pública de documentação confidencial evita conflitos posteriores.

A explicação de uma decisão não precisa revelar pesos completos do modelo. É possível fornecer fatores relevantes, regras de processo, dados utilizados e mecanismos de revisão preservando elementos proprietários. A empresa deve preparar esse nível de explicação antes da implantação.

Auditorias independentes podem funcionar como ponte. Um terceiro avalia o sistema sob confidencialidade

e publica conclusões compatíveis com transparência. O contrato deve prever acesso suficiente para esse tipo de verificação.

No setor público, legitimidade é parte do desempenho. Um sistema estatisticamente eficiente, mas impossível de explicar ou contestar, pode ser inadequado para determinadas funções estatais.

Parte VI — Governança empresarial e preparação regulatória

Capítulo 19 — Programa corporativo de governança de IA

19.1 Estrutura de responsabilidades

Governança de IA não deve ser delegada a um único “comitê de ética”. Ela precisa conectar primeira linha de negócio, funções de risco e auditoria. A área de negócio é dona da finalidade e do resultado; tecnologia administra componentes; segurança protege infraestrutura; privacidade avalia dados; jurídico interpreta regimes; compliance monitora obrigações; auditoria verifica funcionamento independente.

Um Comitê de IA pode decidir casos de maior risco, aprovar políticas e resolver conflitos. Não precisa analisar cada uso trivial. A organização deve definir alçadas. Casos de baixo risco seguem procedimento simplificado; casos de alto impacto exigem revisão multidisciplinar.

O RACI — Responsible, Accountable, Consulted, Informed — é ferramenta útil. Para cada etapa do ciclo de

vida, deve haver quem executa e quem responde. A ausência de accountable é sinal de projeto órfão.

A governança deve possuir orçamento e autoridade. Comitê sem capacidade de suspender implantação ou exigir correção vira estrutura simbólica. O patrocínio executivo é necessário porque alguns controles reduzem velocidade de lançamento em troca de menor risco.

19.2 Política de uso responsável

Uma política corporativa deve ser curta o suficiente para ser lida e detalhada o suficiente para orientar. Pode conter princípios, escopo, categorias de uso, dados proibidos, ferramentas aprovadas, revisão humana, compras, desenvolvimento, segurança, registro e sanções.

A política deve distinguir uso interno de desenvolvimento para clientes. Um funcionário que usa IA para revisar texto apresenta risco diferente de uma empresa que incorpora modelo em produto. Controles precisam refletir essas diferenças.

Exemplos são essenciais. “Não inserir informação confidencial” precisa vir acompanhado de exemplos de contrato, código, folha de pagamento, credencial e documento de cliente. Também deve informar o canal seguro disponível.

A política deve ser revisada periodicamente. Modelos, fornecedores e legislação mudam rapidamente. Atualização anual pode ser insuficiente em organizações intensivas em IA; um ciclo semestral ou gatilhos de mudança podem ser mais adequados.

19.3 Inventário e classificação por risco

O inventário é o coração operacional do programa. Sem saber onde IA está sendo usada, a empresa não consegue cumprir direitos, responder incidentes ou realizar auditoria. O inventário deve integrar processos de compras, arquitetura e segurança para evitar dependência de autodeclaração.

A classificação por risco pode utilizar fatores: impacto sobre direitos, sensibilidade dos dados, escala, autonomia, vulnerabilidade do público, reversibilidade, criticidade do serviço e exposição externa. Pontuação numérica pode ajudar, mas não deve substituir julgamento.

Cada nível precisa ter controles associados. Baixo risco: registro e revisão do responsável. Médio: avaliação de privacidade e segurança, testes e aprovação gerencial. Alto: avaliação de impacto, comitê, testes independentes, monitoramento reforçado e revisão periódica.

O modelo de classificação deve ser simples e explicável. Se apenas especialistas conseguem utilizá-lo, áreas de negócio irão contorná-lo. Governança precisa competir com a velocidade da tecnologia.

Capítulo 20 — Auditoria, evidências e o futuro marco brasileiro

20.1 Auditabilidade e documentação

Auditar IA não significa apenas verificar código. O auditor precisa examinar finalidade, dados, métricas, mudanças, acesso, incidentes, reclamações e decisões. Uma organização madura consegue produzir pacote de evidências por sistema.

Esse pacote pode conter ficha do caso de uso, avaliação de risco, registro de aprovação, contrato, relatório de proteção de dados, testes, model card ou documento equivalente, logs relevantes, histórico de versões, incidentes e revisões. A documentação deve ser proporcional ao risco.

Evidência precisa ser contemporânea. Criar documentos retroativamente após incidente reduz credibilidade. O programa deve incorporar geração de registros ao processo normal de implantação.

Auditoria interna deve selecionar amostras e verificar se controles descritos realmente funcionam. É comum encontrar política que exige revisão humana, mas interface que não permite rejeitar recomendação; ou contrato que promete exclusão enquanto arquitetura mantém backups indefinidos.

20.2 O PL 2.338/2023 como horizonte regulatório

O PL 2.338/2023 foi aprovado pelo Senado em dezembro de 2024 e remetido à Câmara em março de 2025. Em agosto de 2026, permanecia em análise por Comissão Especial, com o deputado Aguinaldo Ribeiro como relator e diversos projetos apensados. Portanto, nenhuma empresa deve apresentar suas disposições como lei vigente.

Ainda assim, o texto aprovado pelo Senado é relevante porque sinaliza temas que provavelmente continuarão no debate: abordagem baseada em risco, direitos de pessoas afetadas, obrigações para determinados sistemas, governança, supervisão e regras relacionadas a IA generativa e propriedade intelectual. A Câmara pode modificar substancialmente esses pontos.

Para empresas, a estratégia racional é investir em controles “sem arrependimento”: inventário, avaliação de risco, documentação, proteção de dados, supervisão humana, segurança, transparência e gestão de fornecedores. Esses mecanismos já reduzem risco sob o direito vigente e facilitam adaptação a futura lei.

A organização deve evitar construir programa baseado em numeração de artigos de um projeto. É melhor criar capacidades. Se o texto final alterar categorias ou autoridade, capacidades de inventário e avaliação continuam úteis.

20.3 Preparação para fiscalização e litígio

Um regulador, juiz ou cliente institucional tende a fazer perguntas semelhantes: por que esse sistema foi usado, que risco era conhecido, que dados foram tratados, como foi testado, quem poderia interromper, como o usuário contesta e o que aconteceu após falha. A empresa deve conseguir responder com documentos e evidências.

Preparação para fiscalização não significa adotar postura defensiva em todos os projetos. Significa tornar decisões rastreáveis. Uma ata curta justificando escolha pode valer mais que política de cinquenta páginas sem conexão com o sistema.

Simulações ajudam. A equipe pode escolher um sistema e encenar pedido de titular, incidente, reclamação de discriminação ou auditoria de cliente. O exercício revela lacunas de logs, responsáveis e contratos.

O Direito da Inteligência Artificial será cada vez menos uma discussão sobre princípios abstratos e mais uma disciplina de governança demonstrável. Empresas

que aprendem a provar o funcionamento de seus controles estarão melhor posicionadas para inovar com segurança.

Parte VII — Manual de implementação empresarial

Capítulo 21 — Implantação em 90 dias

21.1 Dias 1 a 30: descobrir e classificar

O primeiro mês deve priorizar visibilidade. Nomeie um patrocinador executivo e um responsável operacional. Publique orientação provisória sobre ferramentas generativas e estabeleça canal para registro. Faça inventário inicial perguntando a compras, tecnologia, segurança, jurídico, marketing, RH, atendimento e áreas de produto.

Não tente alcançar perfeição. O objetivo é localizar usos de maior impacto. Crie formulário curto com finalidade, ferramenta, dados, pessoas afetadas, decisão e responsável. Classifique preliminarmente em baixo, médio e alto risco.

Paralelamente, identifique contratos existentes com recursos de IA. Verifique termos de treinamento, retenção, suboperadores e transferência internacional. Ferramentas que recebem dados sensíveis ou confidenciais devem ser priorizadas.

Ao final dos 30 dias, a empresa deve possuir lista razoável de casos de uso, política provisória e top 10 riscos. Esse resultado é mais valioso que tentar escrever framework perfeito antes de conhecer a realidade.

21.2 Dias 31 a 60: criar controles

No segundo mês, formalize política, matriz de risco e processo de aprovação. Defina que eventos exigem revisão de privacidade, segurança, jurídico e comitê. Crie modelos de avaliação de impacto e due diligence de fornecedor.

Selecione dois ou três sistemas relevantes para pilotos de documentação completa. Produza ficha, fluxo de dados, análise de base legal, testes, plano de monitoramento e matriz de responsabilidade. Use esses pilotos para ajustar formulários.

Treine equipes com exemplos concretos. Desenvolvedores precisam entender dados e licenças; RH precisa entender decisões automatizadas; marketing precisa entender conteúdo sintético; compras precisa entender cláusulas mínimas.

Configure controles técnicos nas ferramentas aprovadas: autenticação, contas corporativas, retenção, desativação de treinamento quando disponível e gestão de acesso. Governança sem configuração técnica fica vulnerável.

21.3 Dias 61 a 90: monitorar e provar

No terceiro mês, defina indicadores. Quantos sistemas foram inventariados? Quantos são de alto risco? Quantos fornecedores foram avaliados? Quantos incidentes ou reclamações ocorreram? Qual a taxa de revisão humana e reversão em decisões automatizadas?

