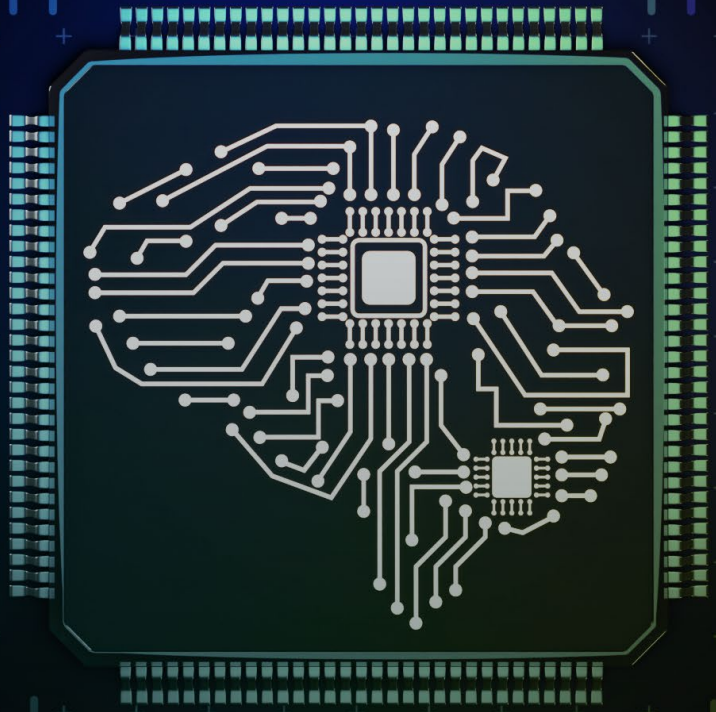
VLK ADV

Onde o Direito impulsiona a Inovação



eBook

O PAPEL DO DPO NA GOVERNANÇA DE IA

Desafios Reais, Funções-chave e Soluções Práticas

PRINCIPAIS TEMAS:

- Distinção entre as funções de DPO e CAIO
- Convergência entre governança de dados e IA
- Comparação prática entre RIPD e AIA
- Novos desafios dos direitos dos titulares e das pessoas afetadas por sistemas automatizados
- **Mais de 60 critérios práticos em formato de checklist**

www.vlklaw.com.br

Agosto de 2025

SUMÁRIO

CONTEXTUALIZAÇÃO **4**

1. DPO e CAIO: distinções, sobreposições de funções e desafios práticos **6**
1.1. Convergência de Funções e a Emergência de Novos Papéis 9
1.2. Sobreposição: Oportunidade ou Armadilha? 10
1.3. Modelos por Porte, Complexidade e Maturidade Organizacional 11
1.4. Checklist para o DPO 12

2. Governança em Proteção de Dados e Governança em IA **14**
2.1 Estruturas em Evolução e Pontos de Convergência 16
2.2 Comunicação Estratégica: Pilar Comum 17
2.3 Reaproveitamento de Estruturas e Ferramentas 18
2.4 Sustentabilidade e Maturidade Organizacional 19
2.5 Checklist para o DPO 20

3. DPIA e AIA: Análise Comparativa Prática **22**
3.1 Conceitos Fundamentais: Finalidade e Escopo 22
3.2 Comparação Técnica e Metodológica 24
3.3 Complementaridade e Reaproveitamento 25
3.4 Limitações e Ações Pragmáticas 26
3.5 Checklist para o DPO 26

4. Direitos dos Titulares e das Pessoas Afetadas por IA **28**
4.1 Dois Marcos Regulatórios, Um Mesmo Centro: a Pessoa 28
4.2 Desafios de Aplicação: IA, Vieses e Transparência 28
4.3 Da Proteção de Dados à Proteção de Pessoas 29
4.4 Caminhos para Interpretação Legal e Governança Integrada 30
4.5 Checklist para o DPO 30

Considerações Finais **32**

Checklist - O Papel do DPO na Governança de IA **37**

Sobre Nós **42**

Autores **42**

VLK

Direito,
Inovação
& Tecnologia

Contextualização

A Inteligência Artificial ("IA") é realidade transformadora como tecnologia de propósito geral que redefine a forma como empresas operam os seus negócios, cada vez mais onipresente em todas as atividades e setores.

Por outro lado, há profundo desafios, como: transformações abruptas no mercado de trabalho; explicabilidade, auditabilidade, supervisão e controle das decisões automatizadas com o uso da IA; preservação de direitos autorais no treinamento de modelos em larga escala; cibersegurança; privacidade; discriminação algorítmica injusta; deepfakes e manipulações; dependência e confiança excessiva; e concentração de poder em poucos países e empresas.

Tais questões, somadas ao intenso tratamento de dados pessoais em aplicações de IA, **têm exigido a revisão estratégica das práticas tradicionais de governança** e a integração efetiva de requisitos técnicos, legais e éticos. **No centro dessa convergência está o papel do Encarregado pelo Tratamento de Dados Pessoais** (que, neste material, será referido como *Data Protection Officer* - "DPO").

A função do DPO, tradicionalmente vinculada ao *compliance* regulatório em proteção de dados pessoais, **tende a se expandir diante dos impactos da IA, exigindo atuação ainda mais estratégica, transversal e multidisciplinar**.

A complexidade se intensifica quando se considera o contexto internacional. Diversas jurisdições impõem obrigações regulatórias distintas, como: o "*General Data Protection Regulation* ("GDPR") na União Europeia; a Lei Geral de Proteção de Dados Pessoais ("LGPD") no Brasil e sua regulamentação; e regulações emergentes sobre IA, como o *EU AI Act*, o PL 2338/2023, a norma internacional ISO/IEC 42001:2023, o AI Risk Management Framework do NIST e os Princípios de IA da OCDE.

O AI Index Report 2025, elaborado pela Universidade de Stanford (EUA), com foco em governança, *compliance* e riscos estratégicos de IA nas empresas, **aponta privacidade e proteção de dados pessoais como o risco que mais preocupa as empresas em termos de IA (65%)**, seguido por confiabilidade técnica diante da imprecisão e alucinação (59%), propriedade intelectual (56%) e perdas financeiras (59%)[1].

Nesse cenário, **o DPO precisa atuar ainda mais em articulação com lideranças de negócios**, responsáveis por inovação, tecnologia e transformação digital, e novas funções, **como o Chief Artificial Intelligence Officer ("CAIO")**, para garantir conformidade jurídica, confiança dos *stakeholders* e a responsabilidade organizacional frente aos riscos algorítmicos, com ou sem uso da IA. Trata-se de desafio que vai além do *compliance* tradicional: envolve governança institucional, maturidade digital e cultura organizacional orientada à ética, explicabilidade, transparência e não discriminação.

Este eBook foi desenvolvido para **apoiar DPOs na compreensão prática, comparativa e estratégica dessa nova interseção entre proteção de dados e governança em IA.** Exploraremos:

- As distinções e sinergias entre os papéis de DPO e CAIO;
- Os pontos de convergência entre as estruturas de governança de dados e de IA;
- A comparação técnica e metodológica entre o Relatório Impacto à Proteção de Dados Pessoais ("RIPD") e a Análise de Impacto Algorítmico ("AIA"); e
- Os desafios jurídicos e práticos relacionados aos direitos dos titulares e das pessoas afetadas por sistemas automatizados.

Cada capítulo é acompanhado de *checklist* prático e estruturado, com mais de 60 critérios de avaliação. O objetivo é fornecer instrumentos funcionais aplicáveis à realidade das organizações, reforçando o compromisso deste material com conteúdo técnico, direto e efetivamente útil para quem atua na linha de frente da proteção de dados, diante dos novos desafios trazidos pela transformação algorítmica.

