VLK ADV

WWW.VLKLAW.COM.BR

O FUTURO DA PRIVACIDADE:

Como estar preparado para

2025

- Contextualização e relevância do tema
- IA e Proteção de Dados
- Resolução e Guia do Encarregado da ANPD
- Transferência internacional de Dados Pessoais
- Cibersegurança e Resposta a incidentes

SUMÁRIO

1. CONTEXTUALIZAÇÃO E RELEVÂNCIA DO TEMA

Dados pessoais já ultrapassaram a analogia de "novo petróleo" e se consolidaram como a espinha dorsal de políticas públicas e um dos principais impulsionadores de mercados e economias modernas. Eles são recursos essenciais para a construção de estratégias econômicas e sociais que orientam a tomada de decisão em diferentes setores. Sua influência permeia desde a prevenção de fraudes e proteção ao crédito, até o marketing direcionado, o comércio digital, medicina preditiva e o desenvolvimento da IA.

Não por acaso, a Lei Geral de Proteção de Dados Pessoais (LGPD) também prevê como fundamento para a proteção de dados pessoais o desenvolvimento econômico e tecnológico e a inovação, trazendo maior segurança jurídica e um norte para as empresas em como utilizar os dados de forma ética, segura responsável. Agora, a LGPD já se encontra em uma nova fase, com a sua regulamentação e fiscalização pela Autoridade Nacional de Proteção de Dados (ANPD).

A agenda da ANPD mostra forte tendência de cobrar maior transparência em casos de incidentes, boas práticas de cibersegurança e nível de governança e documentos de accountability compatíveis com uma legislação existente há mais de 6 anos e já em vigor há mais de 4 anos, incluindo o registro das atividades de tratamento de dados pessoais atualizado, guarda de logs, mecanismos adequados para transferência internacional, avaliação de legitimo interesse e elaboração de relatório de impacto, quando aplicáveis, além de um Encarregado empoderado e com autonomia técnica nas organizações.

Assim, neste #PrivacyDay apresentamos quatro principais tendências de Governança de Privacidade em 2025, considerando as mais recentes e principais mudanças regulatórias que afetam a proteção de dados pessoais no Brasil e no mundo.

2. IA E PROTEÇÃO DE DADOS

O uso de sistemas de IA, sejam especializados ou de propósito geral, tornou-se essencial para a competitividade empresarial. Contudo, o desenvolvimento e a aplicação desses sistemas frequentemente envolvem o tratamento de dados pessoais, exigindo conformidade, entre outras, com a legislação de proteção de dados.

Diante da relevância da IA para a sociedade e de seus impactos potenciais sobre os titulares, as autoridades de proteção de dados têm intensificado esforços para assegurar o cumprimento das normas já aplicáveis. No Brasil, a ANPD tem dado atenção especial ao tema, com ações como:

- Tomada de Subsídios sobre IA e Proteção de Dados, visando à criação de regulamentações futuras sobre o tema;
- Adoção de medidas fiscalizatórias em projetos relacionados à IA, como o caso de treinamento de IA pela Meta e X e o Projeto Estádio Seguro;
- Manifestações sobre a intersecção do PL de IA (2.338/23) com a LGPD e as funções da ANPD;
- Radar Tecnológico acerca da IA Generativa; e
- Sandbox regulatório para IA.

Nesse contexto, vamos apresentar nosso entendimento sobre questões relevantes a serem consideradas na interseção entre IA e Proteção de Dados.

2.1 Como identificar e detalhar finalidades e bases legais no contexto de IA?

Ao falarmos de IA e proteção de dados é fundamental compreender que a Inteligência Artificial (IA) possui seu Ciclo de Vida estruturado em diversas fases, nas quais dados pessoais são tratados e, consequentemente, requerem a identificação clara das finalidades para o tratamento e a fundamentação em uma base legal.

De forma geral, o ciclo de vida da inteligência artificial pode ser dividido em **quatro etapas principais:** (1) projeto; (2) aquisição e preparação de dados; (3) treinamento, teste e validação; e, por fim, (4) implementação, aplicação e monitoramento [1]. É comum que o tratamento de dados pessoais ocorra nas três últimas etapas. Para fins deste tópico, as fases de aquisição e preparação de dados (2), bem como de treinamento, teste e validação (3), podem ser agrupadas em uma única etapa denominada "**desenvolvimento**".