Execute uma auditoria interna curta em um sistema. Verifique se o que está escrito corresponde ao que ocorre. Teste pedido de exclusão, exportação de logs e interrupção. Corrija lacunas.

Apresente ao conselho ou diretoria um dashboard com riscos, ações e decisões pendentes. A governança precisa chegar à liderança em linguagem de negócio: impacto financeiro, reputacional, regulatório e operacional.

Depois de 90 dias, o programa entra em ciclo contínuo. Novos casos são registrados, sistemas mudam, fornecedores atualizam modelos e legislação evolui. O objetivo não é “concluir compliance”, mas manter capacidade de adaptação.

Capítulo 22 — Métricas e indicadores de governança

22.1 Métricas de processo

Métricas de processo indicam se o programa está sendo utilizado. Exemplos: percentual de sistemas inventariados com responsável, percentual de casos de alto risco com avaliação aprovada, tempo médio de análise, cobertura de treinamento e fornecedores com cláusulas mínimas.

Essas métricas são fáceis de medir, mas não provam que o sistema é seguro. Uma empresa pode ter 100% dos formulários preenchidos e ainda produzir decisões injustas. Por isso, precisam ser combinadas com indicadores de resultado.

Tempo de aprovação merece equilíbrio. Processo excessivamente lento incentiva shadow AI. O jurídico deve medir gargalos e simplificar casos de baixo risco. Governança eficiente é proporcional.

Também é útil medir exceções. Quantas implantações receberam waiver? Quem aprovou? Por quanto tempo? Exceção sem data de expiração tende a virar regra permanente.

22.2 Métricas de resultado

Indicadores de resultado dependem do caso. Em decisões, podem incluir taxa de erro, reversão após contestação, diferenças entre grupos e reclamações. Em modelos generativos, podem incluir taxa de resposta incorreta crítica, vazamento de informação, incidentes de conteúdo e necessidade de correção humana.

O jurídico deve evitar definir métricas técnicas sozinho. A equipe multidisciplinar precisa conectar desempenho a dano jurídico. Um modelo com 95% de acurácia pode ser inaceitável se os 5% de erros envolverem situação grave e concentrada.

Reclamações são dado valioso. Classificar motivos permite identificar padrões. Uma taxa crescente de “não reconheço essa decisão” pode indicar problema de transparência; reversões por dados incorretos apontam falha de qualidade.

Dashboards devem mostrar tendência, não apenas fotografia. Mudança súbita após nova versão pode revelar regressão.

22.3 KRIs e apetite de risco

Key Risk Indicators devem antecipar problema. Exemplos: aumento de prompts contendo dados sensíveis, crescimento de decisões sem revisão, fornecedor sem relatório de segurança atualizado, versões não avaliadas e queda de desempenho para grupo específico.

Apetite de risco transforma princípios em limites. A diretoria pode decidir que determinados usos são proibidos, como decisão disciplinar totalmente automatizada ou envio de dados altamente confidenciais a

modelo público. Outros usos podem exigir aprovação específica.

Limites precisam ser mensuráveis. “Não aceitar viés relevante” é vago; “investigar diferença superior a determinado limiar em métrica definida” é operacional. O limiar deve ser escolhido conforme contexto e revisto.

O programa amadurece quando indicadores influenciam decisão real: suspender modelo, renegociar contrato, aumentar revisão ou alterar dados.

Parte VIII — Riscos especializados e operações avançadas

Capítulo 23 — Biometria, visão computacional e reconhecimento de pessoas

23.1 Biometria é dado sensível, não simples conveniência técnica

A LGPD classifica dado biométrico vinculado a pessoa natural como dado pessoal sensível. Isso altera o nível de cuidado jurídico desde a coleta. Sistemas de reconhecimento facial, voz, impressão digital, íris, padrão de marcha e outras características corporais podem ser extremamente úteis para autenticação e segurança, mas também possuem capacidade elevada de vigilância e de identificação persistente.

A primeira pergunta não deve ser “qual tecnologia tem maior acurácia?”, mas “precisamos realmente identificar biometricamente a pessoa?”. Em controle de acesso a áreas de baixo risco, cartão ou autenticação por

dispositivo pode atingir finalidade com menor intrusão. Em operação de alta segurança, biometria pode ser justificável, desde que a base legal, a necessidade e os controles sejam documentados.

É importante diferenciar verificação e identificação. Na verificação 1:1, o sistema testa se a pessoa corresponde à identidade apresentada. Na identificação 1:N, procura a pessoa em uma base de indivíduos. A segunda modalidade tende a ampliar risco porque envolve comparação em escala e pode produzir falsos positivos com consequências relevantes.

O jurídico deve compreender também o template biométrico. Muitos sistemas não armazenam a imagem original como principal elemento de comparação, mas uma representação matemática. Isso não retira automaticamente a natureza sensível do dado. Se o template está vinculado à pessoa e permite autenticação ou identificação, deve ser tratado de acordo com sua função e risco.

23.2 Reconhecimento facial, acurácia e falsos positivos

Acurácia agregada é insuficiente para avaliar reconhecimento facial. Um sistema pode apresentar desempenho global elevado e ainda assim produzir taxas de erro diferentes por iluminação, idade, qualidade da câmera ou características demográficas. A organização precisa medir o contexto real de implantação.

Falso positivo e falso negativo têm consequências distintas. Em autenticação, falso negativo gera inconveniência; falso positivo pode conceder acesso indevido. Em segurança física ou investigação, falso

positivo pode causar constrangimento ou medida injusta. O limiar de decisão deve refletir o dano potencial, não apenas a métrica que maximiza desempenho médio.

A interface deve mostrar incerteza de forma adequada. Uma similaridade estatística não deve ser apresentada ao operador como certeza de identidade. Quando a consequência é relevante, a saída deve ser tratada como indício sujeito a confirmação por outros elementos.

Empresas que comprem tecnologia biométrica precisam exigir teste em condições locais, documentação de desempenho e processo de atualização. Não é adequado aceitar apenas material promocional baseado em benchmark genérico.

23.3 Bases biométricas e ciclo de vida

Bases biométricas são difíceis de substituir. Senhas podem ser trocadas; rosto e impressão digital não. Por isso, segurança, criptografia, segregação e retenção assumem importância excepcional. A empresa deve limitar acesso e registrar operações administrativas.

A coleta precisa ter prazo e finalidade. Manter template de ex-empregado indefinidamente após encerramento do vínculo pode ser incompatível com necessidade. Processos de offboarding devem incluir eliminação ou anonimização quando aplicável.

Fornecedores que processam biometria em nuvem exigem análise de transferência internacional, suboperadores e incidentes. O contrato deve prever notificação rápida, eliminação e proibição de reutilização para desenvolvimento próprio sem base jurídica adequada.

Em auditoria, a organização deve conseguir demonstrar quantas pessoas estão cadastradas, por que estão, por quanto tempo e qual mecanismo alternativo existe quando a biometria falha ou não pode ser utilizada.

Capítulo 24 — Deepfakes, voz sintética e direitos da personalidade

24.1 Identidade digital como ativo e como direito

Ferramentas de geração de imagem, áudio e vídeo tornam simples reproduzir aparência e voz de pessoas. Para empresas, isso cria oportunidades de localização de conteúdo, avatares, treinamento e marketing, mas também risco de violação de imagem, honra, identidade e direitos autorais conexos.

O Código Civil protege direitos da personalidade, e a utilização econômica de imagem e voz deve ser planejada por autorização clara. Uma autorização tradicional para fotografia em campanha não deve ser presumida como licença irrestrita para criar avatar sintético permanente capaz de gerar novas falas.

Contratos com atores, influenciadores, empregados ou executivos devem especificar se haverá clonagem de voz, criação de modelo de imagem, duração, territórios, mídias, finalidade, possibilidade de gerar falas novas e procedimento de retirada. Quanto mais ampla a capacidade sintética, mais importante a precisão contratual.

Também é preciso proteger a própria organização. Criminosos podem simular voz de diretor, fornecedor ou cliente. Procedimentos financeiros devem exigir validação por canal independente para mudanças de conta,

pagamentos excepcionais e instruções sensíveis. A segurança contra deepfake é problema de processo, não apenas de detector tecnológico.

24.2 Rotulagem e transparência

Nem todo conteúdo sintético precisa do mesmo tipo de rótulo. Uma animação claramente fictícia tem contexto diferente de vídeo que imita declaração real de pessoa. A regra de transparência deve observar probabilidade de engano e consequência.

Em publicidade, atendimento ou treinamento, indicar que um avatar é virtual pode preservar confiança. Quando a empresa usa voz sintética de pessoa real, a informação pode ser especialmente relevante. A transparência também protege a marca contra alegações de manipulação.

Metadados e técnicas de proveniência podem ajudar a registrar origem de conteúdo. Entretanto, marcas podem ser removidas e não devem ser a única defesa. A empresa precisa conservar arquivos de origem, autorizações e registros de geração para demonstrar legitimidade.

A ANPD publicou em 2026 Radar Tecnológico dedicado a deepfakes, sinalizando a relevância do tema para privacidade e proteção de dados. Organizações devem acompanhar orientações regulatórias mesmo quando a obrigação específica ainda não está consolidada em lei geral de IA.