VLK Advogados

1. DPO e CAIO: distinções, sobreposições de funções e desafios práticos

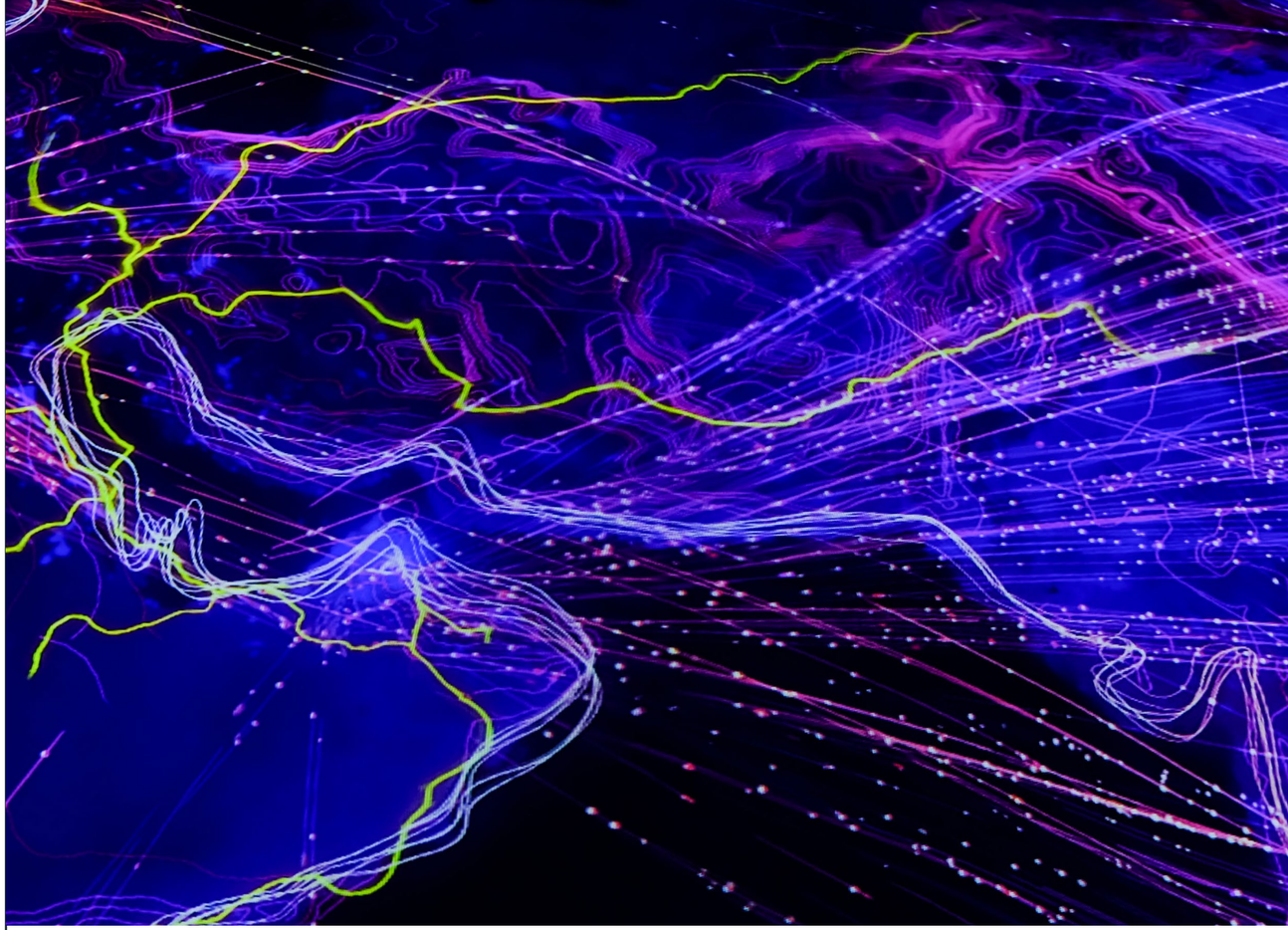
A consolidação da IA como tecnologia de uso geral, onipresente e estratégica nas organizações tem provocado a reorganização de funções e responsabilidades na governança digital. Nesse novo cenário, surgem figuras como CAIO, cuja atuação precisa ser muito bem definida, **inclusive para mitigar o risco de conflito de interesse e sobreposição com o papel do DPO**.

Enquanto o papel central do **DPO é gerar conformidade com normas de proteção de dados e mitigar riscos**, permitindo que novos negócios sejam desenvolvidos respeitando o princípio do *Privacy by Design* ("PbD"), **a nova cadeira de CAIO visa impulsionar a adoção da IA e orquestrar a mudança cultural necessária para que a tecnologia seja integrada em toda a organização**, normalmente com as seguintes funções:

- Definir a estratégia da organização em relação à IA;
- Impulsionar a mudança cultural e o desenvolvimento de competências;
- Atuar como ponte entre tecnologia e negócios;
- Conduzir análises estatísticas, de algoritmos de aprendizado de máquina e de infraestrutura de dados para a empresa implementar eficazmente soluções de IA;
- Lidar com questões éticas e legais de IA, como vieses indevidos, responsabilidade dentro da cadeia de valor da IA, robustez, segurança e transparência.

Embora os Diretores de Tecnologia (CTOs) e os Diretores de Inovação (CIOs) atualmente liderem a maioria das iniciativas de transformação digital nas empresas, pesquisa global recente[2] revela que empresas estão nomeando um executivo dedicado à IA para acelerar a sua adoção e gerenciar a complexidade de implementação, o CAIO:

- No Brasil: 56% das organizações já contam com um CAIO e mais 31% contratarão até 2026;



- Globalmente: o número atual é de 60%, com previsão de subir para 86% em 2026.

Outros números importantes do Brasil: apenas 28% das empresas brasileiras possuem estratégia estruturada para integrar a IA aos negócios. Porém, 93% delas reconhecem a importância de uma gestão eficaz para integrar a tecnologia aos negócios. A previsão é que, até o final de 2026, 91% das empresas já tenham estratégias dedicadas para gerenciar o impacto da IA.

Nos EUA, a nova estratégia de IA "AI Action Plan USA"[3], aborda o *Chief Artificial Intelligence Officer Council* (CAIOC) no contexto da aceleração da adoção de IA no governo, recomendando a formalização do cargo como o principal local para coordenação e colaboração interinstitucional na adoção da IA, em coordenação e colaboração estratégica com outros conselhos executivos federais relevantes, incluindo: o Conselho de Gestão do Presidente, o *Chief Data Officer Council*, *Chief Information Officer Council*, *Interagency Council on Statistical Policy*, *Chief Human Capital Officer Council*, e o *Federal Privacy Council*.

Já pesquisa do Gartner[4] demonstra que a **responsabilidade pelo tema IA é dispersa**, no seguinte sentido:

- Dos 54% dos líderes executivos que indicaram ter líder de IA, 88% disseram que esse líder não recebeu o título de CAIO;
- Para 25% das empresas, a responsabilidade de IA está no cargo de CIO;
- 55% das organizações têm conselho de IA multidisciplinar para superar os desafios de gerar valor e reduzir riscos;
- Dentro do Conselho, os principais focos são: 26% governança; e 21% a estratégia para lidar com o tema.

Na Grã-Bretanha, quase metade das empresas (48%) da *Financial Times Stock Exchange* (FTSE) 100 já estabeleceram cargos de liderança dedicados à IA, com três áreas de atuação predominantes: ciência de dados (50%); consultoria (21%); e engenharia e tecnologia (17%)[5].

Por sua vez, **em termos de governança de IA**, o *AI Governance Profession Report* 2025[6], envolvendo mais de 670 empresas, em 45 países, apontou que:

- 77% das empresas estão adotando governança de IA;
- Mais de 50% dos profissionais de governança de IA são normalmente de equipes de ética, conformidade, privacidade ou jurídica;
- Principais funções encarregadas da responsabilidade primária pela governança da IA: 25% privacidade; 22% jurídica; 17% tecnologia; 10% governança de dados; 6% ética e compliance; e 5% cibersegurança;
- Quando a principal responsabilidade pela governança de IA está acumulada com o responsável por privacidade na organização, os entrevistados demonstraram probabilidade significativamente maior de se sentirem confiantes em sua capacidade de cumprir com o EU AI Act (67%).

Assim, este capítulo se dedica aos limites da sobreposição das funções, os riscos de conflito de interesse e os modelos possíveis de atuação, conforme o porte e a maturidade da organização.

