RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

Direito e tecnologia em diálogo: uma análise conjunta dos impactos da inteligência artificial generativa na privacidade e segurança da informação no contexto corporativo

Law and Technology in Dialogue: A Joint Analysis of the Impacts of Generative Artificial Intelligence on Privacy and Information Security in the Corporate Context

Derecho y tecnología en diálogo: un análisis conjunto de los impactos de la inteligencia artificial generativa en la privacidad y la seguridad de la información en el contexto corporativo

Manoel Pereira de Lima Junior
Juliana Beatriz Moraes Miura

Resumo:
A rápida expansão da Inteligência Artificial Generativa (IAG) no ambiente corporativo impõe novos desafios à proteção de dados pessoais, à segurança da informação e à governança organizacional. O presente artigo analisa, sob perspectiva interdisciplinar, os impactos jurídicos, tecnológicos e filosóficos decorrentes do uso de plataformas de IAG pelas organizações, com ênfase na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), nos riscos de vazamento de informações confidenciais e nos desafios do fenômeno denominado Shadow AI. A investigação articula fundamentos do Direito Digital com princípios de Segurança da Informação, normas técnicas reconhecidas internacionalmente (ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, OWASP LLM Top 10) e referenciais filosóficos de Michel Foucault, Zygmunt Bauman, Byung-Chul Han e Shoshana Zuboff. Como resultado, demonstra-se que a proteção efetiva dos ativos informacionais corporativos exige uma abordagem integrada entre pessoas, processos, tecnologia e cultura organizacional, superando a dicotomia entre inovação tecnológica e conformidade jurídica. Propõe-se um modelo de governança responsável da IAG fundamentado em princípios de Privacy by Design, Zero Trust, gestão de riscos e ética digital.

Palavras-chave:
Inteligência Artificial Generativa. LGPD. Segurança da Informação. Shadow AI. Governança de Dados. Privacidade. Cibersegurança Corporativa.

Abstract:
The rapid expansion of Generative Artificial Intelligence (GAI) in the corporate environment poses new challenges to personal data protection, information security, and organizational governance. This article analyzes, from an interdisciplinary perspective, the legal, technological, and philosophical impacts arising from the use of GAI platforms by organizations, with emphasis on Brazil's General Data Protection Law (LGPD – Law No. 13,709/2018), the risks of confidential information leakage, and the challenges posed by the phenomenon known as Shadow AI. The investigation articulates principles of Digital Law with Information Security standards, internationally recognized technical norms (ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, OWASP LLM Top 10), and philosophical frameworks drawn from Michel Foucault, Zygmunt Bauman, Byung-Chul Han, and Shoshana Zuboff. As a result, it is demonstrated that the effective protection of corporate informational assets requires an integrated approach encompassing people, processes, technology, and organizational culture, transcending the dichotomy between technological innovation and legal compliance. A model of responsible GAI governance is proposed, grounded in Privacy by Design, Zero Trust, risk management, and digital ethics.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

Keywords:
Generative Artificial Intelligence. LGPD. Information Security. Shadow AI. Data Governance. Privacy. Corporate Cybersecurity.

Resumen:
La rápida expansión de la Inteligencia Artificial Generativa (IAG) en el entorno corporativo impone nuevos desafíos a la protección de datos personales, la seguridad de la información y la gobernanza organizacional. El presente artículo analiza, desde una perspectiva interdisciplinaria, los impactos jurídicos, tecnológicos y filosóficos derivados del uso de plataformas de IAG por las organizaciones, con énfasis en la Ley General de Protección de Datos de Brasil (LGPD – Ley n.º 13.709/2018), en los riesgos de filtración de información confidencial y en los desafíos del fenómeno denominado Shadow AI. La investigación articula fundamentos del Derecho Digital con principios de Seguridad de la Información, normas técnicas reconocidas internacionalmente (ISO/IEC 27001, ISO/IEC 42001, NIST AI RMF, OWASP LLM Top 10) y referentes filosóficos de Michel Foucault, Zygmunt Bauman, Byung-Chul Han y Shoshana Zuboff. Como resultado, se demuestra que la protección efectiva de los activos informacionales corporativos exige un enfoque integrado entre personas, procesos, tecnología y cultura organizacional, superando la dicotomía entre innovación tecnológica y conformidad jurídica. Se propone un modelo de gobernanza responsable de la IAG fundamentado en principios de Privacy by Design, Zero Trust, gestión de riesgos y ética digital.

Palabras clave:
Inteligencia Artificial Generativa. LGPD. Seguridad de la Información. Shadow AI. Gobernanza de Datos. Privacidad. Ciberseguridad Corporativa.

INTRODUÇÃO

A Inteligência Artificial Generativa (IAG)[1] emergiu como uma das mais disruptivas inovações tecnológicas do século XXI. Modelos de linguagem de grande escala (Large Language Models – LLMs), como o GPT-4 da OpenAI, o Gemini do Google e o Claude da Anthropic, tornaram-se acessíveis ao público em geral e, de forma acelerada, penetraram os ambientes corporativos, transformando processos de trabalho, comunicação organizacional, análise jurídica, desenvolvimento de software e gestão estratégica (BOMMASANI et al., 2021).

Essa penetração tecnológica, embora portadora de inegáveis benefícios em produtividade e inovação, carrega consigo vetores de risco que transcendem as dimensões puramente técnicas. No âmbito jurídico, a utilização de plataformas públicas de IAG por colaboradores e organizações suscita questões fundamentais sobre o tratamento de dados pessoais, a responsabilidade civil e administrativa dos agentes de tratamento e a conformidade

[1]O termo "Inteligência Artificial Generativa" (IAG) designa sistemas de IA capazes de produzir conteúdo novo — texto, imagem, áudio, código — a partir de padrões aprendidos em grandes volumes de dados. Distingue-se da IA discriminativa, que classifica ou prediz categorias em dados existentes.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

com o marco regulatório brasileiro de proteção de dados — a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018). Esse marco normativo foi inspirado no Regulamento Geral de Proteção de Dados europeu (GDPR)[2] e representa o principal instrumento jurídico de proteção da privacidade no Brasil.