24.3 Fraude e resposta a incidentes de identidade

Deepfakes ampliam engenharia social. Vídeo ou áudio convincente pode pressionar empregado a ignorar controle. Treinamento deve ensinar que autenticidade

aparente não substitui procedimento. A empresa deve reforçar autenticação fora de banda para operações financeiras e mudanças de credenciais.

Quando a marca ou executivo é falsificado, o plano de resposta deve reunir jurídico, segurança, comunicação e plataforma. Preservar evidências é importante para pedidos de remoção, medidas judiciais e investigação.

A comunicação externa precisa ser rápida sem amplificar desnecessariamente o conteúdo fraudulento. A organização pode publicar canal oficial de verificação e orientar clientes sobre sinais e procedimentos.

O risco de identidade sintética deve entrar em matriz de fraude corporativa. Não é apenas “tema de IA”; é evolução de técnicas de falsificação que afeta controles clássicos.

Capítulo 25 — Transferências internacionais e fornecedores globais

25.1 A nuvem transforma um prompt em operação internacional

Ferramentas de IA frequentemente processam dados fora do Brasil ou utilizam infraestrutura distribuída. A organização precisa distinguir localização física, entidade contratada e cadeia de suboperadores. Uma empresa brasileira pode contratar entidade local e ainda assim realizar transferência internacional de dados pessoais.

A Resolução CD/ANPD 19/2024 regulamentou mecanismos de transferência internacional, incluindo decisões de adequação, cláusulas-padrão contratuais, cláusulas específicas e normas corporativas globais. Para

projetos de IA, isso deve ser integrado à contratação e ao mapa de dados.

A empresa deve identificar exportador e importador, finalidade, categorias de dados e mecanismo utilizado. Não é suficiente registrar “servidor nos EUA” ou “cloud global”. A análise jurídica precisa acompanhar o fluxo concreto.

Também é necessário separar hipótese legal do tratamento e mecanismo de transferência. A existência de cláusula-padrão não substitui a necessidade de base legal adequada para o tratamento em si.

25.2 Cláusulas-padrão e decisão de adequação

A Resolução 19/2024 prevê cláusulas-padrão contratuais da ANPD como mecanismo para transferências. Quando aplicáveis, devem ser incorporadas integralmente conforme as regras da Agência. Contratos globais que utilizam apenas modelos estrangeiros de cláusulas não devem ser presumidos equivalentes no Brasil sem análise.

Em janeiro de 2026, a ANPD reconheceu a União Europeia como organismo internacional com grau de proteção adequado por meio da Resolução CD/ANPD 32/2026. Isso adicionou uma rota relevante para transferências cobertas pela decisão. A organização deve verificar escopo e condições aplicáveis ao fluxo concreto.

Para grupos multinacionais, normas corporativas globais podem ser estratégia de longo prazo, mas exigem aprovação quando usadas como mecanismo regulado. Empresas menores normalmente dependem de adequação, cláusulas-padrão ou outras hipóteses legais do art. 33 da LGPD.

A governança de fornecedores deve manter inventário do mecanismo de transferência por serviço. Mudança de suboperador ou região pode exigir atualização.

25.3 Soberania, continuidade e ordens estrangeiras

Além de LGPD, organizações devem considerar continuidade e acesso por autoridades estrangeiras. A pergunta não é apenas onde o dado está, mas sob qual jurisdição o fornecedor opera e que compromissos contratuais assume diante de pedidos governamentais.

Setores estratégicos podem exigir arquitetura específica, criptografia com chaves controladas pelo cliente ou segregação regional. A decisão precisa combinar risco jurídico, segurança, custo e desempenho.

Vendor lock-in global também deve ser considerado. Caso mudança regulatória torne determinada arquitetura inadequada, a empresa precisa ter possibilidade de migrar dados e aplicações. Contratos devem prever exportação e suporte de transição.

Transferência internacional, portanto, não é cláusula isolada de privacidade; é elemento de arquitetura empresarial e resiliência.

Capítulo 26 — Conselho de administração, M&A e diligência corporativa

26.1 IA como risco de governança corporativa

Quando IA afeta produtos centrais, clientes ou operações críticas, o tema ultrapassa departamento de tecnologia. Administradores precisam compreender exposição material, assim como compreendem cibersegurança, privacidade e continuidade. O conselho

não precisa avaliar hiperparâmetros, mas deve receber visão sobre inventário, riscos altos, incidentes e dependências estratégicas.

Relatórios executivos devem evitar linguagem promocional. Informar que “80% dos processos usam IA” não revela risco. Indicadores úteis incluem número de sistemas de alto impacto, casos sem responsável, fornecedores críticos, reclamações, incidentes e riscos aceitos.

A supervisão deve ser proporcional ao porte. Empresas menores podem atribuir função a comitê executivo; companhias maiores podem integrar IA a comitês de risco, tecnologia ou auditoria. O importante é existir cadeia de accountability.

Decisões relevantes devem ser registradas. Se a diretoria aceita risco de lançar sistema com limitação conhecida, a justificativa e mitigadores devem constar em evidência contemporânea.

26.2 Due diligence em fusões e aquisições

Em M&A, IA cria ativos e passivos difíceis de ver no balanço. A diligência deve investigar origem de datasets, direitos de treinamento, dependência de modelos de terceiros, licenças de software, incidentes, reclamações, proteção de dados e compromissos contratuais com clientes.

Uma startup pode afirmar possuir “modelo proprietário” quando, na prática, depende integralmente de API externa e possui apenas camada de interface. Isso não diminui necessariamente valor, mas altera análise de propriedade intelectual, margem, continuidade e poder de negociação.

Datasets são outro ponto crítico. Se vantagem competitiva depende de dados obtidos sem base jurídica ou licença adequada, o risco acompanha aquisição. Comprador deve solicitar documentação de origem e direitos.

Também é importante verificar se clientes receberam promessas sobre acurácia, exclusividade ou localização de dados que não correspondem à arquitetura atual. Passivo comercial pode surgir de marketing técnico exagerado.

26.3 Representations, warranties e integração pós-aquisição

Contratos de aquisição podem incluir declarações sobre conformidade de tratamento de dados, direitos sobre datasets e modelos, ausência de uso indevido de propriedade intelectual, incidentes conhecidos e dependências relevantes.

Quando IA é material para valuation, indenizações específicas podem ser justificadas. Entretanto, cláusulas só são úteis se a diligência identificar riscos concretos e se houver mecanismos econômicos adequados.

Após fechamento, integração deve priorizar inventário. Sistemas da adquirida precisam ser incorporados ao framework do grupo. Ferramentas de shadow AI e contratos pessoais são riscos comuns em empresas de crescimento rápido.

A integração também deve preservar evidências. Migrar plataformas sem conservar logs necessários pode prejudicar defesa em disputas anteriores à aquisição.

Capítulo 27 — Model Risk Management aplicado à IA

27.1 O modelo precisa de dono, finalidade e limites

Model Risk Management surgiu com força em setores financeiros, mas seus princípios são úteis para qualquer empresa. Todo modelo relevante deve possuir responsável, finalidade definida, dados, metodologia, métricas, limitações, validação e monitoramento.

A primeira defesa contra uso indevido é a declaração de uso pretendido. Um modelo validado para priorizar atendimentos não deve ser automaticamente reutilizado para avaliar desempenho de empregados. A mudança de finalidade exige nova análise.

Limitações devem ser registradas em linguagem de negócio. “Performance de 0,87 AUC” é insuficiente para gestor. O documento deve explicar que tipo de erro ocorre, em que cenários e quais consequências.

Model cards, fichas técnicas ou documentação equivalente servem como ponte entre desenvolvedor, jurídico, risco e auditoria.

27.2 Validação independente

Quem desenvolve um modelo pode ter vieses de confirmação. Para sistemas relevantes, validação por equipe independente ou ao menos revisão por pessoa não diretamente responsável pelo desenvolvimento melhora qualidade.

A validação deve reproduzir métricas, testar dados fora da amostra, analisar estabilidade, sensibilidade, grupos e cenários adversos. Para modelos generativos, pode utilizar

suites de testes, critérios humanos estruturados e conjuntos de prompts de risco.

Fornecedores externos complicam validação porque código e dados de treinamento podem não estar disponíveis. A empresa pode então testar comportamento por caixa-preta, exigir documentação e limitar casos de uso conforme incerteza.

Independência não significa distância total. Validadores precisam compreender objetivo e contexto para testar aspectos relevantes.

27.3 Deriva, monitoramento e revalidação

Modelos podem degradar quando população, comportamento ou ambiente muda. Esse fenômeno é conhecido como drift. Monitoramento deve observar variáveis de entrada, distribuição de saídas e desempenho quando verdade de referência se torna disponível.

Modelos generativos de terceiros podem mudar sem que o cliente treine nova versão. Atualização do fornecedor é evento de modelo e deve ser rastreada. Uma resposta que funcionava ontem pode mudar após upgrade.

A empresa precisa definir gatilhos de revalidação: queda de métrica, aumento de reclamações, nova população, atualização de versão, alteração de dados, incidente ou mudança regulatória.

Sem revalidação, a aprovação inicial vira fotografia antiga. Governança deve acompanhar o sistema vivo.

Capítulo 28 — Agentes de IA e automação autônoma

28.1 De responder a executar

Chatbots tradicionais produzem informação. Agentes podem planejar etapas, consultar sistemas, enviar e-mails, criar pedidos, alterar registros e acionar pagamentos. A transição de geração para ação aumenta radicalmente a exposição jurídica.