1.1. CONVERGÊNCIA DE FUNÇÕES E A EMERGÊNCIA DE NOVOS PAPÉIS

Com a ascensão da IA nas operações empresariais, surgem papéis estratégicos voltados à governança algorítmica, especialmente diante da interdependência entre Inteligência Artificial e proteção de dados. Enquanto o DPO é peça central na conformidade com a LGPD, o CAIO responde à crescente complexidade dos sistemas algorítmicos e à necessidade de garantir ética, transparência e responsabilidade em sua implementação, independentemente do uso de dados pessoais. Ambos têm atuação transversal e compartilham objetivos comuns, como:

- Prevenção de riscos regulatórios e reputacionais;
- Promoção da confiança em tecnologias emergentes;
- Sucesso das novas estratégias de negócios e da transformação digital empresarial, cada vez mais pautadas em dados e algoritmos de IA; e
- Garantia de direitos fundamentais.

São, portanto, **funções complementares, mas com competências específicas e técnicas diferentes**. Por isso, muitos programas de governança de IA estão apoiados em estruturas maduras de proteção de dados.

Pesquisas indicam que **metade das organizações estruturam suas políticas de IA a partir de *frameworks* de privacidade já existentes**[7], com destaque para os RIPDs, que têm sido adaptados à elaboração de AIAs (tema abordado especificamente no Capítulo 3). Isso **reforça o papel estratégico do DPO, especialmente nas frentes de mitigação de riscos, explicabilidade dos sistemas e direitos fundamentais**.

Diante desse cenário, fica a reflexão: os papeis de DPO e CAIO podem ser exercidos pela mesma pessoa? Até que ponto a fusão de funções é viável?

1.2. SOBREPOSIÇÃO: OPORTUNIDADE OU ARMADILHA?

Na nossa experiência prática com estruturação e atualização de governança em proteção de dados e IA, temos observado:

- DPOs liderando governança de IA;
- CAIOs capitaneando determinados aspectos de privacidade algorítmica; e
- Times de proteção de dados e governança de IA integrados, mas com lideranças distintas.

A sobreposição pode gerar ganhos em agilidade e coesão, **desde que respeitados limites de autonomia, isenção e especialização**, levando em conta também o porte da organização e os riscos associados aos projetos de IA.

O GDPR (Art. 38) e o Regulamento CD/ANPD no 18/2024 **exigem independência técnica e ausência de conflitos de interesse para a atuação do DPO**. O mesmo profissional não deve supervisionar a conformidade e, simultaneamente, tomar decisões estratégicas sobre o tratamento de dados ou a implementação de IA.

A Autoridade de Proteção de Dados da Bélgica multou uma empresa que acumulava as funções de DPO e diretor de *compliance*[8]. Cargos como CIO e CEO também são considerados potencialmente incompatíveis com a função de DPO.

O Tribunal de Justiça da União Europeia (TJUE) reforçou essa visão no caso C-453/21, afirmando que a independência do DPO é comprometida quando ele define os objetivos e meios do tratamento de dados. A avaliação de conflito de interesses deve considerar a estrutura organizacional e as políticas internas da empresa[9].

No Brasil, o Guia Orientativo sobre a Atuação do Encarregado baseado no Regulamento CD/ANPD no 18/2024, da Autoridade Nacional de Proteção de Dados (ANPD)[10], dispõe que:

> "De modo geral, posições conflitantes são observadas quando o encarregado acumula cargos de chefia, gerência ou direção, responsáveis pela determinação de meios e objetivos do tratamento de dados pessoais, a exemplo de setores responsáveis pela gestão de recursos humanos, **tecnologia da informação**, finanças ou saúde" (g.n.).

Enquanto o DPO adota postura de supervisão e moderação[11], o CAIO atua como líder de IA para a integração da tecnologia na transformação digital e na inovação. Essa diferença de enfoque pode tornar a sobreposição complexa para uma posição de governança, como a do DPO.

1.3. MODELOS POR PORTE, COMPLEXIDADE E MATURIDADE ORGANIZACIONAL

A estrutura ideal de governança de IA, em regra, leva em conta três fatores:

- Porte da organização;
- Complexidade e intensidade dos sistemas de IA e riscos do seu uso; e
- Nível de maturidade em governança digital.

Em empresas de pequeno e médio porte, o acúmulo de funções é comum, muitas vezes por restrições orçamentárias. Nesses casos, o DPO pode atuar de forma ampliada, desde que:

- Haja avaliação formal de conflitos;
- As justificativas sejam registradas; e

» Existam salvaguardas, como reporte direto ao Conselho ou à Alta Administração.

Já em empresas maiores, com projetos complexos ou de alto risco, a tendência é a separação das funções de DPO e CAIO, cada qual com escopo técnico e autonomia decisória.

Funções intermediárias, como o *AI Risk Officer* (dedicado à identificação, avaliação e mitigação dos riscos algorítmicos) também ganham espaço, com foco na identificação e mitigação de riscos, atuando junto ao DPO, mas sem interferência executiva.

Para garantir efetividade, segurança jurídica e transparência, é essencial que a organização estabeleça:

» Definição clara de escopo e autoridade de cada uma dessas funções;

» Protocolos de reporte independentes; e

» Fluxos colaborativos entre jurídico, times de dados, tecnologia e compliance.

A colaboração estruturada entre DPO, CAIO e demais *stakeholders* é essencial para que os sistemas de IA sejam tecnicamente robustos, juridicamente conformes e socialmente confiáveis.

1.4. CHECKLIST PARA O DPO

a) Independência e Conflito de Interesse

☐ Minhas funções atuais não incluem decisões operacionais sobre IA (modelos, critérios ou implementação).

☐ Existe avvaliação formal e documentada de ausência de conflito de interesse, conforme disposto pela ANPD12.

☐ Caso eu exerça outras funções, elas não afetam minha imparcialidade como DPO.

☐ Tenho autonomia técnica para emitir pareceres contrários à estratégia de IA, se necessário.

b) Estrutura e Reporte

☐ Minha atuação está formalmente registrada, com escopo e responsabilidades claros.

☐ Reporto diretamente à Alta Administração ou ao Conselho.

☐ Participo de comitês de risco, mas sem responsabilidade executiva sobre IA.

c) Colaboração com o CAIO e outros *stakeholders*

☐ Há processos estruturados de colaboração com o CAIO e áreas técnicas.

☐ A governança de IA contempla os direitos fundamentais, privacidade e explicabilidade.

☐ Participo das Avaliações de Impacto Algorítmico (AIAs) que envolvem dados pessoais ou direitos do titular.

d) Modelo proporcional ao porte e maturidade da organização

☐ A estrutura atual (acúmulo ou separação de funções) foi adotada com base em análise formal do porte, orçamentário, riscos e da maturidade digital da organização.

☐ Em caso de acúmulo de funções, foram adotadas salvaguardas como reporte independente, validação externa ou revisão periódica.

☐ Estruturei mecanismo para revisar a estrutura organizacional, conforme a evolução dos riscos e projetos.

e) Capacitação e Atualização Contínua

☐ Recebo formação contínua sobre IA, riscos algorítmicos e regulação (AI Act, LGPD, GDPR, ISO 42001, entre outros).

☐ Acompanho decisões regulatórias e boas práticas sobre a função do DPO e sua interface com a governança de IA.

2. Governança em Proteção de Dados e Governança em IA: aproveitamento de frameworks, recursos e políticas

À medida que a IA se consolida como ativo estratégico, cresce a demanda por modelos de governança capazes de integrar privacidade, ética, segurança e responsabilidade algorítmica. O desafio é aproveitar *frameworks* já consolidados de proteção de dados e estruturar a governança de IA com eficiência orçamentária e técnica.

A própria ANPD, ao analisar o PL de IA 2.338/23[13], se alinha a esse entendimento:

> "A LGPD introduziu no Brasil o conceito de governança de dados, estabelecendo a necessidade de as organizações implementarem políticas, práticas e procedimentos robustos para garantir a proteção de dados pessoais. O PL nº 2338/2023, ao abordar a regulação da IA, também destaca a importância de mecanismos de governança robustos para sistemas de IA, especialmente aqueles classificados como de alto risco. **A experiência e as diretrizes já estabelecidos pela LGPD podem servir como base para a elaboração de mecanismos de governança específicos para a IA". (g.n.)**.