No campo da segurança da informação, a adoção não gerenciada de ferramentas de IAG por colaboradores — fenômeno denominado Shadow AI — representa uma ameaça à confidencialidade, integridade e disponibilidade dos ativos informacionais das organizações. Dados estratégicos, segredos industriais, informações de clientes e propriedade intelectual podem ser inadvertidamente inseridos em modelos treinados e mantidos por terceiros, com consequências potencialmente irreversíveis (GARTNER, 2023).

Diante desse cenário, o presente artigo propõe como problema de pesquisa: como as organizações podem equilibrar os benefícios proporcionados pela Inteligência Artificial Generativa com a necessidade de proteção jurídica dos dados, segurança da informação e preservação de seus ativos estratégicos?

A justificativa para esta investigação reside na urgência e atualidade do tema. O Brasil, a despeito de possuir uma legislação de proteção de dados de envergadura comparável ao GDPR europeu, carece ainda de regulamentação específica sobre o uso de IAG, o que torna indispensável a análise integrada dos marcos normativos existentes e das melhores práticas internacionais. A execução de tais tarefas cabe primariamente à Autoridade Nacional de Proteção de Dados (ANPD)[3], que vem gradualmente ampliando sua atuação regulatória nessa área.

O objetivo geral desta pesquisa é analisar os impactos jurídicos, tecnológicos e filosóficos da Inteligência Artificial Generativa sobre a privacidade e a segurança da informação no contexto corporativo. Os objetivos específicos são: (a) examinar o arcabouço normativo da LGPD e sua aplicação ao uso de IAG; (b) identificar os principais riscos de segurança da informação associados ao uso corporativo de IAG; (c) analisar o fenômeno Shadow AI e seus desafios de governança; (d) articular fundamentos filosóficos sobre poder,

[2]O GDPR (General Data Protection Regulation), Regulamento (UE) 2016/679, entrou em vigor em 25 de maio de 2018 e é considerado o padrão global de referência em proteção de dados pessoais, tendo influenciado diretamente a elaboração da LGPD brasileira.

[3]A ANPD foi criada pelo Decreto nº 10.474/2020 como autarquia de natureza especial vinculada à Presidência da República, dotada de autonomia técnica e decisória, patrimônio próprio e receitas específicas. É responsável por zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados e fiscalizar e aplicar sanções.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

dados e vigilância ao cenário da IAG; e (e) propor diretrizes para uma governança responsável da IAG no ambiente corporativo.

A metodologia adotada é bibliográfica, exploratória e qualitativa, fundamentada em revisão de literatura científica, legislação aplicável, normas técnicas e documentos institucionais, conforme delineado na seção metodológica específica.

EVOLUÇÃO DA INTELIGÊNCIA ARTIFICIAL GENERATIVA NO AMBIENTE CORPORATIVO

A trajetória da Inteligência Artificial percorre décadas de avanços científicos e rupturas paradigmáticas. Desde os primeiros modelos simbólicos e sistemas especialistas das décadas de 1950 e 1960, passando pelas redes neurais artificiais e pelo aprendizado de máquina supervisionado, chegou-se ao paradigma do aprendizado profundo (deep learning), que revolucionou as capacidades computacionais de processamento de linguagem natural, visão computacional e geração de conteúdo (GOODFELLOW; BENGIO; COURVILLE, 2016). O marco transformador para a IAG foi a introdução da arquitetura Transformer[4], proposta por Vaswani et al. (2017) no artigo seminal "Attention Is All You Need".

Essa arquitetura possibilitou o treinamento de modelos em escala sem precedentes, culminando no desenvolvimento dos LLMs que caracterizam a geração atual de ferramentas de IAG. O processo de ajuste fino por Reinforcement Learning from Human Feedback (RLHF)[5] tornou esses modelos mais alinhados às expectativas dos usuários. O lançamento público do ChatGPT, em novembro de 2022, representou um ponto de inflexão: em menos de cinco dias, a plataforma atingiu um milhão de usuários, e em dois meses, cem milhões — velocidade de adoção sem precedentes na história da tecnologia de consumo (OPENAI, 2023).

No ambiente corporativo, a penetração da IAG ocorreu em múltiplas dimensões. Departamentos jurídicos passaram a utilizar LLMs para revisão de contratos e pesquisa jurisprudencial; equipes de tecnologia adotaram ferramentas de geração de código; áreas de

[4]O modelo de arquitetura Transformer, introduzido por Vaswani et al. (2017), utiliza mecanismos de atenção (attention mechanisms) que permitem ao modelo ponderar a relevância de diferentes partes do texto de entrada ao gerar cada token de saída. Essa arquitetura supera limitações das redes recorrentes (RNNs) e permite paralelização do treinamento em escala massiva.

[5]O RLHF (Reinforcement Learning from Human Feedback) é uma técnica de ajuste fino de LLMs na qual avaliadores humanos classificam respostas do modelo, e essa classificação é utilizada para treinar um modelo de recompensa que orienta o aprendizado por reforço do LLM. O RLHF foi fundamental para tornar modelos como o ChatGPT mais alinhados às expectativas e preferências dos usuários.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

marketing exploraram a criação automatizada de conteúdo; e gestores recorreram às ferramentas para síntese de relatórios e suporte à tomada de decisão (MCKINSEY GLOBAL INSTITUTE, 2023).

Segundo relatório do McKinsey Global Institute (2023), a IAG tem potencial de automatizar atividades que correspondem a 60% a 70% do tempo de trabalho atual dos colaboradores em diversas funções cognitivas. Esse potencial transformador, contudo, coexiste com riscos que as organizações, em sua maioria, ainda não estão preparadas para gerenciar adequadamente.

A Gartner (2023) identificou que, até 2025, mais de 80% das empresas terão implantado aplicações de IAG em seus processos — mas menos de 30% terão estabelecido políticas e controles adequados para mitigar os riscos associados. Essa assimetria entre adoção e governança configura o núcleo do problema investigado neste artigo.