A pergunta central é autoridade. Que atos o agente pode realizar? Em nome de quem? Qual limite monetário? Quais sistemas acessa? Que ações exigem aprovação? As respostas devem estar em controles técnicos e políticas, não apenas em prompt.

A empresa deve tratar credenciais do agente como identidades de máquina. Princípio do menor privilégio, segregação de funções e rotação de chaves continuam aplicáveis. Um agente de atendimento não deve possuir acesso de escrita a sistema financeiro apenas porque isso é tecnicamente conveniente.

A trilha de auditoria precisa mostrar instrução, ferramentas chamadas, parâmetros e resultado. Sem isso, incidentes autônomos são difíceis de reconstruir.

28.2 Delegação e representação

Direito contratual e societário pressupõe pessoas autorizadas a representar organizações. Quando agente envia proposta ou aceita termo, surge questão sobre manifestação de vontade e limites de autorização. A empresa deve definir claramente quais atos automatizados são vinculantes.

Para operações de baixo valor e regras determinísticas, automação pode ser autorizada de forma ampla. Para contratos, pagamentos ou decisões relevantes, aprovação humana pode ser necessária. Limites precisam ser configurados.

A contraparte também deve saber quando interage com agente se isso for material à transação. Em determinados contextos, transparência reduz disputa sobre expectativa e interpretação.

O risco de “agente alucinar compromisso” deve ser prevenido por templates, retrieval de regras oficiais e impossibilidade técnica de ultrapassar parâmetros autorizados.

28.3 Multiagentes e responsabilidade difusa

Arquiteturas com múltiplos agentes podem dividir tarefas de pesquisa, planejamento, execução e controle. Isso melhora modularidade, mas aumenta dificuldade de identificar causa de erro. Logs estruturados e atribuição de função tornam-se essenciais.

A empresa deve evitar confiar em agente supervisor como substituto completo de controle. Se todos os agentes compartilham o mesmo modelo ou vulnerabilidade, podem confirmar erro uns dos outros.

Testes devem incluir falhas encadeadas e dados maliciosos. Um agente pode recuperar documento comprometido e transmitir instrução a outro com maior privilégio.

Do ponto de vista jurídico, complexidade técnica não reduz dever de governança. Ao contrário, aumenta necessidade de desenhar fronteiras de autoridade compreensíveis.

Capítulo 29 — IA em departamentos jurídico, compliance e auditoria

29.1 Pesquisa e redação jurídica

IA generativa pode resumir processos, comparar cláusulas, produzir rascunhos e organizar jurisprudência. O ganho é relevante, mas a responsabilidade profissional permanece humana. Citações precisam ser verificadas em fonte oficial e o sistema não deve ser tratado como autoridade jurídica.

O departamento deve separar tarefas de baixa e alta criticidade. Reescrever texto interno pode exigir revisão comum; protocolar petição, emitir parecer ou responder regulador exige conferência de fatos e fundamentos.

Dados de clientes e processos podem estar protegidos por confidencialidade. Ferramentas aprovadas devem possuir termos adequados e controles de retenção. O uso de conta pública para documentos sigilosos deve ser proibido.

Uma boa prática é criar prompts e workflows oficiais com fontes autorizadas, reduzindo variação individual e facilitando treinamento.

29.2 Compliance e investigação interna

IA pode priorizar transações, analisar comunicações e identificar padrões suspeitos. Contudo, resultados são sinais, não culpabilidade. Investigações internas devem validar evidências e preservar direito de defesa e proporcionalidade.

Monitoramento de empregados envolve privacidade e legislação trabalhista. A empresa precisa definir finalidade, escopo e critérios. Capturar todas as

mensagens para um modelo sem justificativa pode ser excessivo.

Modelos de detecção de fraude e corrupção também podem reproduzir vieses. O jurídico deve monitorar falsos positivos e evitar que determinada unidade ou grupo seja investigado apenas por características correlacionadas.

Evidências produzidas por IA devem conservar origem. Um resumo sem acesso ao documento base pode ser inadequado para procedimento disciplinar ou judicial.

29.3 Auditoria assistida por IA

Auditoria pode usar IA para selecionar amostras, detectar anomalias e revisar documentos. A ferramenta amplia alcance, mas o auditor precisa compreender critérios e limitações para não automatizar conclusão.

A independência da auditoria deve ser preservada. Se o mesmo time que desenvolve sistema também configura ferramenta que o audita, pode haver conflito. Validação e acesso a dados devem ser separados quando possível.

Logs de consultas e transformações precisam ser conservados quando sustentam achado material. O objetivo é permitir reprodutibilidade.

IA pode tornar auditoria contínua mais viável, transformando controles periódicos em monitoramento. Isso exige governança para evitar volume de alertas que ninguém consegue investigar.

Capítulo 30 — Fiscalização, prova e litígios envolvendo IA

30.1 O que será pedido em uma investigação

Em disputa, a parte interessada provavelmente solicitará explicação sobre finalidade, dados, critérios, versão e pessoas responsáveis. Empresas precisam preparar preservação antes que o problema exista.

O inventário permite localizar sistema. Logs mostram operação. Avaliação de impacto demonstra riscos conhecidos. Testes indicam diligência. Contratos revelam responsabilidades. Reclamações mostram sinais anteriores. Juntos, esses elementos formam narrativa probatória.

Documentação excessiva e contraditória pode ser tão ruim quanto ausência. Registros devem refletir realidade e possuir controle de versão. Templates copiados sem análise específica podem comprometer credibilidade.

Legal hold deve abranger artefatos técnicos quando litígio é previsível: prompts, outputs, logs, datasets relevantes, versões e tickets. Jurídico precisa coordenar preservação com tecnologia.

30.2 Segredo comercial versus direito de defesa

Litígios podem exigir informação sobre modelo que a empresa considera segredo. O conflito deve ser tratado por mecanismos processuais de confidencialidade, perícia e acesso restrito, quando cabíveis. Simples recusa total pode ser inadequada se impede exercício de direito.

A organização deve separar previamente camadas de documentação. Informações de alto nível podem ser fornecidas a usuário; documentação técnica mais

detalhada pode ser disponibilizada a auditor ou perito sob sigilo.

Explicações devem ser verdadeiras e consistentes. Não é recomendável produzir justificativa diferente para cada audiência. A capacidade de explicar nasce do design do sistema.

Segredo comercial protege vantagem legítima, não serve para ocultar ausência de governança.

30.3 Perícia e reprodução de decisões

Perícia em IA pode exigir reproduzir ambiente histórico. Se o fornecedor atualizou modelo sem manter versão, reprodução exata pode ser impossível. Por isso, sistemas de alto impacto devem registrar identificadores de versão e, quando viável, preservar artefatos necessários.

Também é importante conservar dados de entrada relevantes dentro dos prazos legais e de retenção. A empresa precisa equilibrar minimização com necessidade de prova. Políticas podem prever retenção específica de logs de decisão sem guardar dados brutos indefinidamente.

Peritos podem avaliar desempenho, viés, segurança e causalidade. Jurídico deve formular quesitos ligados à controvérsia e evitar perguntas vagas como “a IA é confiável?”.

A maturidade probatória é parte da governança. Um sistema que não pode ser auditado depois pode ser inadequado para decisões que provavelmente serão contestadas.

Parte IX — Estudos de caso empresariais

Estudo de caso 1 — Banco usa IA para negar crédito

Um banco contrata fornecedor que atribui score a clientes usando dados cadastrais, histórico financeiro e sinais comportamentais. A aplicação recusa crédito automaticamente para parcela dos solicitantes. Após reclamações, a equipe jurídica descobre que não existe processo claro de revisão e que o fornecedor não entrega fatores explicativos por decisão.

A análise começa pela LGPD. Há tratamento de dados pessoais e decisão automatizada que afeta interesse do titular, com menção expressa ao perfil de crédito no art. 20. O banco precisa avaliar mecanismos de revisão, transparência e correção de dados. O fato de score vir de terceiro não elimina sua posição como agente que define finalidade e utiliza resultado.

Em paralelo, o CDC se aplica à relação de consumo e exige informação e tratamento compatível com boa-fé. O banco deve avaliar se as razões comunicadas são adequadas e se o processo cria barreira indevida à contestação.

Do ponto de vista de governança, o erro principal foi contratar antes de definir requisitos de explicabilidade e logs. A correção inclui renegociar acesso a fatores, criar canal de revisão, testar diferenças entre grupos, monitorar reversões e registrar versão do modelo. Se o fornecedor

não oferece capacidade mínima, a empresa deve limitar uso ou substituí-lo.

Estudo de caso 2 — RH usa análise de vídeo em entrevistas

Uma empresa adota ferramenta que analisa vídeo de candidatos e produz notas de “energia”, “confiança” e “aderência cultural”. O fornecedor afirma utilizar IA para identificar padrões de expressão e voz. O RH usa a nota para eliminar automaticamente candidatos abaixo de determinado limiar.

O jurídico deve questionar validade científica da inferência e necessidade. Voz e imagem podem envolver biometria e dados pessoais; atributos inferidos podem produzir discriminação. A classificação automática afeta oportunidade profissional e exige supervisão cuidadosa.

A empresa deve pedir evidências independentes de validade, métricas por grupos e descrição das variáveis. Se o fornecedor não consegue explicar o que mede, o risco é elevado. “Aderência cultural” também pode funcionar como proxy de homogeneidade e perpetuar padrões históricos.