Mas quais os principais desafios para governar a IA? O já mencionado AI Governance Profession Report 2025, aponta:

- 49% – falta de compreensão sobre IA e sobre as obrigações de conformidade com a tecnologia;
- 37% – recursos insuficientes dedicados às atividades de governança de IA;
- 35% – ausência de representação da função de governança de IA nos níveis seniores da organização;
- 31% – prioridades concorrentes reduzem o foco nas atividades de governança de IA;
- 27% – integração ineficaz da gestão de riscos de IA com as atividades mais amplas de gestão de riscos da organização; e
- 26% – Privacy by design não é efetivamente implementado na organização.

O mesmo relatório traz casos práticos interessantes de determinadas empresas acerca da integração entre governança de IA e proteção de dados[14], como:

- **Mastercard**: quando um risco de IA é considerado potencialmente alto, ele é analisado pelo Conselho de IA e Dados, composto por líderes seniores de várias áreas e co-presidido pelo Chief Privacy Officer e pelo Chief AI and Data Officer;
- **IBM**: o "Chief Privacy Office" (posteriormente renomeado para "Office of Privacy and Responsible Technology") foi encarregado de garantir o desenvolvimento e a implantação responsável da IA. Este departamento aumentou o programa originalmente desenvolvido para identificar

avaliações de impacto de privacidade e conformidade com o GDPR para incorporar a governança de IA e dados em geral;

- **Randstad**: a governança de IA é operada a partir do departamento jurídico e de proteção de dados;

- **TELUS**: a empresa já tinha histórico de desenvolvimento de tecnologias que exigiam considerações sobre ética de dados, governança e privacidade. Isso permitiu que as equipes já existentes abordassem rapidamente os desafios da governança de IA.

Assim, este capítulo explora essa convergência prática e conceitual, apontando caminhos, limites e boas práticas.

2.1. ESTRUTURAS EM EVOLUÇÃO E PONTOS DE CONVERGÊNCIA

A governança digital está promovendo a integração entre proteção de dados e IA. Ambos compartilham pontos de atenção, como:

- Prevenção de riscos e segurança da informação;

- Garantia de direitos; e

- Transparência e prestação de contas (accountability).

Frameworks consolidados (como RIPDs, políticas de *privacy by design* e comitês de governança de dados) são frequentes ponto de partida para a governança de IA. Eles permitem a inclusão de:

- Avaliação de Impacto Algorítmico (AIA);

- Fundamental Rights Impact Assessment (FRIA)15;

- Inventário (ou mapeamento) de sistemas de IA;

- Programas de treinamentos e cultura organizacional (ex: “Champions de IA”); e

- Políticas e contratos (clausulados) adaptados.

As normas internacionais, como o NIST AI RMF (2023), *EU AI Act*, ISO/IEC 42001, os Princípios da OCDE e orientações do *European Data Protection Board* (“EDPB”) e da própria ANPD[16] reforçam a centralidade dos princípios de proteção de dados como base para uma IA responsável, como:

- Abordagem baseada em risco;

- Mecanismos de governança; e

- Comunicação de incidentes.

2.2. COMUNICAÇÃO ESTRATÉGICA: PILAR COMUM

A transparência ativa é componente essencial de ambas as estruturas, incluindo: titulares e pessoas afetadas; reguladores; e o público em geral. Essas governanças devem:

- Adotar linguagem acessível e design jurídico nas comunicações;

- Estruturar canais claros de reclamação e resposta; e

- Promover confiança institucional, especialmente em setores críticos (financeiro, saúde, seguro, educação, telecomunicações, energia e segurança pública).

A reutilização para IA dos canais e estruturas de resposta já presentes para proteção de dados é, portanto, prática eficiente e sustentável.

2.3 REAPROVEITAMENTO DE ESTRUTURAS E FERRAMENTAS

Destacamos exemplos de estruturas da governança de dados que podem ser estendidas ou adaptadas à governança de IA, de acordo com o inventário realizado e os riscos identificados a serem mitigados:

Ferramenta/Estrutura	Uso em Privacidade	Adaptação para IA
Programa de Governança	Políticas, indicadores e planos de ação	Inclusão de eixos éticos e métricas de risco e desempenho algorítmico
RIPD	Avaliação de riscos e medidas de mitigação	Base para a AIA e a FRIA, com ampliação de escopo
Comitê de Privacidade	Deliberação sobre riscos e decisões de dados	Expansão para Comitê de Ética e IA
Treinamentos de LGPD	Capacitação em privacidade	Inclusão de conceitos específicos e temas como viés, explicabilidade e ética algorítmica
Códigos e Políticas	Regras internas sobre tratamento de dados	Extensão para uso responsável, ético, explicável e auditável de IA
Atendimento aos Direitos dos Titulares	Respostas a solicitações dos titulares (acesso, exclusão, correção, revisão de decisões)	Ampliação para decisões automatizadas, revisão humana e explicabilidade de IA
Princípios de Transparência e Finalidade	Avisos de privacidade e comunicação clara sobre os propósitos de tratamento	Inclusão de transparência sobre critérios algorítmicos e finalidade de uso da IA
Cláusulas Contratuais com Terceiros	Obrigações de proteção de dados com fornecedores	Inserção de requisitos específicos sobre uso de IA, avaliação de riscos e auditorias técnicas
Avaliação de Terceiros (*Third-Party Risk Assessment*)	*Due dilligence* de operadores	Auditoria de práticas algorítmicas e verificação de alinhamento ético e regulatório de fornecedores de IA
Comunicação de Incidentes	Avaliação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares	Avaliação de incidentes considerados como graves, que possam envolver risco à vida e à integridade física de pessoas, a interrupção de funcionamento de operações críticas e graves danos à propriedade ou ao meio ambiente e violações aos direitos fundamentais

Fonte: VLK Advogados

2.4 SUSTENTABILIDADE E MATURIDADE ORGANIZACIONAL

Dados do IAPP-EY *Privacy Governance Report* 2023[17] e do *Cisco Privacy Benchmark*[18] mostram que empresas com programas de privacidade maduros estão melhor preparadas para estruturar políticas de IA. Isso inclui: orçamento dedicado (em média US$ 2,7 milhões em 2023); equipes especializadas; e estratégias ESG consolidadas.

O maior entrave, no tanto, é a falta de capacitação: 51% das empresas identificam a ausência de conhecimento interno como barreira à IA responsável. O DPO deve estar envolvido desde a concepção dos projetos de IA que envolvam dados pessoais, oferecendo visão crítica e orientando decisões com base em princípios legais e éticos[19]. Integrar as duas governanças favorece:

- Redução de custos regulatórios com estruturas compartilhadas;
- Clareza de papéis e responsabilidades; e
- Fortalecimento da cultura organizacional orientada à ética e inovação.

Governança de IA não é tarefa isolada, mas estrutura viva, ajustada a riscos,

stakeholders e maturidade tecnológica. O papel do DPO é ser um dos pilares dessa construção, atuando em sinergia com as demais lideranças para garantir que o uso da IA seja inovador, eficaz e responsável.

2.5. CHECKLIST PARA O DPO

a) Estrutura Integrada de Governança

- ☐ A organização possui programa institucional que abrange dados pessoais e IA de forma integrada.
- ☐ Há comitê multidisciplinar para decisões sobre ética, risco e IA, com regulamento estruturado e aprovado.
- ☐ Os RIPDs são utilizados como base para a elaboração das AIAs.
- ☐ As políticas de governança de dados incluem diretrizes específicas para sistemas automatizados.