2.2 Finalidade da atividade de tratamento

Ao selecionar a **finalidade da atividade de tratamento** é importante ter em consideração, além da etapa do ciclo de vida da IA, qual é o contexto relacionado com a IA que estamos tratando. Em linhas gerais, podemos falar de **três contextos distintos**[2]:

Desenvolvimento ou aplicação de Sistemas Especialistas:

Especialistas são os sistemas de IA desenvolvidos para usos operacionais específicos. Nessas hipóteses, a finalidade (seja no seu desenvolvimento ou em sua aplicação) geralmente corresponde ao objetivo operacional da IA. Assim, se se objetivar desenvolver IA para realizar cobranças, por exemplo, essa tende a ser a finalidade apontada em todo o ciclo de vida da IA.

Pesquisas Científicas relacionadas a IA:

No contexto da inteligência artificial, é comum a realização de pesquisas científicas para objetivos que incluem o desenvolvimento ou a avaliação da capacidade de modelos e a identificação de padrões úteis em bases de dados, que poderão ser aplicados futuramente em soluções baseadas em IA. Nessas situações, pode não ser viável estabelecer

finalidade específica no início do tratamento, uma vez que o uso efetivo dos dados dependerá dos resultados obtidos durante o processo de pesquisa e desenvolvimento. Por exemplo: um banco pode analisar dados transacionais para identificar padrões úteis nesses dados (ex. fraudes, inadimplência etc.). Só após descobrir, concretamente, os padrões é possível definir a finalidade específica para a qual os dados serão utilizados.

Nesses casos é admissível a definição de finalidades, porém genéricas (ex. descoberta de padrões úteis em dados, aprimoramento de produtos e serviços etc.), as quais devem ser mais detalhadas e concretizadas, conforme o resultado assim o permitir.

Desenvolvimento ou aplicação de Sistemas de IA de propósito geral:

Como o nome sugere, IA de propósito geral é aquela apta a desempenhar de forma eficiente diversas tarefas distintas, consequentemente, não existe finalidade clara e pré-estabelecida para a solução desde a fase de projetos.

Nesses casos, na etapa de desenvolvimento, a finalidade de treinar (ou desenvolver) a solução de propósito geral pode, em si mesma, ser finalidade legítima[3].

Considerando a aplicação de IA de Propósito Geral, é possível se deparar com duas situações distintas: a adaptação de um modelo de IA de propósito geral para finalidade específica (ex. por finetuning) ou sua disponibilização para o público-alvo como IA de propósito geral.

No primeiro caso, aplicam-se as regras para a Sistemas Especialistas de IA. No segundo caso, entendemos que o princípio da finalidade deve ser encarado de forma mais flexível, sendo abarcado não por uma finalidade específica e concretamente determinada, mas pelo conjunto de usos permitidos e proibidos, nos termos de eventual política de uso aceitável.

2.3 Base Legal – Aspectos Gerais

Igualmente, ao determinar a **base legal**, a finalidade e a etapa do ciclo de vida da IA devem ser considerados. Algumas bases legais podem ser mais propensas e apropriadas para o treinamento e/ou implantação de IA do que outras. Por exemplo [4]:

- Sistema de reconhecimento facial pode ser treinado para reconhecer rostos, mas essa funcionalidade pode ser usada para múltiplos propósitos, como prevenção de crimes, autenticação e marcação de amigos em uma rede social. Cada uma dessas aplicações adicionais pode exigir uma base legal diferente;

- Você implementa um sistema de IA de terceiros, qualquer tratamento de dados pessoais realizado pelo desenvolvedor terá sido para finalidade diferente (por exemplo, para desenvolver o sistema) daquela para a qual você pretende usar o sistema, portanto, você pode precisar identificar base legal diversa;

- O uso da base legal de “execução de contrato” é limitado àquelas hipóteses em que o tratamento é estritamente necessário para, concretamente, pactuar ou executar um contrato com o titular de dados. Assim, embora uma solução de IA possa ser utilizada para, por exemplo, executar atividade contratada com fundamento nessa base legal, a utilização de dados do titular para treinar esse sistema, como regra, não poderá se fundar nessa base.