A alternativa pode ser reduzir autonomia: utilizar ferramenta apenas para transcrição e organização, deixando avaliação de competências a critérios objetivos. O princípio de necessidade recomenda não manter funcionalidade intrusiva sem ganho comprovado.

Estudo de caso 3 — Escritório cola processo sigiloso em chatbot público

Um advogado copia peças de processo confidencial para conta pessoal de ferramenta generativa a fim de criar resumo. Dias depois, percebe que os termos do serviço permitem retenção e possível uso para melhoria.

O problema envolve confidencialidade profissional, proteção de dados e segurança. A primeira ação é preservar informação sobre o envio e verificar configurações do serviço. Deve-se solicitar eliminação quando disponível, avaliar exposição e documentar incidente.

A organização precisa decidir se existe risco ou dano relevante a titulares e se outras obrigações de comunicação se aplicam. O caso também revela falha de governança: havia proibição, mas nenhuma ferramenta corporativa alternativa.

A remediação inclui contratar ambiente aprovado, configurar retenção, treinar equipe e classificar tipos de documento. Política realista reduz reincidência.

Estudo de caso 4 — E-commerce cria publicidade infantil personalizada

Uma plataforma vende produtos variados e não se declara infantil, mas possui grande número de usuários adolescentes. O sistema de recomendação utiliza histórico de navegação para direcionar anúncios e um módulo de análise emocional ajusta mensagens conforme reação do usuário.

Com o ECA Digital vigente, a empresa precisa analisar acesso provável por menores. A lei veda perfilamento

para publicidade comercial a crianças e adolescentes e também análise emocional para esse fim. A classificação do serviço como “generalista” não elimina a incidência se o uso por menores for provável.

A correção exige separar recomendação funcional de publicidade, rever aferição de idade e impedir uso de técnicas proibidas para menores. Configurações devem priorizar proteção por padrão.

O caso mostra por que produto, publicidade e privacidade precisam trabalhar juntos. A obrigação não pode ser resolvida apenas em termos de uso.

Estudo de caso 5 — Modelo gera campanha com celebridade não contratada

Equipe de marketing pede a modelo generativo “uma imagem semelhante a famoso apresentador” e publica anúncio com rosto que claramente evoca a pessoa. Não houve autorização.

A empresa pode enfrentar questões de imagem, personalidade, publicidade e concorrência desleal, dependendo do contexto. O fato de a imagem ser sintética não elimina associação identificável.

Política de marketing deve proibir geração de pessoas reais ou identificáveis para uso comercial sem autorização. Ferramentas podem ser configuradas com filtros, mas revisão humana continua necessária.

O processo de aprovação deve registrar origem do ativo e licença. “Foi criado por IA” não é cadeia de titularidade suficiente.

Estudo de caso 6 — Agente autônomo altera preço e envia proposta

Uma empresa implementa agente conectado ao CRM e ao sistema de propostas. Para acelerar vendas, o agente pode ajustar descontos. Em determinado caso, interpreta instrução incorretamente e oferece desconto muito superior ao permitido, enviando proposta ao cliente.

A questão jurídica envolve representação, validade da oferta, controles internos e contrato com fornecedor. A organização precisa analisar se o agente estava autorizado a enviar proposta vinculante e como a contraparte percebeu a manifestação.

Do ponto de vista técnico, faltou limite rígido. Regras monetárias importantes não devem depender apenas de prompt. O sistema deveria bloquear desconto acima de faixa e exigir aprovação humana.

A lição é que autonomia transforma linguagem em ato. Controles jurídicos precisam ser convertidos em permissões técnicas.

Estudo de caso 7 — Hospital usa modelo treinado em outro país

Hospital contrata IA para priorizar exames radiológicos. O fornecedor apresenta excelente desempenho em estudo estrangeiro, mas não há validação com população local. Após meses, médicos percebem desempenho menor em determinado subgrupo.

O problema combina dados sensíveis, segurança do paciente, validação e possível discriminação. A instituição deveria ter realizado validação local antes de confiar na ferramenta em fluxo crítico.

A correção inclui reduzir peso da recomendação, revisar casos anteriores, testar por subgrupos e negociar com fornecedor. Mudança de população é risco previsível em modelos de saúde.

Jurídico deve participar da definição de evidências mínimas e responsabilidade, mas a decisão depende de equipe clínica e técnica. Governança de IA é necessariamente multidisciplinar.

Estudo de caso 8 — Startup descobre que dataset comprado não tinha licença

Uma startup treina modelo com dataset adquirido de intermediário. Durante rodada de investimento, comprador pede documentos de origem e descobre que parte do conteúdo foi coletada de sites com restrições e inclui obras protegidas.

O risco afeta propriedade intelectual, proteção de dados, valuation e continuidade do modelo. Excluir registros da base não necessariamente remove influência do treinamento já realizado. Pode ser necessário avaliar retraining ou outra remediação.

A diligência deveria ter ocorrido antes da compra do dataset. Contrato com fornecedor precisa conter garantias e cooperação. A startup também deveria conservar documentação de proveniência.

Para investidores, o caso mostra que “dados” não são ativo automaticamente limpo. Direitos de uso fazem parte do valor.

Estudo de caso 9 — Chatbot de atendimento inventa política de reembolso

Chatbot responde a consumidor que existe direito a reembolso integral em situação não prevista. O cliente toma decisão com base nessa informação e depois a empresa tenta negar.

A resposta gerada integra atendimento oficial e pode produzir expectativa legítima. A empresa não pode tratar o bot como terceiro sem relação. O CDC e boa-fé são relevantes.

A arquitetura deveria limitar respostas a base oficial de políticas, com RAG e citações internas, além de bloquear criação de condições comerciais não autorizadas. Casos fora da base devem escalar para humano.

Logs são essenciais para comprovar o que foi informado. Treinar o chatbot apenas para “ser útil” sem limite jurídico é erro de design.

Estudo de caso 10 — Fornecedor global altera termos e passa a treinar com prompts

Uma empresa utiliza ferramenta empresarial há um ano. O fornecedor atualiza termos online e amplia uso de conteúdo para melhoria do serviço. Ninguém percebe porque contrato remete genericamente às políticas publicadas no site.

O risco mostra importância de hierarquia documental e gestão contínua de fornecedor. Contrato crítico não deveria permitir mudança material silenciosa que altere finalidade do tratamento.

A empresa precisa avaliar se a mudança se aplica à sua conta, interromper envio de dados sensíveis se necessário e renegociar. Também deve implantar monitoramento de alterações contratuais.

Governança não termina na assinatura. Serviços de IA mudam rapidamente e cláusulas precisam acompanhar o ciclo de vida.

Apêndice A — Modelo de Política Corporativa de Uso de Inteligência Artificial

A.1 Objetivo e escopo

Esta Política estabelece princípios e regras para aquisição, desenvolvimento, implantação e uso de sistemas de inteligência artificial pela organização. Aplica-se a empregados, administradores, prestadores e terceiros autorizados que utilizem recursos tecnológicos em nome da empresa.

São abrangidos sistemas generativos, preditivos, classificadores, recomendadores, agentes automatizados e funcionalidades de IA incorporadas a softwares. O fato de uma funcionalidade ser gratuita, experimental ou disponibilizada por fornecedor já contratado não exclui sua incidência.

A.2 Princípios

A organização utilizará IA de forma compatível com legalidade, finalidade legítima, necessidade, segurança, transparência proporcional, supervisão, não discriminação

e responsabilização. Sistemas devem possuir responsável de negócio e controles proporcionais ao impacto.

Nenhum projeto será aprovado exclusivamente com base em promessa comercial de precisão. Desempenho, limites e riscos devem ser avaliados no contexto real de uso.

A.3 Dados e confidencialidade

Informações públicas podem ser utilizadas em ferramentas autorizadas conforme regras gerais. Informações internas, pessoais ou confidenciais somente podem ser inseridas em serviços aprovados para a respectiva classificação de dados. Credenciais, segredos, chaves privadas e informações cuja divulgação seja proibida não devem ser inseridos em ferramentas externas sem autorização técnica específica.

O usuário deve verificar se a conta utilizada é corporativa e se as configurações de retenção e treinamento são compatíveis com a finalidade. Contas pessoais não devem ser utilizadas para processar dados corporativos protegidos.

A.4 Revisão humana

Saídas de IA devem ser revisadas conforme o risco. Conteúdos que criem obrigação jurídica, sejam enviados a reguladores, afetem direitos de pessoas, envolvam aconselhamento profissional ou sejam utilizados em decisão relevante exigem verificação independente por pessoa qualificada.

A revisão deve ser real. O revisor deve ter autoridade e informação suficiente para discordar do sistema.

Aprovação automática ou meramente formal não constitui controle adequado.

A.5 Usos proibidos sem aprovação específica

É proibido utilizar IA para decisões totalmente automatizadas de alto impacto sobre empregados, candidatos, clientes ou terceiros sem avaliação e aprovação formal; para inferir atributos sensíveis sem finalidade e base jurídica adequadas; para gerar conteúdo enganoso que simule pessoa real sem autorização; para contornar controles de segurança; ou para inserir dados protegidos em ferramentas não autorizadas.