b) Comunicação Estratégica e Transparência

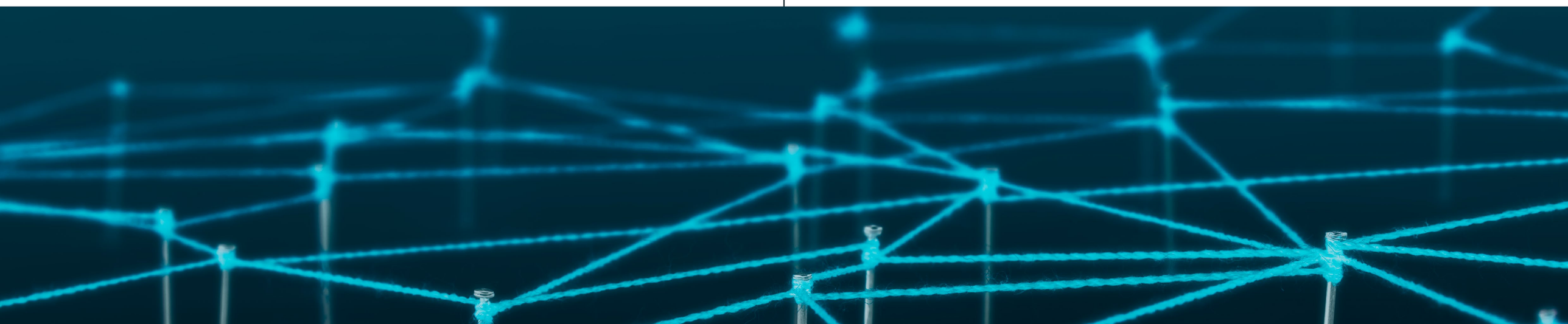
- ☐ As comunicações explicam, com linguagem clara e acessível, o uso de IA e os critérios automatizados.
- ☐ Os avisos de privacidade incluem menções específicas à finalidade da IA.
- ☐ Os canais de atendimento estão preparados para solicitações relacionadas IA.
- ☐ Há uso de design jurídico nos materiais voltados ao público, promovendo compreensão real sobre o uso de algoritmos.

c) Reaproveitamento de Estruturas e Ferramentas

- ☐ O comitê de privacidade tratar também de ética e risco em IA.
- ☐ Os treinamentos incluem tópicos como vieses, explicabilidade, responsabilidade algorítmica e uso ético de IA.
- ☐ Os contratos com terceiros incluem cláusulas sobre IA, auditoria e mitigação de riscos.
- ☐ A organização realiza due diligence técnica e ética em terceiros que desenvolvem ou operam soluções de IA.

d) Sustentabilidade e Maturidade Organizacional

- ☐ A estrutura de IA reaproveita processos e recursos da governança de dados.
- ☐ Há orçamento e equipe (dedicada ou compartilhada) para iniciativas de IA responsável.
- ☐ O DPO participa desde o início de projetos de IA que envolvem dados pessoais, contribuindo na avaliação de riscos e na definição de salvaguardas éticas e legais.
- ☐ O modelo adotado respeita o estágio de maturidade digital e é revisado conforme a evolução dos projetos e dos riscos envolvidos.



3. DPIA e AIA: análise Comparativa Prática

A governança responsável de IA exige avaliação prévia dos riscos e impactos que essas tecnologias podem gerar. Nesse contexto, o RIPD e a AIA são ferramentas centrais, muitas vezes confundidos ou aplicados de forma isolada. Este capítulo analisa técnica, jurídica e estrategicamente esses dois mecanismos, destacando suas diferenças, pontos de complementariedade e caminhos para estrutura integrada.

3.1. CONCEITOS FUNDAMENTAIS: FINALIDADE E ESCOPO

O RIPD é exigido pela LGPD (arts. 5º, XVII e 38) e pelo GDPR (art. 35) em situações de tratamento de dados pessoais com risco elevado aos direitos e às liberdades dos titulares. Seu objetivo é mapear operações de tratamento, identificar bases legais, avaliar e mitigar os riscos relacionados ao uso de dados pessoais e propor medidas de mitigação.

Já a AIA possui escopo mais amplo, vai além da proteção de dados pessoais e analisa o funcionamento técnico e ético do sistema de IA, abordando temas como:

- Opacidade algorítmica;
- Vieses;
- Violação de direitos de terceiros;
- Impactos ambientais;
- Imprevisibilidade do algoritmo, possíveis externalidades negativas e perda de autonomia.

Ainda que não seja legalmente obrigatória, em muitos contextos, sua adoção pode voluntária é recomendada para mitigar riscos reputacionais e regulatórios.

Inclusive, a AIA está prevista no Projeto de Lei nº 2338/23[20] como obrigação do desenvolvedor ou do aplicador que introduzir ou colocar sistema de IA em circulação no mercado, sempre que o sistema ou o seu uso forem de alto risco, considerando o papel e a participação do agente na cadeia.

O *EU AI Act*, apesar de não usar o termo "AIA" de forma abrangente para se referir a uma única avaliação de impacto, prevê (art. 27), entre outras formas de gestão de risco, a Avaliação de Impacto sobre Direitos Fundamentais (FRIA), exigida de entidades que implantam sistemas de IA de alto risco e sejam organismos de direito público ou operadores privados que prestam serviços públicos, ou operadores que implementam sistemas de análise de crédito (exceto para detecção de fraude) ou utilizados para avaliação de riscos e precificação de seguro de vida e de saúde. A avaliação detalha o uso previsto do sistema, identifica as populações afetadas e os riscos potenciais aos direitos fundamentais, devendo os resultados serem notificados à autoridade competente.

3.2. COMPARAÇÃO TÉCNICA E METODOLÓGICA

Apesar das diferenças, RIPD e AIA compartilham fundamentos metodológicos: identificação de riscos, medidas de mitigação e documentação estruturada. A seguir, alguns pontos comparativos práticos:

Item	RIPD	AIA e FRIA
Base Normativa	LGPD e GDPR	AI Act, NIST AI RMF, OCDE AI Principles, ISO/IEC 42001
Gatilho para Aplicação	Tratamento de dados pessoais com alto risco, de dados sensíveis ou com fundamento no legítimo interesse	Desenvolvimento, aquisição ou uso de sistemas de IA, especialmente de alto risco
Foco Principal	Privacidade, proteção de dados e conformidade jurídica	Riscos técnicos, éticos e sociais relacionados ao uso de IA
Objeto de Análise	Dados pessoais e suas operações de tratamento	Sistema de IA como um todo: modelo, lógica, dados, contexto de uso
Ciclo de Vida Analisado	Ciclo completo: coleta, uso, armazenamento, compartilhamento e exclusão	Todo ciclo de vida do sistema de IA: design, testes, implementação e monitoramento
Participação Multidisciplinar	Jurídico, DPO, segurança da informação	Jurídico, DPO, engenharia, ciência de dados, *compliance*, ética
Aspectos de Risco Abordados	Base legal, minimização, segurança e direitos dos titulares	Viés, explicabilidade, acurácia, robustez, impactos sociais e discriminatórios

Fonte: VLK Advogados

3.3. COMPLEMENTARIDADE E REAPROVEITAMENTO

A integração entre RIPD e AIA é possível e recomendável, especialmente quando o sistema de IA envolver o tratamento de dados pessoais. O RIPD pode servir como a base jurídico-regulatória para a construção da AIA, a qual ampliará o escopo de análise e incorporar aspectos técnico-sociais da governança algorítmica, incluindo:

- Avaliação de vieses discriminatórios e impactos desiguais em grupos sociais;
- Verificação de explicabilidade, robustez e acurácia dos sistemas automatizados; e
- Análise de externalidades, riscos coletivos e efeitos sistêmicos sobre direitos fundamentais.

Tanto o *EU AI Act* quanto o PL 2338/21 preveem o aproveitamento de RIPDs existentes, como base para a AIA, desde que o conteúdo seja expandido[21] para incluir aspectos técnicos e éticos específicos da IA, passando a trazer:

- O funcionamento técnico do sistema de IA;
- Os riscos éticos e não relacionados a dados pessoais;
- Medidas específicas para IA, como revisão humana e mitigação de vieses;
- Acurácia estatística, robustez técnica e segurança contra eventuais ataques adversariais; e
- Explicabilidade e impacto ambiental.

A própria ANPD já se manifestou no seguinte sentido[22]:

> "Ambos os mecanismos compõem um ferramental de governança que tem o objetivo de antecipar e abordar potenciais problemas antes que eles ocorram. Para uma governança eficaz, é essencial que haja clareza sobre como esses dois mecanismos se relacionam e se complementam. Pode-se considerar a relação dessas avaliações, garantindo que, ao avaliar sistemas de IA, tanto os impactos algorítmicos quanto os de proteção de dados sejam considerados de forma integrada".

Na prática, o DPO pode liderar a elaboração do RIPD e colaborar com a AIA ou até mesmo elaborá-la, respeitando os limites técnicos da sua atuação. Em organizações maduras, essa integração permite visão mais holística dos riscos e assegura a conformidade legal junto com a responsabilidade ética e a segurança técnica.