Assim, enquanto na etapa de aplicação, as mais distintas bases legais sejam aplicáveis, conforme finalidade concreta da IA, as bases legais aplicáveis a etapa de desenvolvimento da IA, especialmente as de propósito geral, serão, principalmente, as seguintes:

- Legítimo Interesse;
- Consentimento; e
- Realização de Pesquisas, para agentes de tratamento que se enquadrem como órgãos de pesquisa.

É possível, ainda, que outras bases legais sejam aplicáveis no desenvolvimento de soluções de IA com propósito específico, especialmente:

- Prevenção a fraudes, para o desenvolvimento de soluções de identificação biométrica; e

- Proteção ao Crédito, para o desenvolvimento de soluções que avaliem o risco de crédito.

2.4 Qual é a base legal mais adequada no desenvolvimento de IA?

A exigência de consentimento no contexto do desenvolvimento da IA enfrenta desafios como falta de escalabilidade, sobrecarga aos indivíduos e impacto negativo em terceiros,

sendo mais adequado explorar bases legais como o legítimo interesse para atender à complexidade do ambiente digital e proteger direitos dos titulares de dados. Esses desafios incluem [1]:

- **Revalidação constante do consentimento:** alterações ou expansões na finalidade do tratamento requerem nova coleta de consentimento, tornando o processo oneroso e repetitivo.

- **Indefinição da finalidade no início do projeto:** projetos de pesquisa frequentemente não possuem finalidade específica no início, o que impede a validação do consentimento.

- **Garantia de informação adequada e granularidade:** é desafiador oferecer explicações claras, detalhadas e compreensíveis em contextos técnicos complexos.

- **Possibilidade de revogação do consentimento:** a exclusão de dados, especialmente em bases não estruturadas, pode ser tecnicamente difícil e comprometer a eficácia do sistema, particularmente em situações de alta demanda por exclusões.

Dessa forma, o legítimo interesse se mostra mais adequado, desde que, satisfeitos seus requisitos de enquadramento – isto é, a atividade seja aprovada no teste de balanceamento.

2.5 Quais cuidados são importantes para fundamentar o desenvolvimento de IA no legítimo interesse?

Assim como em qualquer atividade de tratamento de dados, o enquadramento no legítimo interesse no contexto do desenvolvimento de IA exige a realização do Teste de Balanceamento. Nesse Teste, o tratamento de dados deve atender aos seguintes critérios:

- **Ausência de dados pessoais sensíveis:** O tratamento não pode envolver categorias de dados pessoais sensíveis.

- **Fundamentação em um interesse legítimo:** O interesse deve ser legítimo, podendo ser do agente de tratamento, de um terceiro ou da sociedade.

- **Necessidade razoável:** O tratamento deve ser indispensável para alcançar o(s) interesse(s) legítimo(s) pretendido(s).

- **Razoabilidade dos interesses legítimos:** O interesse legítimo perseguido não pode ser superado pelos impactos negativos nos direitos e interesses dos titulares dos dados.

Embora as medidas para atender a esse teste dependam do caso concreto, algumas práticas podem aumentar significativamente as chances de enquadramento no legítimo interesse:

- **Filtragem de dados:** Ao minerar informações da internet ou utilizar bases open-source, é comum que dados pessoais sensíveis sejam coletados, mesmo que de forma não intencional. Para mitigar esses riscos, recomenda-se realizar filtragens em duas etapas [2]:

  1. Antes da coleta:

  Defina critérios precisos que reduzam a probabilidade de capturar dados pessoais sensíveis;

  2. Após a coleta, mas antes do treinamento da IA:

  Adote processos para anonimizar ou excluir dados sensíveis coletados, sempre que possível, e documente essas etapas de forma detalhada.