A.6 Aquisição e desenvolvimento

Novos fornecedores de IA devem passar por avaliação proporcional envolvendo segurança, privacidade, propriedade intelectual, continuidade e termos de uso. Desenvolvimento interno deve registrar origem de dados, versão de modelos, testes e responsáveis.

Mudanças materiais de modelo, finalidade, dados ou autonomia exigem reavaliação.

A.7 Incidentes

Erros relevantes, vazamentos, comportamento inesperado, conteúdo potencialmente ilícito, decisões discriminatórias ou uso indevido devem ser reportados imediatamente pelos canais internos. A empresa avaliará necessidade de suspensão, investigação e comunicação a autoridades ou titulares.

A.8 Treinamento e sanções

Usuários receberão treinamento compatível com suas funções. Violações serão tratadas conforme políticas internas e legislação, considerando gravidade, intenção, impacto e cooperação na correção.

Apêndice B — Avaliação de Impacto Algorítmico

B.1 Identificação

Nome do sistema:

Área responsável:

Responsável executivo:

Fornecedor/modelo:

Versão:

Data da avaliação:

Finalidade de negócio: descreva o problema que o sistema pretende resolver e por que IA é necessária.

B.2 Pessoas afetadas

Identifique usuários diretos e pessoas que podem sofrer consequência mesmo sem interagir com a ferramenta. Informe se há crianças, adolescentes, empregados, candidatos, consumidores, pacientes, estudantes ou grupos vulneráveis.

B.3 Dados

Liste categorias de dados de entrada, origem, base legal, dados sensíveis, retenção, transferências e

suboperadores. Diferencie dados observados, inferidos e gerados. Informe se dados são usados para treinamento, fine-tuning ou melhoria do fornecedor.

B.4 Decisão

Descreva a saída do sistema e o que acontece depois. A saída apenas informa, recomenda, prioriza ou execução? Há revisão humana? O revisor pode rejeitar? Qual o prazo e qual informação ele recebe?

B.5 Riscos

Avalie pelo menos: privacidade, discriminação, segurança, erro, fraude, propriedade intelectual, manipulação, explicabilidade, dependência do fornecedor, impacto reputacional e regulação setorial.

Para cada risco, registre probabilidade, impacto, controle existente, risco residual e responsável.

B.6 Testes

Registre métricas de desempenho, grupos avaliados, casos extremos, testes adversariais, limites conhecidos e critérios de aprovação. Evite aceitar apenas métricas fornecidas pelo vendedor quando o contexto de uso for diferente.

B.7 Transparência e direitos

Defina que informação será apresentada a usuários e pessoas afetadas. Descreva canal de contestação, correção de dados e revisão. Informe como a empresa preservará segredos comerciais sem eliminar explicação significativa.

B.8 Monitoramento

Defina indicadores, frequência, gatilhos de reavaliação e autoridade de suspensão. Inclua eventos como troca de modelo, mudança de finalidade, aumento de reclamações, queda de desempenho e incidente de segurança.

B.9 Aprovação

A avaliação deve conter parecer ou aprovação das funções exigidas pelo nível de risco. Decisões de aceitar risco residual relevante devem ser atribuídas a gestor com autoridade adequada.

Apêndice C — Due diligence de fornecedor de IA

C.1 Empresa e serviço

1. Quem é a entidade contratada e em quais países opera?
2. O serviço é fornecido diretamente ou depende de outro provedor de modelo?
3. Quais suboperadores e regiões de processamento são utilizados?
4. O fornecedor possui histórico público relevante de incidentes ou sanções?

C.2 Dados e privacidade

5. Prompts e arquivos são usados para treinamento ou melhoria?
6. É possível desativar esse uso contratualmente e tecnicamente?

7. Qual a retenção de prompts, outputs, logs e backups?
8. Como pedidos de eliminação são propagados?
9. Há transferências internacionais e qual mecanismo jurídico é utilizado?
10. O fornecedor coopera com direitos de titulares?

C.3 Segurança

11. Há criptografia em trânsito e repouso?
12. Existe isolamento entre clientes?
13. Quais mecanismos de autenticação e SSO estão disponíveis?
14. O fornecedor possui relatórios independentes de segurança?
15. Qual o processo de gestão de vulnerabilidades?
16. Em quanto tempo comunica incidente relevante?
17. É possível obter logs suficientes para investigação?

C.4 Modelo e desempenho

18. Qual modelo e versão são utilizados?
19. O fornecedor pode alterar o modelo sem aviso?
20. Quais métricas e limitações são documentadas?
21. O sistema foi avaliado para o domínio da empresa?
22. Há mecanismos de filtragem e proteção contra abuso?
23. O fornecedor permite testes antes de mudanças materiais?

C.5 Propriedade intelectual

24. Quem detém direitos sobre inputs e outputs?

- 25. O fornecedor concede licença sobre dados do cliente?
- 26. Há garantia ou indenização para reclamações de propriedade intelectual?
- 27. Como o fornecedor trata alegações de conteúdo infrator?
- 28. O serviço pode produzir conteúdo semelhante para outros clientes?

C.6 Continuidade e saída

- 29. É possível exportar dados, configurações e históricos?
- 30. Há suporte de migração?
- 31. O que ocorre com os dados após rescisão?
- 32. Existe dependência de formato proprietário que impeça substituição?
- 33. Há plano de continuidade para indisponibilidade do modelo?

Apêndice D — Cláusulas-modelo para contratos de IA

D.1 Finalidade autorizada

“O Serviço será utilizado exclusivamente para as finalidades descritas no Anexo Técnico. Qualquer utilização que implique decisão de alto impacto sobre pessoa natural, tratamento de nova categoria de dados pessoais ou ampliação material de autonomia dependerá de avaliação e aprovação prévias das Partes, quando aplicável.”

D.2 Uso de dados para treinamento

“O Fornecedor não utilizará Dados do Cliente, inclusive prompts, arquivos e outputs que contenham informação do Cliente, para treinamento, ajuste ou melhoria de modelos de uso geral, salvo autorização prévia e expressa do Cliente em instrumento específico. Dados estritamente necessários à segurança e prestação do Serviço serão tratados conforme finalidades, retenção e medidas descritas no Anexo de Proteção de Dados.”

D.3 Mudança de modelo

“O Fornecedor notificará alterações materiais do modelo ou da arquitetura que possam afetar segurança, desempenho, localização de processamento, tratamento de dados ou funcionalidade essencial. Para sistemas classificados pelo Cliente como críticos, será disponibilizado período razoável de validação ou mecanismo equivalente antes da migração obrigatória, quando tecnicamente possível.”

D.4 Incidentes

“O Fornecedor comunicará ao Cliente, sem demora indevida e dentro do prazo contratual acordado, qualquer incidente capaz de afetar confidencialidade, integridade, disponibilidade ou tratamento regular dos Dados do Cliente, fornecendo informações necessárias para avaliação de obrigações legais e regulatórias.”

D.5 Auditoria

“O Fornecedor disponibilizará documentação e evidências razoavelmente necessárias à avaliação de segurança, privacidade e controles do Serviço, podendo utilizar relatórios independentes, certificações e respostas técnicas. Em caso de incidente material ou exigência regulatória, as Partes cooperarão para auditoria direcionada sob condições de confidencialidade.”

D.6 Propriedade intelectual

“Cada Parte manterá direitos sobre materiais preexistentes de sua titularidade. O regime aplicável aos outputs, prompts, configurações, bases curadas e materiais derivados será aquele descrito no Anexo de Propriedade Intelectual, observados direitos de terceiros e limitações inerentes a conteúdo gerado por sistemas de inteligência artificial.”

Apêndice E — Playbook de incidente envolvendo IA

E.1 Detecção

O incidente pode ser identificado por alerta técnico, reclamação, auditoria, fornecedor ou empregado. Exemplos: exposição de prompt, vazamento de dataset, resposta que revela informação confidencial, comportamento discriminatório em massa, modelo comprometido, uso de credencial indevida ou execução autônoma não autorizada.

E.2 Contenção

Defina se é necessário desabilitar modelo, revogar chave, bloquear integração, reduzir autonomia ou voltar à versão anterior. Preserve evidências antes de apagar logs. Acione fornecedor quando a causa puder estar no serviço externo.

E.3 Classificação jurídica

Avalie dados pessoais afetados, titulares, direitos envolvidos, relação de consumo, contratos, propriedade intelectual e regulação setorial. Determine se o evento é

incidente de segurança nos termos da LGPD e da Resolução CD/ANPD 15/2024 e se pode acarretar risco ou dano relevante.

E.4 Comunicação

Centralize comunicações externas. Não prometa causa ou extensão antes de investigação suficiente. Quando houver obrigação legal de comunicar ANPD, titulares, clientes ou reguladores setoriais, cumpra prazos e forneça informação clara.

E.5 Correção e aprendizado

Realize análise de causa raiz e defina ações. Atualize modelo, dados, filtro, interface, política ou contrato conforme necessário. Verifique se decisões anteriores precisam ser revistas. Registre encerramento e lições aprendidas.