3.4. LIMITAÇÕES E AÇÕES PRAGMÁTICAS

Aplicados isoladamente, RIPD e AIA podem deixar lacunas de análise, comprometendo a efetividade da governança. Veja exemplos:

Situação Crítica	Riscos Associados	Ações Recomendadas
Realizar apenas o RIPD em projetos com IA	Desconsidera aspectos como viés, explicabilidade e impactos éticos	Expandir o escopo do RIPD, incorporando os mencionados elementos essenciais da AIA
Conduzir AIA sem análise jurídica estruturada	Insegurança sobre a legalidade do tratamento de dados	Integrar análise jurídica conforme LGPD, GDPR e fundamentos legais relacionados
Produzir documentos formais e isolados	Baixa efetividade prática e risco de desconexão entre áreas	Criar modelos integrados e funcionais

Fonte: VLK Advogados

3.5. CHECKLIST PARA O DPO

a) Aplicação Integrada

- ☐ Tenho clareza sobre quando utilizar o RIPD, a AIA ou ambos.
- ☐ Os documentos são integrados ou complementares, evitando retrabalho e lacunas de escopo.
- ☐ Em projetos com IA que tratam dados pessoais, sempre considero as exigências da LGPD, além das diretrizes do AI Act e do PL 2.338 e outros frameworks de governança.

b) Metodologia e Participação

- ☐ Existe metodologia formal para condução de RIPDs e AIAs, com etapas, responsáveis e critérios definidos.
- ☐ As avaliações contam com participação multidisciplinar: jurídico, técnico, segurança da informação e ciência de dados.
- ☐ As análises incluem aspectos técnicos (robustez, acurácia), legais (base jurídica, direitos) e éticos (viés, impacto social).

c) Reaproveitamento e Eficiência

- ☐ Os RIPDs são reutilizados como insumo direto para compor ou iniciar AIAs.
- ☐ A equipe conhece modelos de referência (NIST AI RMF, OCDE AI Principles, ISO/IEC 42001) e os aplica conforme necessário.
- ☐ Existe histórico organizado das avaliações realizadas, com lições aprendidas e plano de ação monitorado.

d) Limites e Ações Corretivas

- ☐ São mapeadas as limitações de cada tipo de avaliação e adotadas ações complementares (ex: simulações e revisões externas).
- ☐ Existe procedimento para revisão periódica dos documentos de RIPD e AIA, especialmente após mudanças em modelos de IA.
- ☐ A organização sabe justificar, de forma documentada, por que uma avaliação foi realizada ou dispensada.

4. Direitos dos Titulares e das Pessoas Afetadas: desafios e caminhos para a governança integrada

4.1. DOIS MARCOS REGULATÓRIOS, UM MESMO CENTRO: A PESSOA

A proteção de dados pessoais (LGPD, GDPR) e a governança de IA (AI Act, ISO/IEC 42001, NIST AI RMF) partem de premissas distintas, mas convergem em um ponto essencial: a proteção da pessoa humana.

- A LGPD se estrutura em torno dos titulares de dados pessoais.
- O AI Act e demais normas de IA ampliam o foco para qualquer pessoa afetada por sistemas algorítmicos, mesmo que não identificável nos dados tratados.

Essa ampliação exige novo olhar regulatório: nem todo risco de IA decorre do uso de dados pessoais, mas IA de alto risco pode impactar direitos fundamentais, inclusive de quem não é titular de dados no sentido estrito da LGPD.

4.2. DESAFIOS DE APLICAÇÃO: IA, VIESES E TRANSPARÊNCIA

As tecnologias de IA desafiam a aplicabilidade prática dos direitos previstos na legislação de proteção de dados. Quatro desafios principais estão envolvidos nesta questão:

- **Vieses algorítmicos** que afetam grupos ou coletividades;
- **Decisões automatizadas** com impacto significativo, mas sem clareza sobre quem é o "titular" afetado;
- **Dificuldade de explicabilidade**, o que compromete o exercício dos direitos de revisão e oposição;
- **Dados derivados ou inferidos**, que não foram fornecidos pelo titular, mas afetam diretamente sua vida.

A LGPD (art. 20) garante o direito à revisão de decisões automatizadas, mas sua efetividade prática ainda é limitada. O GDPR vai além ao trazer aos titulares a possibilidade de solicitar revisão humana. Decisão do Tribunal de Justiça da União Europeia (TJUE) reforçou essa exigência, ao considerar ilegal a ausência de revisão humana em sistemas de pontuação de crédito, sendo entendido como violação à autodeterminação informativa[23].

A governança de IA deve ser construída com base na justiça algorítmica, transparência e proporcionalidade, não se limitando à perspectiva tradicional de "titular de dados".

Importante lembrar que o direito fundamental dos indivíduos à transparência e à compreensão de como as decisões automatizadas afetam suas vidas não significa a entrega do algoritmo ou todas as suas complexidades técnicas, o que poderia, inclusive, comprometer segredo comercial. O que é exigido é explicação compreensível e útil da lógica subjacente à decisão.

A maioria das decisões automatizadas não trazem grandes riscos. A explicabilidade dos algoritmos precisa ser ponderada e aplicada de acordo com o respectivo risco aos indivíduos.

Ainda, a heterogeneidade de perfis exige que a explicabilidade seja pensada enquanto processo de comunicação graduada, e não como resposta única, genérica ou excessivamente técnica. Prática recomendável é a adoção de explicações em camadas: parte-se de camada inicial, acessível, com visão geral da lógica da decisão, e, a partir dela, são oferecidos caminhos para o aprofundamento, conforme o interesse, a necessidade e o nível de compreensão do público envolvido, sendo protegido o segredo comercial.

Modelos de explicabilidade devem traduzir a "lógica" do algoritmo em termos compreensíveis sem expor o código-fonte, como: explicar quais fatores foram considerados pelo sistema para chegar à decisão; identificar quais dados foram mais relevantes na predição; apresentar como a variação nesses dados afeta o resultado; indicar as possíveis consequências daquela decisão automatizada.

4.3. DA PROTEÇÃO DE DADOS À PROTEÇÃO DE PESSOAS

Governança eficaz exige foco nos efeitos da IA sobre os indivíduos. O papel do DPO, que passe a acumular funções de governança de IA, deve evoluir de guardião da conformidade para articulador de proteção ética, social e técnica. Isso exige atuação coordenada com áreas de risco, tecnologia, *compliance* e direitos humanos.

É nessa convergência que RIPD e AIA ganham relevância. Ambas devem proteger não apenas dados, mas pessoas. O foco deve ser a mitigação de impactos em escala individual e coletiva. Para tanto, é recomendável:

- Abranger no conceito de "titular" as pessoas afetadas por decisões algorítmicas (lembrando que as avaliações se aplicariam para alto risco);
- Incorporar o conceito de "afetado" em relatórios de impacto e canais de resposta;
- Avaliar impactos coletivos, como parte do risco regulatório e reputacional.

4.4. CAMINHOS PARA INTERPRETAÇÃO LEGAL E GOVERNANÇA INTEGRADA

Para mitigar riscos, antecipar possíveis exigências regulatórias e gerar confiança aos titulares e pessoas afetadas, é recomendável:

- Ampliar os canais de exercício de direitos, para incluir mecanismos de revisão, contestação e esclarecimento de decisões automatizadas;
- Revisar políticas de privacidade com base em Legal Design e Visual Law, detalhando impactos de IA;
- Integrar o DPO e o CAIO em comitês de ética e risco, especialmente em contextos de impacto coletivo; e
- Criar mecanismos de escuta ativa com stakeholders, incluindo testes com usuários reais e feedb*ack* contínuo.

4.5 CHECKLIST PARA O DPO

a) Compreensão e Escopo

- ☐ Reconheço que nem todos os impactos da IA se restringem à proteção de dados pessoais.
- ☐ Políticas e relatórios consideram também pessoas afetadas indiretamente, mesmo que não sejam titulares no sentido estrito da LGPD.
- ☐ Avaliações de impacto abordam riscos sociais, éticos e coletivos, além dos jurídicos.

b) Transparência e Comunicação

- ☐ As comunicações sobre uso de IA são claras quanto a critérios de decisão, lógica e efeitos potenciais.
- ☐ Há a possibilidade de solicitar revisões humanas para decisões automatizadas comprovadamente de alto impacto.
- ☐ É usada linguagem simples, Legal Design e estratégias de educação.

c) Exercício de Direitos

- ☐ Os canais de atendimento consideram titulares e qualquer pessoa impactada por IA.
- ☐ Há meios efetivos para mecanismos de revisão, contestação e esclarecimento de decisões automatizadas.
- ☐ Os direitos dos titulares estão adaptados às realidades algorítmicas (explicabilidade, proporcionalidade e não discriminação).

d) Governança Colaborativa

- ☐ DPO e CAIO atuam conjuntamente em casos com potencial de afetar direitos fundamentais de forma ampla.
- ☐ O comitê de governança considera impactos em grupos vulneráveis.
- ☐ Há protocolos claros para responder a denúncias, reclamações ou efeitos adversos não previstos, assim como incidentes de segurança.