DADOS COMO NOVO ATIVO ESTRATÉGICO DAS ORGANIZAÇÕES

A ascensão da economia digital transformou radicalmente a natureza e o valor dos dados. Antes tratados como subproduto das operações organizacionais, os dados tornaram-se o principal ativo estratégico das empresas do século XXI. A expressão popularmente atribuída ao economista britânico Clive Humby — "data is the new oil" — sintetiza, ainda que de forma simplificada, a centralidade que a informação estruturada e não estruturada adquiriu na criação de valor econômico (THE ECONOMIST, 2017).

No contexto corporativo, os dados assumem múltiplas categorias estratégicas: dados de clientes (histórico de compras, preferências, dados financeiros), dados de colaboradores (informações pessoais, dados de desempenho, registros de saúde), propriedade intelectual (código-fonte, fórmulas, processos produtivos), informações financeiras confidenciais e segredos comerciais. Cada uma dessas categorias representa, simultaneamente, um ativo competitivo e um passivo jurídico — cuja exposição não autorizada pode gerar danos patrimoniais, reputacionais e legais de magnitude significativa.

A valorização dos dados como ativo estratégico tem implicações diretas para a governança corporativa. O Conselho de Administração e a Alta Gestão passaram a reconhecer que a proteção dos dados não é questão exclusivamente técnica ou de conformidade regulatória, mas dimensão fundamental da estratégia de negócios e da gestão de riscos (WORLD ECONOMIC FORUM, 2020).

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

Nessa perspectiva, a chegada da IAG ao ambiente corporativo cria um paradoxo: as mesmas ferramentas que permitem extrair valor dos dados com eficiência sem precedentes são, simultaneamente, potenciais vetores de vazamento e exposição não autorizada dessas informações. Quando um colaborador insere dados corporativos sensíveis em uma plataforma pública de IAG para obter análises, sugestões ou sínteses, ele pode estar transferindo esse ativo estratégico para os servidores de terceiros — com consequências jurídicas e competitivas potencialmente devastadoras.

A classificação e o inventário de dados corporativos, portanto, tornam-se pressupostos indispensáveis de qualquer estratégia de governança da IAG. Sem saber quais dados existem, onde residem e qual é o seu grau de sensibilidade, as organizações não conseguem estabelecer controles adequados sobre o que pode ou não ser processado por ferramentas externas de inteligência artificial (ISO/IEC 27001, 2022).

ANÁLISE JURÍDICA: LGPD, PRIVACIDADE E RESPONSABILIDADE EMPRESARIAL

A Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 14 de agosto de 2018 e vigente desde setembro de 2020, representa o principal marco regulatório brasileiro para o tratamento de dados pessoais. Inspirada no Regulamento Geral de Proteção de Dados da União Europeia (GDPR – Regulation 2016/679), a LGPD estabelece princípios, direitos dos titulares, obrigações dos agentes de tratamento e sanções administrativas aplicáveis pelo órgão regulador — a ANPD.

O artigo 6º da LGPD elenca os princípios que devem nortear o tratamento de dados pessoais, com especial relevância para o contexto da IAG: finalidade (tratamento para propósitos legítimos, específicos, explícitos e informados ao titular); adequação (compatibilidade com as finalidades informadas); necessidade (limitação ao mínimo necessário para a finalidade); livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas (BRASIL, 2018, art. 6º).

No que concerne às bases legais para o tratamento de dados pessoais, o artigo 7º da LGPD enumera as hipóteses que autorizam o tratamento, entre as quais se destacam o consentimento do titular, o legítimo interesse do controlador e o cumprimento de obrigação

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

legal. Para dados pessoais sensíveis[6] — categoria que abrange dados sobre saúde, orientação sexual, convicções religiosas, dados genéticos e biométricos —, o artigo 11 da LGPD impõe restrições ainda mais rigorosas, exigindo, em regra, o consentimento específico e destacado do titular.

A inserção de dados pessoais em plataformas públicas de IAG sem base legal adequada, sem cláusulas contratuais específicas com os fornecedores e sem avaliação de impacto à proteção de dados pode configurar infração à LGPD sujeita a sanções que incluem advertência, multa simples de até 2% do faturamento da empresa no Brasil (limitada a R$ 50 milhões por infração), multa diária, publicização da infração, bloqueio ou eliminação dos dados pessoais envolvidos (BRASIL, 2018, art. 52).

A responsabilidade civil das organizações no contexto da IAG apresenta dimensões particularmente complexas. O artigo 42 da LGPD dispõe que o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo ao titular, é obrigado a repará-lo. A questão da distribuição de responsabilidade entre controlador (a organização que define as finalidades do tratamento) e operador (o fornecedor da plataforma de IAG) é tema que demanda atenção especial dos contratos de prestação de serviços.

Nessa perspectiva, o fenômeno Shadow AI pode fazer com que a organização assuma a posição de controladora de tratamentos de dados que sequer tem ciência de estar realizando. Isso evidencia a necessidade de políticas claras, mecanismos de controle e programas de conscientização interna.

A transferência internacional de dados representa outra dimensão jurídica crítica. Os principais fornecedores de plataformas públicas de IAG — OpenAI, Google, Microsoft, Anthropic — são empresas estadunidenses, cujos servidores residem, em grande medida, fora do território brasileiro. O artigo 33 da LGPD condiciona a transferência internacional de dados pessoais à existência de adequado nível de proteção no país de destino (a ser reconhecido pela ANPD), à existência de garantias contratuais específicas ou a outras hipóteses taxativas (ANPD, 2023).

A ANPD tem avançado na publicação de orientações relevantes para o contexto da IAG. Contudo, regulamentação específica sobre IA ainda se encontra em desenvolvimento no âmbito

[6]Dados pessoais sensíveis são definidos pelo art. 5º, II, da LGPD como aqueles "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

do processo legislativo brasileiro — notadamente o Projeto de Lei nº 2.338/2023[7], que tramita no Senado Federal e propõe um marco regulatório específico para a inteligência artificial no Brasil.