Apêndice F — Matriz de risco de IA

Dimensão	Baixo	Médio	Alto
Impacto sobre pessoas	Apoio interno sem efeito relevante	Recomendação com efeito limitado e reversível	Decisão ou recomendação que afeta direito, oportunidade, acesso ou segurança
Dados	Públicos ou sem dados pessoais	Dados pessoais comuns limitados	Sensíveis, biometria, crianças, grande escala ou dados confidenciais críticos
Autonomia	Gera rascunho	Recomenda ação	Executa ação ou bloqueia acesso

Dimensão	Baixo	Médio	Alto
			sem revisão prévia
Reversibilidade	Correção simples	Exige processo de correção	Dano difícil de reverter
Exposição	Interna	Clientes limitados	Público amplo ou serviço essencial
Controles mínimos	Registro e revisão básica	Avaliação de privacidade/segurança, testes	Avaliação de impacto, comitê, auditoria, monitoramento e plano de contingência

A matriz é ponto de partida. Setores regulados podem exigir controles superiores. Uma única característica crítica pode elevar classificação mesmo que a pontuação total seja baixa.

Apêndice G — Checklist jurídico antes do go-live

1. A finalidade do sistema está escrita em linguagem de negócio?
2. Existe responsável executivo identificado?
3. O fluxo de dados está documentado?
4. Papéis de controlador e operador foram analisados?
5. Bases legais e dados sensíveis foram avaliados?
6. O fornecedor foi submetido a due diligence?
7. Termos permitem uso de dados para treinamento? Isso é aceitável?
8. Transferências internacionais estão mapeadas?

9. Direitos de titulares podem ser atendidos?
10. Há decisão automatizada que afeta interesses?
11. Existe revisão humana real quando necessária?
12. O sistema foi testado em casos extremos?
13. Há avaliação de desempenho por grupos relevantes?
14. Métricas mínimas foram aprovadas?
15. Limitações conhecidas estão documentadas?
16. Usuários recebem informação adequada?
17. Conteúdo sintético precisa ser identificado no contexto?
18. Propriedade intelectual de dados e outputs foi analisada?
19. Código e dependências foram revisados?
20. Segredos e credenciais estão protegidos?
21. Logs permitem reconstruir decisão relevante?
22. Mudanças de modelo geram reavaliação?
23. Existe plano de incidente?
24. Existe autoridade para suspender o sistema?
25. Contrato prevê cooperação, segurança e saída?
26. ECA Digital foi avaliado quando há acesso provável de menores?
27. Regras de consumo foram avaliadas quando há usuário consumidor?
28. Regras trabalhistas foram avaliadas quando afeta empregados ou candidatos?
29. Regulação setorial foi consultada?
30. A decisão de aceitar risco residual foi registrada?

Apêndice H — Glossário essencial

Agente de IA: sistema que combina modelo com ferramentas e capacidade de executar etapas ou ações com certo grau de autonomia.

Alucinação: saída plausível, porém incorreta ou não sustentada, produzida por modelo generativo.

Avaliação de Impacto Algorítmico: processo estruturado para identificar finalidade, pessoas afetadas, riscos, controles, testes e monitoramento de sistema de IA.

Controlador: agente que toma decisões referentes ao tratamento de dados pessoais nos termos da LGPD.

Embedding: representação numérica de informação utilizada para medir similaridade e realizar recuperação semântica, entre outras tarefas.

Fine-tuning: ajuste adicional de modelo com dados ou exemplos específicos para alterar seu comportamento.

Human in the loop: desenho em que pessoa participa de etapa decisória; juridicamente relevante apenas quando a participação é efetiva.

Inferência: resultado ou estimativa produzida pelo modelo a partir de dados de entrada.

LLM: large language model, modelo de linguagem de grande porte capaz de gerar e processar texto e outras modalidades conforme arquitetura.

Model card: documento que descreve finalidade, desempenho, dados, limitações e condições de uso de um modelo.

Operador: agente que realiza tratamento de dados pessoais em nome do controlador.

Perfilamento: processamento destinado a avaliar ou prever aspectos relacionados a pessoa, como preferências, comportamento, desempenho ou risco.

Prompt: instrução ou conjunto de dados fornecidos ao modelo para orientar sua saída.

Prompt injection: tentativa de manipular o modelo por instruções inseridas em conteúdo não confiável.

RAG: retrieval-augmented generation, técnica que combina recuperação de documentos com geração por modelo.

Shadow AI: uso de ferramentas de IA sem aprovação, visibilidade ou governança organizacional adequada.

Viés: termo amplo que pode se referir a distorção estatística, de dados ou a efeitos discriminatórios; exige definição precisa no caso concreto.

Apêndice I — Modelo de relatório executivo ao conselho

1. Visão geral

No período, a organização mantém [número] sistemas de IA inventariados, dos quais [número] são classificados como alto risco, [número] médio e [número] baixo. Os principais domínios são [áreas]. Não foram identificados/foram identificados casos sem responsável executivo, conforme detalhamento abaixo.

2. Riscos materiais

Apresente no máximo cinco riscos com linguagem executiva. Para cada um: sistema, impacto potencial, controle atual, risco residual, decisão necessária e prazo. Evite listas de dezenas de problemas técnicos.

3. Incidentes e reclamações

Informe incidentes relevantes, número de pessoas potencialmente afetadas, status de comunicação regulatória e medidas corretivas. Inclua tendência de reclamações e reversões em decisões automatizadas.

4. Fornecedores críticos

Liste fornecedores de modelo ou infraestrutura cuja falha interromperia operação relevante. Informe riscos de concentração, renovação contratual e mecanismo de transferência internacional de dados.

5. Mudanças regulatórias

Resuma normas efetivamente vigentes e projetos em tramitação separadamente. Em agosto de 2026, destaque evolução da ANPD, ECA Digital e acompanhamento do PL 2.338/2023 sem tratá-lo como lei.

6. Decisões solicitadas

O relatório deve terminar com decisões claras: aceitar risco, financiar controle, suspender sistema, renegociar contrato ou alterar política. Conselho não deve receber apenas informação sem ação definida.

Apêndice J — Perguntas de auditoria interna

1. O inventário corresponde às ferramentas encontradas em compras e logs de rede?
2. Todo sistema relevante possui responsável de negócio ativo?
3. Casos classificados como alto risco têm avaliação completa e atualizada?
4. Mudanças de modelo foram registradas?
5. Os testes documentados podem ser reproduzidos?
6. A revisão humana ocorre de fato ou apenas formalmente?
7. Usuários conseguem contestar decisões relevantes?
8. O fornecedor cumpre retenção contratada?
9. Dados eliminados são removidos de índices e ambientes auxiliares quando aplicável?
10. Há ferramentas pessoais sendo usadas com dados corporativos?
11. Logs são suficientes para reconstruir decisão?
12. Dados de treinamento possuem proveniência documentada?
13. Resultados são monitorados por grupos relevantes quando necessário?
14. Incidentes anteriores geraram ações concluídas?
15. Contratos críticos contêm mecanismo de saída?
16. Transferências internacionais possuem mecanismo válido?

17. Produtos acessíveis a menores foram avaliados sob ECA Digital?
18. Conteúdos sintéticos comerciais possuem autorização e origem?
19. Agentes autônomos possuem limites técnicos e segregação de funções?
20. O conselho recebe informação sobre riscos materiais de IA?

Apêndice K — Registro mestre de sistema de IA e plano de evidências

K.1 Ficha de identificação permanente

Todo sistema relevante deve possuir uma ficha mestre que acompanhe o ativo durante todo o ciclo de vida. O objetivo não é produzir burocracia, mas criar um ponto único de verdade capaz de responder às perguntas básicas de auditoria, fiscalização, incidente e mudança. A ficha deve conter nome do sistema, código interno, área proprietária, patrocinador executivo, responsáveis técnico e jurídico, fornecedor, modelo, versão, ambiente, data de entrada em produção e classificação de risco vigente.

A finalidade deve ser descrita em linguagem de negócio e não em linguagem promocional. Em vez de “usar IA para otimizar a jornada”, registre “priorizar solicitações de atendimento conforme urgência estimada, sem encerrar chamados automaticamente”. Essa precisão ajuda a identificar expansão de escopo. Se o sistema passa a bloquear clientes, por exemplo, a finalidade mudou materialmente e exige nova avaliação.

A ficha também deve indicar pessoas afetadas, categorias de dados, integrações, principais decisões influenciadas, mecanismo de revisão humana e autoridade capaz de suspender a operação. Links para documentos detalhados podem ser usados para evitar duplicação.

K.2 Registro de versões e mudanças

Mudanças precisam ser tratadas como eventos jurídicos quando podem alterar risco. O registro deve indicar data, versão anterior, nova versão, motivo, responsável, testes realizados e decisão de aprovação. Atualizações automáticas de fornecedor devem ser incluídas quando forem conhecidas ou detectáveis.

A empresa pode definir categorias de mudança. Mudança menor inclui correção de interface sem impacto no modelo. Mudança relevante inclui troca de modelo, nova fonte de dados, alteração de prompt de sistema com efeito sobre comportamento, aumento de autonomia, mudança de fornecedor, inclusão de nova população ou nova finalidade. Mudança crítica inclui qualquer alteração capaz de afetar direitos, segurança ou conformidade de forma significativa.

Para cada categoria, o programa estabelece quem precisa revisar. Assim, a organização evita submeter toda atualização ao comitê e, ao mesmo tempo, impede que mudanças materiais entrem em produção sem avaliação.

K.3 Plano de evidências

Para cada sistema de médio ou alto risco, defina previamente quais evidências precisam ser preservadas. O pacote mínimo pode incluir avaliação de risco, fluxo de dados, base legal, contrato, documentação de fornecedor,

testes, aprovação, política aplicável, logs, reclamações, incidentes e revisões periódicas.