Considerações Finais

À medida que os sistemas algorítmicos se tornam mais sofisticados e com maior impacto social, os papéis do DPO e do CAIO ganham relevância estratégica. O DPO, antes restrito ao *compliance* em proteção de dados pessoais, passa a desempenhar papel transversal na governança digital, contribuindo na identificação de riscos, na avaliação ética e na promoção da transparência. Já o CAIO surge como liderança voltada à inovação e à execução da estratégia de IA, com foco no valor de negócio, mas também com corresponsável pela integridade algorítmica.

Ao longo deste eBook, analisamos a distinção e possível sobreposição entre essas duas funções. A experiência prática e os entendimentos de autoridades ao redor do mundo indicam que a acumulação de papéis exige análise de conflito de interesse.

Demonstramos também que estruturas de governança de dados bem consolidadas, incluindo RIPDs, comitês e políticas internas, representam ativos valiosos para a governança de IA. Contudo, sua reutilização exige adaptações metodológicas e éticas voltadas aos desafios específicos dos sistemas algorítmicos.

Exploramos, ainda, como RIPDs e AIAs se complementam, fornecendo bases robustas para o mapeamento, a mitigação e a justificativa dos riscos relacionados à privacidade e aos efeitos sistêmicos da IA. A integração entre esses instrumentos fortalece a prestação de contas e a confiança institucional.

Ampliamos a lente da proteção jurídica: embora o ponto de partida continue sendo o titular de dados, recomenda-se considerar, especialmente no contexto de avaliações de alto risco, os possíveis impactos sobre qualquer pessoa afetada por decisões automatizadas. Nesse sentido, a governança de IA evolui para incorporar, além da proteção de dados, preocupações mais amplas com dignidade humana, não discriminação e justiça social.

Nesse cenário, DPO e CAIO não competem. São parceiros estratégicos. Cada qual, a partir de seu campo de atuação, contribui para garantir que a IA seja tecnicamente robusta, juridicamente segura, socialmente legítima e eticamente defensável.

O futuro da IA nas organizações brasileiras será definido não apenas pela capacidade de inovar, mas pela maturidade em governar com responsabilidade, confiança e propósito. O DPO bem-preparado será figura-chave nesse processo, não para frear a inovação, mas para viabilizá-la de forma justa, auditável e centrada nas pessoas. É o Direito impulsionando a inovação com ética e efetividade.

Governar a Inteligência Artificial de forma ética e responsável reduz riscos regulatórios e reputacionais; antecipa tendência normativa; aumenta a eficiência operacional e a qualidade das decisões automatizadas; fortalece a reputação institucional; atrai e retém talentos; estimula a confiança de *stakeholders*, clientes, investidores e sociedade; e impulsiona uma inovação segura, sustentável e alinhada às expectativas sociais e ao ESG.

*****

Outros materiais relevantes sobre o tema

- IA Reponsável em Dados
- Por que governar a IA no cenário de incerteza regulatória
- O Futuro da Privacidade
- IA e Reponsabilidade civil dos agentes
- EU AI Act: Mapa Interativo das Obrigações e Categorias de Riscos
- O Encarregado (DPO) e sua relevância para as organizações

Notas e Referências

[1] O AI Index Report 2025 foi realizado entre janeiro e fevereiro de 2025, coletou respostas de 1.500 organizações com faturamento mínimo anual de US$ 500 milhões, em 20 países e 19 setores.

[2] Gen AI Adoption Index . Esses achados vêm de pesquisa realizada pela Access Partnership em colaboração com a Amazon Web Services (AWS). Tomadores de decisão de TI envolvidos em investimento e implementação de tecnologia em mais de 3.739 organizações em nove países — Estados Unidos da América (EUA), Brasil, Canadá, França, Alemanha, Japão, Índia, Coreia do Sul e Reino Unido (UK). No Brasil, 411 tomadores de decisão de TI foram entrevistados. Disponível aqui.

[3] "Winning the Race - AMERICA'S AI ACTION PLAN", de Julho de 2023. Disponível aqui.

[4] Gartner, Inc. com mais de 1.800 líderes executivos, de junho de 2024. Disponível aqui.

[5] Disponível aqui.

[6] AI Governance Profession Report 2025. IAPP e Credo AI. O relatório baseia-se em duas fontes de dados, sendo a principal a pesquisa anual de governança da IAPP, realizada na primavera de 2024. Participaram mais de 670 profissionais de 45 países e territórios, respondendo a perguntas demográficas sobre o porte e a receita das organizações, além de 25 questões específicas sobre governança de inteligência artificial. A pesquisa buscou avaliar práticas institucionais, estruturas de governança e o grau de confiança dos respondentes em relação às abordagens adotadas por suas organizações. Disponível aqui.

[7] CENTRE FOR INFORMATION POLICY LEADERSHIP (Hunton Andrews Kurth LLP). Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL *Accountability* Framework. Fevereiro de 2024. Disponível aqui.

[8] CENTRE FOR INFORMATION POLICY LEADERSHIP (Hunton Andrews Kurth LLP). Building Accountable AI Programs: Mapping Emerging Best Practices to the CIPL *Accountability* Framework. Fevereiro de 2024. Disponível aqui. Acesso em: 20 jul. 2025.

[9] Disponível aqui.

[10] ANPD. Guia orientativo Atuação do encarregado pelo tratamento de dados Pessoais. Dezembro de 2024. Disponível aqui.

[11] PALLARDY, Carrie. How will the role of chief AI officer evolve in 2025? InformationWeek, 18 abr. 2025. Disponível aqui. Acesso em: 18 jul. 2025.

[12] Vide Guia Orientativo sobre Atuação do encarregado pelo tratamento de dados pessoais, elaborado pela ANPD. Disponível aqui.

[13] Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023. Nota Técnica nº 16/2023/CGTP/ANPD. Disponível aqui.

[14] AI Governance Profession Report 2025 – a partir da página 19.

[15] Avaliação de Impacto dos Direitos Fundamentais. Obrigação legal prevista no art. 27 do *EU AI Act*.

[16] Conforme "Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023". Nota Técnica nº 16/2023/CGTP/ANPD. Disponível aqui.

[17] IAPP; EY. Annual *Privacy Governance Report* 2023: Executive Summary. 2023. Disponível aqui. Acesso em: 20 jul. 2025.

[18] CISCO. *Cisco privacy benchmark* study 2024. [S.l.]: Cisco, 2024. Disponível aqui. Acesso em: 20 jul. 2025.

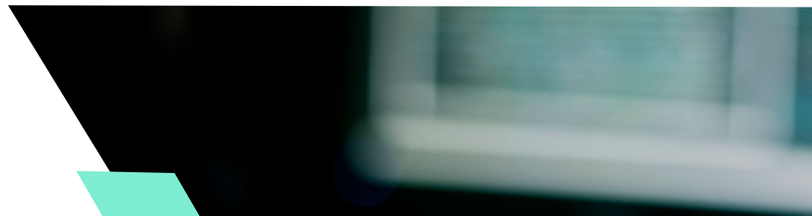
[19] MASLEJ, Nestor et al. The AI Index 2025 Annual Report. Stanford: AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, 2025. Disponível aqui.

[20] Conforme texto aprovado no Senado em 10/12/24.

[21] LAPIN – Laboratório de Políticas Públicas e Internet. Relatório sobre o Marco Regulatório da Inteligência Artificial no Brasil. Brasília: LAPIN, abr. 2023. Disponível aqui.

[22] Conforme "Sugestões de incidência legislativa em projetos de lei sobre a regulação da Inteligência Artificial no Brasil, com foco no PL nº 2338/2023". Nota Técnica nº 16/2023/CGTP/ANPD. Disponível aqui.