No âmbito da responsabilidade administrativa, a ANPD pode instaurar processo administrativo sancionador contra organizações que utilizem plataformas de IAG sem observância dos requisitos da LGPD. A demonstração da adoção de medidas técnicas e organizacionais de segurança — e a existência de um programa de governança em privacidade robusto — são fatores que podem atenuar a responsabilidade dos agentes de tratamento (BRASIL, 2018, art. 50).

ANÁLISE TECNOLÓGICA: RISCOS, VULNERABILIDADES E CONTROLES DE SEGURANÇA

Do ponto de vista da segurança da informação, a Inteligência Artificial Generativa representa um vetor de risco multidimensional que desafia os modelos tradicionais de proteção corporativa. Para compreender esses riscos adequadamente, é necessário analisar o funcionamento técnico dos LLMs e as vulnerabilidades que lhes são inerentes, bem como os riscos associados ao uso corporativo não gerenciado dessas ferramentas.

Os LLMs são treinados em vastos conjuntos de dados textuais utilizando técnicas de aprendizado profundo baseadas na arquitetura Transformer. Uma vez treinados, esses modelos são ajustados com dados adicionais e técnicas como o RLHF para alinhar seu comportamento às expectativas dos usuários. O processo de inferência — a geração de respostas em tempo real — ocorre nos servidores do provedor, o que significa que todo prompt enviado pelo usuário é transmitido e processado na infraestrutura de terceiros (OUYANG et al., 2022).

O OWASP (Open Web Application Security Project) publicou, em 2023, o "OWASP Top 10 for Large Language Model Applications", documento que cataloga as principais vulnerabilidades de segurança dos sistemas baseados em LLMs. As mais relevantes para o contexto corporativo incluem: Prompt Injection (manipulação do comportamento do modelo por meio de instruções maliciosas inseridas nos prompts); vazamento de dados sensíveis contidos no contexto da conversa; treinamento com dados envenenados (data poisoning);

[7]O Projeto de Lei nº 2.338/2023, de autoria do Senador Rodrigo Pacheco, propõe um marco regulatório abrangente para a inteligência artificial no Brasil, baseado em abordagem de risco similar ao EU AI Act. O PL classifica os sistemas de IA em três categorias de risco — inaceitável, alto e limitado — e estabelece obrigações diferenciadas para cada categoria, incluindo avaliações de conformidade, transparência e supervisão humana.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

geração de conteúdo não confiável — as chamadas "alucinações"[8] — com potencial de causar danos; e excessiva dependência de saídas do modelo sem validação humana adequada (OWASP, 2023).

No que concerne ao risco de exposição de informações confidenciais, estudos realizados por empresas de segurança como a Cyberhaven e a LayerX Security (2023) revelaram que uma parcela significativa dos dados inseridos por colaboradores em plataformas públicas de IAG contém informações corporativas sensíveis. O episódio da Samsung[9], em março de 2023, tornou-se emblemático: engenheiros da empresa inseriram código-fonte proprietário no ChatGPT para depuração, resultando na potencial exposição de segredos industriais (BUSINESSINSIDER, 2023).

A norma ISO/IEC 27001:2022, que especifica os requisitos para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI), oferece o arcabouço estrutural para a gestão desses riscos. O Anexo A da norma enumera controles de segurança organizados em quatro categorias — organizacionais, humanos, físicos e tecnológicos — que, aplicados ao contexto da IAG, implicam a necessidade de políticas de uso aceitável, treinamento de colaboradores, avaliação de fornecedores, controles técnicos de Data Loss Prevention (DLP) e gestão de vulnerabilidades específicas de aplicações baseadas em IA (ISO/IEC 27001, 2022). A norma ISO/IEC 42001:2023[10] complementa esse arcabouço com requisitos específicos para sistemas de gestão de inteligência artificial.

A arquitetura Zero Trust[11], formalizada pelo NIST na publicação especial SP 800-207 (2020), baseia-se no princípio de que nenhum usuário, dispositivo ou serviço deve ser

---

[8]O fenômeno das "alucinações" em LLMs refere-se à geração de informações factualmente incorretas, referências bibliográficas inexistentes ou afirmações inverificáveis apresentadas com aparente confiança pelo modelo. Esse fenômeno é consequência da natureza estatística dos LLMs, que geram tokens com base em probabilidades, sem acesso a um modelo interno de verdade ou verificação factual.

[9]Em março de 2023, funcionários da Samsung Semiconductor inseriram código-fonte proprietário no ChatGPT em ao menos três ocasiões distintas: para depuração de código de banco de dados, para verificação de código relacionado a equipamentos de semicondutores e para converter notas de reunião em apresentação. A Samsung proibiu posteriormente o uso de ferramentas de IA generativa externas em seus dispositivos corporativos.

[10]A ISO/IEC 42001:2023 é a primeira norma internacional de sistema de gestão especificamente dedicada à inteligência artificial. Estabelece requisitos e fornece orientações para organizações que desenvolvem, fornecem ou utilizam sistemas de IA de forma responsável, abordando aspectos como governança, gestão de riscos, impacto sobre os direitos humanos, transparência e melhoria contínua.

[11]A Zero Trust Architecture (ZTA), conforme definida pelo NIST SP 800-207, baseia-se em três princípios fundamentais: (1) todas as fontes de dados e serviços computacionais são considerados recursos; (2) toda

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

considerado confiável por padrão. Aplicada ao contexto da IAG, implica que o acesso a ferramentas de IAG deve ser concedido com base em políticas explícitas de autorização, verificação contínua de identidade e monitoramento de comportamento, com o mínimo de privilégios necessários para a função desempenhada.

As soluções de Cloud Access Security Broker (CASB)[12] e de Data Loss Prevention (DLP) completam o arsenal técnico disponível para a mitigação dos riscos da IAG corporativa. Por fim, a implantação de ambientes privados e seguros para IA corporativa — como instâncias on-premises ou em nuvem privada de modelos de linguagem — permite que as organizações usufruam dos benefícios da IAG sem expor dados sensíveis a terceiros (MICROSOFT, 2023).