- **Definição de hipóteses:** para assegurar que os dados tratados sejam razoavelmente necessários às finalidades almejadas, é recomendável justificar, por meio de hipóteses bem fundamentadas, a lógica de vinculação entre os dados utilizados e a finalidade pretendida;

- **Minimização de dados:** sempre que possível e sem comprometer o desempenho do sistema, priorize a anonimização ou, no mínimo, a pseudonimização dos dados de treinamento. Essa prática reduz impactos potenciais aos titulares; e

- **Opt-out facilitado:** garantir aos titulares a possibilidade de escolha é essencial para preservar sua autonomia e alinhar-se às suas expectativas. Assim, é fundamental oferecer mecanismo claro e acessível para o exercício do Direito de Oposição, preferencialmente com destaque nas configurações padrão do portal de privacidade ou outra solução

adotada pela organização para gerenciar solicitações dos titulares [3].

- **Transparência:** para a fundamentação da atividade no legítimo interesse é relevante a prestação de informações apropriadas aos titulares sobre as finalidades e dados tratados. No caso de desenvolvimento de IA de Propósito Geral é recomendável o fornecimento de informações das capacidades esperadas do modelo.

2.6 Qual a diferença entre o Relatório de Impacto à Proteção de Dados (RIPD) e a Avaliação de Impacto Algorítmico (AIA)?

A Avaliação de Impacto Algorítmico (AIA) e o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) são instrumentos distintos de análise de riscos, embora apresentem similaridades. O RIPD, previsto na LGPD, é obrigatório em situações de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais, conforme os arts. 5º, XVII e 38 da Lei. Ele foca exclusivamente nos impactos do tratamento de dados pessoais sobre indivíduos, abordando dados tratados, metodologias utilizadas e medidas de mitigação para proteger direitos fundamentais, sempre observando os segredos comerciais e industriais.

Já a AIA, embora ainda não seja obrigação legal neste momento, estando prevista no Projeto de Lei nº 2338/21, é mais abrangente, indo além dos riscos relacionados ao tratamento de dados pessoais, porém também busca avaliar os impactos sobre direitos fundamentais. Ela considera todo o funcionamento de sistemas de IA incluindo a programação, a imprevisibilidade do algoritmo e possíveis externalidades negativas em qualquer contexto de atuação da tecnologia. Além de aspectos legais, a AIA aborda reflexões éticas, impactos intencionais e não intencionais e estratégias de mitigação. Contudo, pela ausência de regulamentação específica, a AIA carece de padrão universal para sua implementação, resultando em discricionariedade e falta de orientações claras sobre sua metodologia.

2.7 Quando fazer?

O RIPD, é definido no art. 5º, XVII, da LGPD, como a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem

gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

Assim, considerando que, pela própria natureza da tecnologia, o tratamento de dados pessoais pela IA envolve tratamento automatizado de dados, o RIPD será necessário sempre que a atividade de tratamento se opere em larga escala ou puder gerar danos significativos aos direitos e interesses do titular.

Já a AIA, (considerando a aprovação do PL 2338/21[4][5], deverá ser realizada, em momento anterior à introdução ou à colocação em circulação no mercado de sistema de IA, sempre que o desenvolvedor ou aplicador introduzir ou colocar sistema de IA em circulação no mercado, quando o sistema ou o seu uso forem de alto risco, considerando o papel e a participação do agente na cadeia – isto é, quando o uso pretendido da IA, por si só, puder impactar significativamente os direitos e interesses fundamentais das pessoas afetadas.

Conforme a própria ANPD [5] , apesar de o escopo de tratamento de um RIPD ser restrito a contextos que envolvam tratamento de dados pessoais e sua análise limitada à gestão de riscos a liberdades e direitos fundamentais afetados em virtude deste tratamento, é indubitável a correlação entre as duas ferramentas, tanto no aspecto metodológico de sua elaboração, quanto no conteúdo (para os casos em que sistemas de IA tratem dados pessoais). Inclusive, o

Laboratório de Políticas Públicas e Internet (LAPIN) comenta que, como a AIA é usada para gerir riscos de sistemas de IA a direitos fundamentais, inevitavelmente, os direitos à privacidade e à proteção de dados pessoais devem ser considerados na análise [6].

2.8 É possível reaproveitar o RIPD para o AIA? Como?