A retenção deve observar necessidade e legislação. Nem sempre é preciso conservar conteúdo integral de prompts por longos períodos. Em alguns casos, metadados, hash, identificador de versão e fatores principais são suficientes. Em outros, especialmente quando a decisão pode ser contestada, maior detalhamento será necessário. O desenho deve equilibrar minimização de dados e capacidade de prova.

Evidência deve ser acessível. Documentos espalhados em e-mails pessoais ou pastas sem controle de versão tornam o processo frágil. Um repositório corporativo com permissões e nomenclatura padronizada facilita auditoria e resposta a incidentes.

K.4 Registro de revisão humana

Quando a empresa afirma que existe supervisão humana, deve ser capaz de demonstrá-la. O registro pode indicar quem revisou, qual recomendação o sistema produziu, qual decisão final foi tomada e, quando houver divergência, motivo resumido. Não é necessário registrar justificativa extensa para cada caso de baixo impacto, mas sistemas críticos precisam de evidência suficiente para mostrar que o humano tinha participação real.

Métricas agregadas também são úteis: percentual de recomendações aceitas, rejeitadas ou modificadas; tempo médio de revisão; e taxa de reversão após contestação. Uma taxa de aceitação de 99,9% pode indicar excelente modelo ou revisão meramente formal; a organização deve investigar o contexto.

K.5 Evidências de testes

Relatórios de teste devem registrar conjunto utilizado, data, versão, métricas e critério de aprovação. Screenshots isolados não substituem resultados estruturados. Para modelos generativos, conserve suites de prompts representativos, categorias de risco, avaliação humana quando utilizada e resultados de red teaming.

Testes devem ser repetíveis dentro do possível. Quando o fornecedor oferece modelo não determinístico e muda infraestrutura, a reprodução exata pode não ser viável; ainda assim, registrar versão, parâmetros disponíveis e data permite reconstrução razoável.

O jurídico deve participar da definição do que é material, enquanto equipes técnicas definem método. A colaboração evita relatórios tecnicamente sofisticados que não respondem à pergunta jurídica principal.

K.6 Revisão periódica

A ficha mestre deve possuir data de próxima revisão. Sistemas de baixo risco podem ter ciclo anual; sistemas relevantes podem exigir revisão semestral, trimestral ou por evento. Gatilhos extraordinários incluem incidente, reclamação recorrente, atualização de modelo, mudança de finalidade, nova categoria de dados, expansão para menores ou entrada em setor regulado.

A revisão deve terminar com decisão explícita: manter, manter com ação corretiva, restringir, suspender ou desativar. Ações precisam de responsável e prazo. Sem decisão, a revisão vira ritual documental.

K.7 Checklist de fechamento

Antes de considerar a documentação completa, confirme: o sistema possui dono; a finalidade está atualizada; o modelo e a versão são conhecidos; dados e transferências estão mapeados; riscos e controles possuem responsáveis; testes foram aprovados; revisão humana é real quando necessária; logs permitem reconstrução proporcional; contratos refletem a arquitetura; mudanças materiais geram reavaliação; incidentes e reclamações alimentam monitoramento; e existe autoridade clara para interromper o uso.

Esse registro mestre transforma governança de IA em capacidade demonstrável. Em vez de procurar informações depois de um problema, a organização mantém desde o início as evidências necessárias para explicar por que o sistema existe, como foi controlado e quem tomou cada decisão relevante.

Apêndice L — Rotina de atualização normativa

A governança jurídica de IA precisa prever revisão periódica do próprio marco regulatório. Recomenda-se que o jurídico mantenha calendário semestral para verificar alterações na LGPD, resoluções e orientações da ANPD, normas setoriais, decisões relevantes dos tribunais e andamento do PL 2.338/2023 ou de eventual texto que o substitua.

A revisão deve comparar a legislação nova com o inventário de sistemas da empresa. Não basta registrar que uma norma foi publicada: é preciso identificar quais

processos, contratos, produtos, políticas e avaliações de impacto precisam ser alterados. Mudanças sobre biometria, crianças e adolescentes, transferências internacionais, decisões automatizadas ou conteúdo sintético devem acionar análise específica dos sistemas afetados.

Para cada atualização, registre a fonte oficial, data de vigência, responsável pela análise, sistemas impactados, ações necessárias e prazo. Quando a norma ainda for projeto de lei, mantenha-a separada das obrigações vigentes para evitar antecipar como definitivo um texto sujeito a mudanças. Essa disciplina reduz retrabalho e permite demonstrar que a empresa acompanha de forma contínua a evolução regulatória da inteligência artificial no Brasil.

Conclusão

Regular inteligência artificial dentro de uma empresa não significa impedir experimentação. Significa criar condições para que a experimentação possa escalar sem transformar incertezas técnicas em passivos jurídicos. O ponto de equilíbrio não está em exigir a mesma documentação para todos os usos nem em confiar que contratos e avisos genéricos resolvam qualquer risco.

A abordagem mais robusta combina cinco capacidades. A primeira é visibilidade: saber quais sistemas existem, que dados usam e quem responde por eles. A segunda é proporcionalidade: dedicar maior esforço aos usos que realmente podem afetar direitos, segurança ou serviços essenciais. A terceira é evidência: testar, registrar, monitorar e conservar documentação suficiente para

explicar decisões. A quarta é integração: conectar jurídico, tecnologia, privacidade, segurança, negócio e auditoria. A quinta é adaptação: reconhecer que modelos, fornecedores e normas mudam.

O Brasil chega a 2026 com um conjunto normativo mais denso do que muitas organizações percebem. A LGPD continua sendo eixo central para sistemas baseados em dados pessoais; a proteção de dados ganhou status constitucional; a ANPD tornou-se agência reguladora; o ECA Digital criou deveres concretos no ambiente online; e normas civis, consumeristas, trabalhistas, autorais e concorrenciais já alcançam muitos efeitos de sistemas algorítmicos. Ao mesmo tempo, o PL 2.338/2023 permanece em construção legislativa.

A empresa que espera uma lei única para começar a governar IA está atrasada. A empresa que tenta prever cada artigo futuro também pode desperdiçar esforço. O caminho mais resiliente é desenvolver capacidades permanentes: inventário, avaliação de impacto, supervisão, segurança, transparência, contratos, documentação e auditoria. Essas capacidades são úteis sob o direito vigente e continuarão úteis quando o marco legal brasileiro for finalmente definido.

Referências legislativas e institucionais

BRASIL. Constituição da República Federativa do Brasil de 1988.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Inclui a proteção de dados pessoais entre os direitos e garantias fundamentais.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Lei da Propriedade Industrial.

BRASIL. Lei nº 9.609, de 19 de fevereiro de 1998. Lei de Software.

BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. Lei de Direitos Autorais.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil.

BRASIL. Lei nº 12.529, de 30 de novembro de 2011. Lei de Defesa da Concorrência.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.

BRASIL. Lei nº 14.133, de 1º de abril de 2021. Lei de Licitações e Contratos Administrativos.

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Estatuto Digital da Criança e do Adolescente.

BRASIL. Lei nº 15.352, de 25 de fevereiro de 2026. Transforma a ANPD em agência reguladora e altera a LGPD.

BRASIL. Decreto nº 12.622, de 17 de setembro de 2025. Designa a ANPD como autoridade administrativa autônoma de proteção de crianças e adolescentes em ambientes digitais.

BRASIL. Decreto nº 12.880, de 18 de março de 2026. Regulamenta o ECA Digital e institui política nacional de promoção e proteção de direitos de crianças e adolescentes no ambiente digital.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Regulamento de Comunicação de Incidente de Segurança.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 19, de 23 de agosto de 2024. Regulamento de Transferência Internacional de Dados e cláusulas-padrão contratuais.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Agenda Regulatória 2025-2026, com item específico sobre Inteligência Artificial e art. 20 da LGPD.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Radar Tecnológico nº 3 — Inteligência Artificial Generativa.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. Radar Tecnológico nº 6 — Deepfakes. 2026.

CÂMARA DOS DEPUTADOS. PL 2.338/2023. Situação consultada em 6 de agosto de 2026: aguardando parecer na Comissão Especial sobre Inteligência Artificial.

SENADO FEDERAL. PL 2.338/2023. Texto aprovado pelo Plenário em 10 de dezembro de 2024 e remetido à Câmara dos Deputados em 17 de março de 2025.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. Plano Brasileiro de Inteligência Artificial 2024-2028.

Referências técnicas e internacionais para governança

NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology, 2023.

NIST. Generative Artificial Intelligence Profile. Companion resource to the AI Risk Management Framework.

ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system.

ISO/IEC 23894:2023. Information technology — Artificial intelligence — Guidance on risk management.

OECD. OECD Principles on Artificial Intelligence, atualizados em 2024.

UNESCO. Recommendation on the Ethics of Artificial Intelligence, 2021.

ISO/IEC 22989:2022. Information technology — Artificial intelligence — Artificial intelligence concepts and terminology.

ISO/IEC 23053:2022. Framework for Artificial Intelligence Systems Using Machine Learning.

ISO/IEC 5338:2023. Information technology — Artificial intelligence — AI system life cycle processes.

ISO/IEC TR 24027:2021. Information technology — Artificial intelligence — Bias in AI systems and AI aided decision making.

UNIÃO EUROPEIA. Regulation (EU) 2024/1689 — Artificial Intelligence Act.

CONSELHO DA EUROPA. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 2024.