SHADOW AI E OS NOVOS DESAFIOS DE GOVERNANÇA

O conceito de Shadow IT, referente ao uso de sistemas de tecnologia da informação sem aprovação explícita do departamento de TI corporativo, é fenômeno amplamente estudado na literatura de gestão de TI desde a década de 1980 (SILIC; BACK, 2014). Com a disseminação das plataformas públicas de IAG, emergiu uma manifestação contemporânea e particularmente perigosa desse fenômeno: o Shadow AI, caracterizado pelo uso de ferramentas de IAG por colaboradores sem o conhecimento, a aprovação ou o controle da organização.

O Shadow AI representa um desafio de governança de natureza singular em relação ao Shadow IT tradicional. Primeiramente, a barreira de entrada é praticamente inexistente: ferramentas de IAG de alto poder computacional estão disponíveis gratuitamente ou a custo marginal, acessíveis por meio de qualquer dispositivo conectado à internet, sem necessidade de instalação de software ou configuração de rede. Em segundo lugar, as consequências potenciais são imediatas e possivelmente irreversíveis: dados inseridos em plataformas externas de IAG podem ser utilizados para retreinamento dos modelos, tornando virtualmente impossível a sua recuperação posterior.

Pesquisa conduzida pela Cyberhaven (2023) analisou o comportamento de mais de 1,6 milhão de colaboradores e constatou que 11% dos dados inseridos em ferramentas de IAG eram

comunicação é protegida independentemente da localização na rede; (3) o acesso a recursos individuais é concedido por sessão, com verificação contínua de identidade e contexto.

[12]O Cloud Access Security Broker (CASB) é uma solução de segurança posicionada entre os usuários corporativos e os provedores de serviços em nuvem, que aplica políticas de segurança ao tráfego de dados em tempo real. As principais funções de um CASB incluem visibilidade do uso de serviços em nuvem, controle de acesso, proteção contra ameaças e conformidade regulatória.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

corporativos sensíveis, com destaque para código-fonte, dados financeiros, estratégias de negócios e comunicações internas. Estudo da LayerX Security (2023) revelou que apenas 8% das organizações pesquisadas possuíam controles efetivos para monitorar e controlar o uso de IAG por seus colaboradores.

Os vetores de risco do Shadow AI podem ser categorizados em três dimensões: (a) risco de confidencialidade, pela exposição de informações sensíveis e propriedade intelectual a provedores externos sem base contratual adequada; (b) risco jurídico, pelo potencial de violação da LGPD e de cláusulas de confidencialidade contratuais com clientes e parceiros; e (c) risco de integridade e confiabilidade, pela tomada de decisões baseadas em outputs de modelos não validados, potencialmente imprecisos ou enviesados.

Do ponto de vista da governança, o enfrentamento do Shadow AI requer uma abordagem simultaneamente preventiva, detectiva e corretiva. As medidas preventivas incluem o estabelecimento de políticas claras de uso aceitável de ferramentas de IAG, comunicadas e treinadas a todos os colaboradores; a disponibilização de alternativas corporativas aprovadas; e a criação de processos ágeis de avaliação e homologação de novas ferramentas. As medidas detectivas incluem o monitoramento de tráfego de rede para identificar o acesso a plataformas de IAG não homologadas. As medidas corretivas envolvem a resposta a incidentes, a avaliação de danos e a adequação dos processos e controles.

É fundamental que a abordagem de governança do Shadow AI não seja percebida pelos colaboradores como meramente restritiva ou punitiva. A literatura sobre gestão da mudança e comportamento organizacional demonstra que proibições absolutas, sem alternativas adequadas, tendem a aumentar a resistência dos colaboradores e a impulsionar comportamentos clandestinos mais sofisticados (SILIC; BACK, 2014). A governança efetiva do Shadow AI, portanto, deve equilibrar controle e habilitação.

DIÁLOGO ENTRE DIREITO E TECNOLOGIA

A relação entre Direito e Tecnologia tem sido historicamente marcada por assimetrias temporais: a regulação jurídica tende a chegar após a consolidação dos fenômenos tecnológicos, resultando em lacunas normativas que os agentes econômicos exploram em detrimento de indivíduos e da coletividade. No contexto da IAG, essa defasagem regulatória é particularmente pronunciada.

O diálogo entre Direito e Tecnologia no campo da IAG exige a superação de barreiras epistemológicas significativas. Os juristas, em sua formação tradicional, não estão equipados

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

para compreender os mecanismos técnicos dos LLMs; os engenheiros e cientistas de dados, por sua vez, frequentemente desconhecem os requisitos legais e as implicações jurídicas de suas decisões de design. A construção de pontes entre esses domínios do conhecimento é condição sine qua non para o desenvolvimento de uma governança efetiva da IAG.

No plano normativo brasileiro, a LGPD fornece o principal substrato jurídico para o tratamento dos riscos da IAG ao patrimônio informacional das organizações. O artigo 20 da LGPD, que garante ao titular o direito de solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, representa uma norma de particular relevância para o contexto da IAG aplicada a processos decisórios corporativos.

No plano internacional, o Regulamento de Inteligência Artificial da União Europeia (EU AI Act)[13], aprovado em 2024, representa o primeiro marco regulatório abrangente especificamente voltado para sistemas de IA. Embora não vinculante para o Brasil, o AI Act exerce influência sobre a regulação global de IA e serve como referência importante para o processo legislativo brasileiro (EUROPEAN PARLIAMENT, 2024).

A perspectiva interdisciplinar entre Direito e Tecnologia revela que a proteção jurídica dos dados no contexto da IAG não pode ser reduzida à conformidade formal com a LGPD. Nesse sentido, o princípio do Privacy by Design[14], articulado por Ann Cavoukian (2009) e incorporado ao arcabouço normativo do GDPR europeu e, de forma implícita, ao artigo 46 da LGPD, estabelece que a proteção de dados deve ser incorporada ao design dos sistemas e processos desde a sua concepção, e não tratada como elemento externo de conformidade.