[23] UNIÃO EUROPEIA. Judgment of the Court (First Chamber) of 7 December 2023 — OQ v Land Hessen (Case C 634/21, SCHUFA Holding (Scoring)); Jornal Oficial da União Europeia, série C, n. 913, de 29.1.2024. Disponível aqui. Acesso em: 20 jul. 2025.



CHECKLISTS CONSOLIDADOS: O PAPEL DO DPO NA GOVERNANÇA DE IA

1. AS DISTINÇÕES E SINERGIAS ENTRE DPO E O CAIO

a) Independência e Conflito de Interesse

- ☐ Minhas funções atuais não incluem decisões operacionais sobre IA (modelos, critérios ou implementação).
- ☐ Existe avaliação formal e documentada de ausência de conflito de interesse, conforme disposto pela ANPD .
- ☐ Caso eu exerça outras funções, elas não afetam minha imparcialidade como DPO.
- ☐ Tenho autonomia técnica para emitir pareceres contrários à estratégia de IA, se necessário.

b) Estrutura e Reporte

- ☐ Minha atuação está formalmente registrada, com escopo e responsabilidades claros.
- ☐ Reporto diretamente à Alta Administração ou ao Conselho.
- ☐ Participo de comitês de risco, mas sem responsabilidade executiva sobre IA.

c) Colaboração com o CAIO e outros *stakeholders*

- ☐ Há processos estruturados de colaboração com o CAIO e áreas técnicas.
- ☐ A governança de IA contempla os direitos fundamentais, privacidade e explicabilidade.
- ☐ Participo das Avaliações de Impacto Algorítmico (AIAs) que envolvem dados pessoais ou direitos do titular.

d) Modelo proporcional ao porte e maturidade da organização

- [ ] A estrutura atual (acúmulo ou separação de funções) foi adotada com base em análise formal do porte, orçamentário, riscos e da maturidade digital da organização.
- [ ] Em caso de acúmulo de funções, foram adotadas salvaguardas como reporte independente, validação externa ou revisão periódica.
- [ ] Estruturei mecanismo para revisar a estrutura organizacional, conforme a evolução dos riscos e projetos.

e) Capacitação e Atualização Contínua

- [ ] Recebo formação contínua sobre IA, riscos algorítmicos e regulação (AI Act, LGPD, GDPR, ISO 42001, entre outros).
- [ ] Acompanho decisões regulatórias e boas práticas sobre a função do DPO e sua interface com a governança de IA.

2. CONVERGÊNCIA ENTRE AS ESTRUTURAS DE GOVERNANÇA DE DADOS PESSOAIS E IA

a) Estrutura Integrada de Governança

- [ ] A organização possui programa institucional que abrange dados pessoais e IA de forma integrada.
- [ ] Há comitê multidisciplinar para decisões sobre ética, risco e IA, com regulamento estruturado e aprovado.
- [ ] Os RIPDs são utilizados como base para a elaboração das AIAs.
- [ ] As políticas de governança de dados incluem diretrizes específicas para sistemas automatizados.

b) Comunicação Estratégica e Transparência

- [ ] As comunicações explicam, com linguagem clara e acessível, o uso de IA e os critérios automatizados.
- [ ] Os avisos de privacidade incluem menções específicas à finalidade da IA.

- [ ] Os canais de atendimento estão preparados para solicitações relacionadas IA.
- [ ] Há uso de *design* jurídico nos materiais voltados ao público, promovendo compreensão real sobre o uso de algoritmos.

c) Reaproveitamento de Estruturas e Ferramentas

- [ ] O comitê de privacidade tratar também de ética e risco em IA.
- [ ] Os treinamentos incluem tópicos como vieses, explicabilidade, responsabilidade algorítmica e uso ético de IA.
- [ ] Os contratos com terceiros incluem cláusulas sobre IA, auditoria e mitigação de riscos.
- [ ] A organização realiza due diligence técnica e ética em terceiros que desenvolvem ou operam soluções de IA.

d) Sustentabilidade e Maturidade Organizacional

- [ ] A estrutura de IA reaproveita processos e recursos da governança de dados.
- [ ] Há orçamento e equipe (dedicada ou compartilhada) para iniciativas de IA responsável.
- [ ] O DPO participa desde o início de projetos de IA que envolvem dados pessoais, contribuindo na avaliação de riscos e na definição de salvaguardas éticas e legais.
- [ ] O modelo adotado respeita o estágio de maturidade digital e é revisado conforme a evolução dos projetos e dos riscos envolvidos.

3. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (“RIPD”) E ANÁLISE DE IMPACTO ALGORÍTMICO (“AIA”);

a) Aplicação Integrada

- [ ] Tenho clareza sobre quando utilizar o RIPD, a AIA ou ambos.
- [ ] Os documentos são integrados ou complementares, evitando retrabalho e

lacunas de escopo.

☐ Em projetos com IA que tratam dados pessoais, sempre considero as exigências da LGPD, além das diretrizes do AI Act e do PL 2.338 e outros *frameworks* de governança.

b) Metodologia e Participação

☐ Existe metodologia formal para condução de RIPDs e AIAs, com etapas, responsáveis e critérios definidos.

☐ As avaliações contam com participação multidisciplinar: jurídico, técnico, segurança da informação e ciência de dados.

☐ As análises incluem aspectos técnicos (robustez, acurácia), legais (base jurídica, direitos) e éticos (viés, impacto social).

c) Reaproveitamento e Eficiência

☐ Os RIPDs são reutilizados como insumo direto para compor ou iniciar AIAs.

☐ A equipe conhece modelos de referência (NIST AI RMF, OCDE AI Principles, ISO/IEC 42001) e os aplica conforme necessário.

☐ Existe histórico organizado das avaliações realizadas, com lições aprendidas e plano de ação monitorado.

d) Limites e Ações Corretivas

☐ São mapeadas as limitações de cada tipo de avaliação e adotadas ações complementares (ex: simulações e revisões externas).

☐ Existe procedimento para revisão periódica dos documentos de RIPD e AIA, especialmente após mudanças em modelos de IA.

☐ A organização sabe justificar, de forma documentada, por que uma avaliação foi realizada ou dispensada.

4. DIREITOS DOS TITULARES E DIREITOS DAS PESSOAS AFETADAS POR IA

a) Compreensão e Escopo

☐ Reconheço que nem todos os impactos da IA se restringem à proteção de dados pessoais.

☐ Políticas e relatórios consideram também pessoas afetadas indiretamente, mesmo que não sejam titulares no sentido estrito da LGPD.

☐ Avaliações de impacto abordam riscos sociais, éticos e coletivos, além dos jurídicos.

b) Transparência e Comunicação

☐ As comunicações sobre uso de IA são claras quanto a critérios de decisão, lógica e efeitos potenciais.

☐ Há a possibilidade de solicitar revisões humanas para decisões automatizadas comprovadamente de alto impacto.

☐ É usada linguagem simples, Legal *Design* e estratégias de educação.

c) Exercício de Direitos

☐ Os canais de atendimento consideram titulares e qualquer pessoa impactada por IA.

☐ Há meios efetivos para mecanismos de revisão, contestação e esclarecimento de decisões automatizadas.

☐ Os direitos dos titulares estão adaptados às realidades algorítmicas (explicabilidade, proporcionalidade e não discriminação).

d) Governança Colaborativa

☐ DPO e CAIO atuam conjuntamente em casos com potencial de afetar direitos fundamentais de forma ampla.

☐ O comitê de governança considera impactos em grupos vulneráveis.

☐ Há protocolos claros para responder a denúncias, reclamações ou efeitos adversos não previstos, assim como incidentes de segurança.

Direito,
Inovação
& Tecnologia

SOBRE NÓS

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

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

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

AUTORES

Rony Vainzof
rony@vlklaw.com.br

Caio Lima
caio@vlklaw.com.br

Ingrid Soares
ingrid.soares@vlklaw.com.br

Giovanna Milanese
giovanna.milanese@vlklaw.com.br

Paulo Sarmento
paulo.sarmento@vlklaw.com.br

Direito,
Inovação
& Tecnologia

E-book "O Papel do DPO na Governança de IA",
de Agosto de 2025.