REFLEXÕES FILOSÓFICAS SOBRE PODER, DADOS E INTELIGÊNCIA ARTIFICIAL

A análise dos impactos da IAG sobre a privacidade e a segurança da informação no contexto corporativo não pode prescindir de uma fundamentação filosófica que situe o

[13]O EU AI Act (Regulamento (UE) 2024/1689) classifica como sistemas de IA de risco inaceitável, proibidos na União Europeia: sistemas de pontuação social por autoridades públicas; exploração de vulnerabilidades de grupos específicos; identificação biométrica remota em tempo real em espaços públicos (com exceções limitadas); manipulação subliminar; e sistemas de categorização biométrica com base em características sensíveis.

[14]O princípio Privacy by Design foi desenvolvido por Ann Cavoukian, ex-Comissária de Informação e Privacidade de Ontário (Canadá), e estabelece sete princípios fundamentais: proatividade em vez de reatividade; privacidade como configuração padrão; privacidade incorporada ao design; funcionalidade total (soma positiva, não de soma zero); segurança de ponta a ponta; visibilidade e transparência; e respeito pela privacidade do usuário.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

fenômeno em sua dimensão mais ampla — as relações de poder que permeiam a produção, o controle e a exploração do conhecimento e da informação na contemporaneidade.

Michel Foucault, em "Vigiar e Punir" (1975), descreve o panóptico benthamiano[15] como metáfora da sociedade disciplinar moderna — uma arquitetura de vigilância em que o olhar do observador, ainda que potencialmente ausente, induz no observado a consciência permanente de sua visibilidade, produzindo um efeito de autocontrole e docilidade. A IAG, com sua capacidade de processar e analisar quantidades massivas de dados comportamentais, representa uma forma radicalmente nova e mais sofisticada de panoptismo — não mais localizada em uma torre de observação, mas distribuída de forma ubíqua nas infraestruturas digitais das organizações e da sociedade (FOUCAULT, 1975).

O conceito foucaultiano de biopoder[16] — o poder sobre a vida, que atua sobre os corpos individuais e sobre as populações — encontra sua expressão contemporânea nos sistemas algorítmicos que classificam, segmentam e condicionam comportamentos de consumidores, trabalhadores e cidadãos. A IAG, ao inferir padrões comportamentais, tendências psicológicas e categorias identitárias a partir de dados aparentemente neutros, exerce uma forma de biopoder algorítmico que opera com eficiência e escala sem precedentes na história humana.

Zygmunt Bauman, com o conceito de modernidade líquida, oferece um enquadramento fundamental para compreender a fragilidade das estruturas sociais e institucionais frente à velocidade das transformações tecnológicas. Em "Modernidade Líquida" (2001), Bauman descreve uma condição social marcada pela instabilidade, pela efemeridade dos vínculos e pela dissolução das estruturas sólidas que outrora organizavam a vida social e política. No contexto da IAG, a liquidez manifesta-se na velocidade com que novos modelos e plataformas emergem e se disseminam, tornando obsoletos os marcos regulatórios e as práticas de governança antes mesmo de sua consolidação (BAUMAN, 2001).

Byung-Chul Han, em "A Sociedade da Transparência" (2012), analisa os paradoxos da hiperconectividade e da exposição voluntária de dados. Para Han, a sociedade contemporânea

---

[15]O panóptico, projetado por Jeremy Bentham no século XVIII, é uma arquitetura carcerária circular com uma torre de vigilância central, na qual o guarda pode observar todos os presos sem ser visto. Foucault utiliza essa metáfora para descrever o funcionamento das instituições disciplinares modernas — prisões, escolas, hospitais, fábricas — nas quais a consciência da possibilidade de ser observado é suficiente para produzir o efeito de autocontrole.

[16]O conceito de "biopoder" foi elaborado por Foucault no primeiro volume de "História da Sexualidade" (1976) e em cursos no Collège de France. O biopoder se manifesta em duas formas: a anátomo-política do corpo humano (disciplina dos corpos individuais) e a biopolítica da população (regulação dos processos biológicos das populações). A IA analítica representa uma nova tecnologia de biopoder que opera em escala e granularidade sem precedentes.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

é caracterizada por uma compulsão à transparência e à visibilidade — os indivíduos e as organizações expõem voluntariamente informações pessoais e estratégicas nas plataformas digitais, movidos pela lógica da performatividade e da otimização. Esse impulso à transparência, na perspectiva de Han, não representa a emancipação prometida pela retórica tecnológica, mas antes uma nova forma de controle — mais eficaz porque internalizada e aparentemente voluntária (HAN, 2017).

Shoshana Zuboff, em "A Era do Capitalismo de Vigilância" (2019), fornece a análise mais diretamente pertinente ao contexto da IAG corporativa. Zuboff descreve o capitalismo de vigilância[17] como uma nova lógica econômica que transforma a experiência humana em matéria-prima para produtos e serviços comportamentais. Para Zuboff, as grandes plataformas tecnológicas — e os fornecedores de IAG se encaixam paradigmaticamente nessa categoria — extraem dados comportamentais dos usuários sem contraprestação adequada, processam-nos para prever e influenciar comportamentos futuros, e os monetizam no "mercado de futuros comportamentais" (ZUBOFF, 2021).

A articulação desses referenciais filosóficos revela que os desafios da IAG para a privacidade e a segurança da informação não são apenas técnicos ou jurídicos — são fundamentalmente políticos e éticos. A questão de quem controla os dados, para que fins e com quais consequências para a autonomia individual e coletiva é, em última análise, uma questão de poder — e sua resposta exige não apenas regulação e tecnologia, mas uma reflexão ética profunda sobre os valores que devem orientar o desenvolvimento e o uso da inteligência artificial.

PROPOSTAS PARA UMA GOVERNANÇA SEGURA E RESPONSÁVEL DA IA

Com base na análise interdisciplinar desenvolvida nas seções precedentes, esta seção apresenta um conjunto de propostas para a construção de um modelo de governança segura e responsável da IAG no ambiente corporativo. No plano da governança corporativa, propõe-se a criação de uma estrutura de Governança de IA (AI Governance) que integre representantes das áreas jurídica, de segurança da informação, de tecnologia, de recursos humanos, de

[17]Zuboff cunhou o termo "capitalismo de vigilância" para descrever uma nova lógica econômica emergente a partir das práticas do Google, que descobriu que os dados comportamentais dos usuários — originalmente subproduto das buscas — podiam ser utilizados para prever e influenciar comportamentos futuros, criando um mercado altamente lucrativo de publicidade comportamental. Essa lógica foi posteriormente adotada pelo Facebook e outras plataformas digitais.

compliance e da alta direção. A norma ISO/IEC 42001:2023[18] oferece o arcabouço estrutural para essa governança.

No plano jurídico e de compliance, propõe-se a realização de uma Avaliação de Impacto à Proteção de Dados (AIPD)[19], conforme previsto no artigo 38 da LGPD, para cada caso de uso significativo de IAG envolvendo dados pessoais. Adicionalmente, os contratos com fornecedores de plataformas de IAG devem incluir cláusulas específicas sobre tratamento de dados, confidencialidade, proibição de uso dos dados para retreinamento dos modelos, notificação de incidentes e responsabilidade civil.

No plano tecnológico, propõe-se a implementação de uma arquitetura de segurança baseada nos princípios do Zero Trust, com controles específicos para o uso de IAG: políticas de DLP configuradas para identificar e bloquear a transmissão de dados sensíveis para plataformas de IAG não homologadas; soluções de CASB para monitoramento e controle do uso de serviços de IAG em nuvem; gestão rigorosa de identidades e acessos (IAM) para as ferramentas de IAG corporativas aprovadas; e implementação preferencial de ambientes de IAG privados para casos de uso envolvendo dados sensíveis.

No plano da cultura organizacional e da gestão de pessoas, propõe-se o desenvolvimento de um programa contínuo de conscientização e capacitação sobre o uso responsável de ferramentas de IAG, que aborde os riscos de segurança, as obrigações legais decorrentes da LGPD, as políticas corporativas de uso aceitável e as ferramentas aprovadas disponíveis para as necessidades dos colaboradores.

No plano ético, propõe-se a adoção de um conjunto de princípios para o uso responsável de IAG no ambiente corporativo, alinhados com as diretrizes éticas da União Europeia para IA confiável (EUROPEAN COMMISSION, 2019) e com os princípios da OCDE sobre IA (OECD, 2019): supervisão e controle humanos; transparência e explicabilidade; justiça e não discriminação algorítmica; privacidade e segurança de dados; responsabilidade e prestação de contas; e benefício social e sustentabilidade ambiental.

Por fim, propõe-se o engajamento ativo das organizações nos processos de construção regulatória, contribuindo com sua experiência prática para o desenvolvimento de marcos

---

[19]A Avaliação de Impacto à Proteção de Dados (AIPD), denominada Data Protection Impact Assessment (DPIA) no GDPR, é exigida pelo art. 38 da LGPD quando o tratamento de dados puder gerar riscos às liberdades civis e aos direitos fundamentais. A ANPD poderá estabelecer as hipóteses em que a realização da AIPD será obrigatória.

normativos que sejam ao mesmo tempo protetivos dos direitos fundamentais e promotores da inovação responsável.

METODOLOGIA

O presente artigo adota metodologia de pesquisa bibliográfica, exploratória e qualitativa, fundamentada em revisão de literatura científica, legislação aplicável, normas técnicas e documentos institucionais.

A pesquisa bibliográfica abrangeu obras de referência nos campos do Direito, Direito Digital, da Segurança da Informação, da Filosofia da Tecnologia e da Governança Corporativa, com ênfase em publicações dos últimos dez anos, sem prejuízo de obras clássicas de referência filosófica. As bases de dados consultadas incluíram o Portal de Periódicos da CAPES, o Google Scholar, a Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) e repositórios institucionais de universidades nacionais e internacionais.

A revisão da literatura técnica e normativa abrangeu as principais normas e frameworks internacionais relevantes: ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 42001:2023, NIST Cybersecurity Framework (2018), NIST AI Risk Management Framework (2023) e OWASP Top 10 for LLM Applications (2023). A legislação brasileira e estrangeira aplicável foi examinada na íntegra, com especial atenção à LGPD e ao EU AI Act.

O caráter exploratório da pesquisa decorreu da relativa novidade do fenômeno investigado e da escassez de estudos empíricos específicos sobre o uso corporativo de IAG no contexto brasileiro. A abordagem qualitativa permitiu a análise interpretativa e crítica dos dados coletados, com ênfase na construção de conexões interdisciplinares entre os campos do Direito, da Tecnologia e da Filosofia.

O procedimento metodológico adotado compreendeu: (a) levantamento e seleção da literatura relevante; (b) análise crítica dos textos selecionados; (c) síntese e articulação interdisciplinar dos conteúdos; (d) formulação de propostas baseadas na análise realizada. As referências bibliográficas foram organizadas e formatadas segundo as normas ABNT NBR 6023:2018.

CONSIDERAÇÕES FINAIS

A análise desenvolvida ao longo deste artigo evidencia que a Inteligência Artificial Generativa representa simultaneamente uma das mais poderosas ferramentas de inovação

disponíveis para as organizações contemporâneas e um vetor de risco jurídico, tecnológico e organizacional de magnitude sem precedentes. A tensão entre esses dois polos, inovação e risco, não pode ser resolvida pela simples adoção tecnológica nem pela regulação isolada, mas exige uma abordagem verdadeiramente integrada.

O problema de pesquisa proposto não admite resposta simples ou universal. Cada organização possui um perfil único de riscos, uma cultura organizacional própria e um contexto regulatório específico. Não obstante, os princípios e as práticas identificados nesta pesquisa oferecem um arcabouço consistente para a construção de respostas contextualizadas e efetivas.

A análise jurídica demonstrou que a LGPD, embora não elaborada especificamente para o contexto da IAG, fornece um conjunto de princípios e instrumentos normativos suficientemente robusto para disciplinar o uso corporativo dessas ferramentas — desde que interpretada e aplicada de forma criativa e contextualizada. A responsabilidade das organizações não se limita à conformidade formal com os requisitos legais, mas abrange a adoção de uma postura proativa de proteção dos direitos dos titulares de dados.

A análise tecnológica revelou que os riscos da IAG para a segurança da informação são reais e potencialmente devastadores, mas são gerenciáveis por meio de controles técnicos e organizacionais adequados. A arquitetura Zero Trust, as soluções de DLP e CASB, a gestão rigorosa de identidades e acessos, e a implantação de ambientes privados de IAG representam o estado da arte dos controles técnicos disponíveis.

A análise filosófica revelou que os desafios da IAG transcendem as dimensões técnicas e jurídicas, situando-se no campo das relações de poder, da vigilância, da mercantilização da experiência humana e da erosão da autonomia individual e coletiva. Os referenciais de Foucault, Bauman, Han e Zuboff oferecem lentes críticas indispensáveis para compreender as implicações mais profundas da IAG.

A conclusão fundamental desta pesquisa é que a proteção efetiva contra os riscos da IAG não depende exclusivamente de tecnologia ou legislação isoladamente, mas da integração entre pessoas, processos, governança, segurança e cultura organizacional. As organizações que construírem essa integração de forma consistente e sustentável não apenas estarão em conformidade com os requisitos legais e melhores práticas de segurança — estarão também melhor posicionadas para extrair o valor real que a IAG tem a oferecer, de forma responsável, ética e sustentável.

O caminho à frente demanda esforço coletivo: das organizações, no desenvolvimento de programas robustos de governança da IAG; do Poder Legislativo, na construção de marcos normativos específicos e adequados; da ANPD, na regulamentação e na orientação dos agentes

de tratamento; da academia, na produção de conhecimento interdisciplinar rigoroso; e da sociedade civil, na vigilância e na defesa dos direitos fundamentais ameaçados pelo uso irresponsável dessas tecnologias. A inteligência artificial generativa é, em última análise, um espelho da inteligência humana — e as escolhas que fazemos sobre como desenvolvê-la e utilizá-la refletem, para o bem ou para o mal, os valores que como sociedade decidimos priorizar.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Guia Orientativo sobre Transferência Internacional de Dados Pessoais. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd. Acesso em: 8 jun. 2026.

BAUMAN, Zygmunt. Modernidade Líquida. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

BOMMASANI, Rishi et al. On the Opportunities and Risks of Foundation Models. Stanford CRFM, 2021. Disponível em: https://arxiv.org/abs/2108.07258. Acesso em: 8 jun. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BUSINESSINSIDER. Samsung workers accidentally leaked trade secrets while using ChatGPT. Business Insider, 2023. Disponível em: https://www.businessinsider.com/samsung-workers-leaked-trade-secrets-chatgpt-2023-4. Acesso em: 8 jun. 2026.

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Ontario: Information and Privacy Commissioner of Ontario, 2009.

CYBERHAVEN. Cyberhaven 1 Million User Study: How Employees Use ChatGPT and Other AI Tools at Work. San Francisco: Cyberhaven, 2023.

EUROPEAN COMMISSION. Ethics Guidelines for Trustworthy AI. Bruxelas: European Commission High-Level Expert Group on Artificial Intelligence, 2019.

EUROPEAN PARLIAMENT. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, 2024.

FOUCAULT, Michel. Vigiar e Punir: Nascimento da Prisão. Tradução de Raquel Ramalhete. Petrópolis: Vozes, 1987. (Original publicado em 1975).

GARTNER. Top Strategic Technology Trends for 2024. Stamford: Gartner Research, 2023.

GOODFELLOW, Ian; BENGIO, Yoshua; COURVILLE, Aaron. Deep Learning. Cambridge: MIT Press, 2016.

HAN, Byung-Chul. A Sociedade da Transparência. Tradução de Enio Paulo Giachini. Petrópolis: Vozes, 2017. (Original publicado em 2012).

HAN, Byung-Chul. No Enxame: Perspectivas do Digital. Tradução de Lucas Machado. Petrópolis: Vozes, 2018. (Original publicado em 2013).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Genebra: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls. Genebra: ISO, 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 42001:2023 – Artificial intelligence – Management system. Genebra: ISO, 2023.

LAYERX SECURITY. Annual Browser Security Report 2023. Tel Aviv: LayerX Security, 2023.

MCKINSEY GLOBAL INSTITUTE. The Economic Potential of Generative AI: The Next Productivity Frontier. Nova York: McKinsey & Company, 2023.

MICROSOFT. Azure OpenAI Service: Data, Privacy, and Security for Azure OpenAI Service. Redmond: Microsoft, 2023. Disponível em: https://learn.microsoft.com/azure/ai-services/openai/. Acesso em: 8 jun. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg: NIST, 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg: NIST, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg: NIST, 2020.

OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Paris: OECD, 2019.

OPENAI. GPT-4 Technical Report. San Francisco: OpenAI, 2023. Disponível em: https://arxiv.org/abs/2303.08774. Acesso em: 8 jun. 2026.

OUYANG, Long et al. Training language models to follow instructions with human feedback. In: ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 35., 2022. Proceedings [...]. NeurIPS, 2022.

OWASP FOUNDATION. OWASP Top 10 for Large Language Model Applications. Version 1.1. Wilmington: OWASP, 2023. Disponível em: https://owasp.org/www-project-top-10-for-large-language-model-applications/. Acesso em: 8 jun. 2026.

SILIC, Mario; BACK, Andrea. Shadow IT: A view from behind the curtain. Computers & Security, v. 45, p. 274-283, 2014.

THE ECONOMIST. The world's most valuable resource is no longer oil, but data. The Economist, London, 6 maio 2017.

VASWANI, Ashish et al. Attention Is All You Need. In: ADVANCES IN NEURAL INFORMATION PROCESSING SYSTEMS, 30., 2017. Proceedings [...]. NeurIPS, 2017.

WORLD ECONOMIC FORUM. Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows. Cologny/Geneva: World Economic Forum, 2020.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo - SP.
Ano VII, v.1 2026 | submissão: 03/07/2026 | aceito: 06/07/2026 | publicação: 09/07/2026

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância: A Luta por um Futuro Humano na Nova Fronteira do Poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021. (Original publicado em 2019).