Sim, inclusive o próprio EU AI Act prevê essa possibilidade [7]. O PL 2.338/23 também prevê que caso o agente de IA tenha que elaborar RIPD, nos termos da LGPD, a AIA poderá ser realizada em conjunto com o referido documento.

Conforme o art. 38, parágrafo único, da LGPD, o RIPD envolve, no mínimo a:

(i) descrição dos tipos de dados coletados;

(ii) metodologia utilizada para a coleta e para a garantia da segurança das informações; e

(iii) análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

De igual modo, o AIA, geralmente, envolve uma descrição:

(a) do sistema e de sua utilização;

(b) das medidas adotadas para conformar o sistema aos princípios da IA;

(c) de uma avaliação dos riscos às pessoas afetadas; e

(d) das medidas a serem adotadas para mitigar referidos riscos, incluindo de supervisão humana, e tratamento de sua eventual materialização.

Assim, é possível reaproveitar o RIPD para o AIA, desde que este seja complementado, no seguinte sentido:

- A descrição da atividade de tratamento seja aprofundada, de modo a abarcar o funcionamento e aplicação do sistema de IA como um todo;

- Aprofundamento dos princípios, de modo que passem a abarcar quesitos próprios de IA. Por exemplo:
  1. Autonomia e critérios de revisão humana;
  2. Ao abordar o princípio da não-discriminação é importante destacar as medidas adotadas quanto à seleção da base de dados e os testes no sistema para evitar vieses;
  3. Ao abordar o princípio da qualidade, é necessário destacar as medidas para garantir a acuracidade estatística do sistema, evitando alucinações de IA e outros resultados incorretos ou imprecisos.
  4. Ao abordar os princípios da prevenção e segurança, é importante destacar as medidas adotadas para garantir a robustez técnica da IA (ex. planos aprova de falhas) e proteger o sistema de ataques tipicamente voltados à soluções de IA (ex. ataques adversariais);
  5. Explicabilidade: deve determinar se o sistema de IA é suficientemente explicável e interpretável para os desenvolvedores e usuários;

- Confiabilidade: sistema de IA produz resultados consistentes;

- Resiliência e continuidade: considerar plano de ação, caso haja algum problema com o sistema de IA;

- Avaliação de Impacto Ambiental.

3. RESOLUÇÃO E GUIA DO ENCARREGADO DA ANPD (No 18/2024)

A economia e os negócios contemporâneos estão cada vez mais impulsionados por dados pessoais, força motriz de diversas transações econômicas e vetores essenciais para o desenvolvimento de diversos mercados. Nesse contexto, o papel desempenhado pelo Encarregado ganha fundamental importância e se apresenta como estratégico ao ocupar posição central na garantia da conformidade, em especial, do controlador com a legislação de proteção de dados pessoais no Brasil.

A relevância do Encarregado (ou Data Protection Officer - DPO) passou a ser melhor assimilada quando o tratamento lícito, ético e responsável dos dados pessoais se revelou como um grande diferencial competitivo entre os agentes econômicos [1] [2]. A posição se tornou mais valorizada e mais recursos passaram a ser disponibilizados para a proteção de dados dentro das organizações. [3] O aumento do orçamento das empresas destinado a proteção de dados traz retorno sobre o investimento por meio da melhoria da confiança de clientes, de parceiros de negócio e da conformidade regulatória.

A Autoridade Nacional de Proteção de Dados (ANPD) regulamentou o tema por meio da Resolução nº CD/ANPD nº 18/2024[4] e trouxe, recentemente, boas práticas com o Guia Orientativo publicado em dezembro de 2024 [4].

3.1 Da nomeação do Encarregado e do Encarregado Substituto

A nomeação do Encarregado é uma obrigação legal do controlador, detalhada na Resolução nº 18 e reforçada no Guia Orientativo de Atuação do Encarregado. Por não haver semelhante obrigação ao operador ou aos agentes de pequeno porte de forma expressa, a nomeação de Encarregado é facultativa, sendo considerada boa prática.

De acordo com esses documentos, deve haver a indicação formal do Encarregado (e um substituto ou “DPO Interino”), suas formas de atuação e das atividades a serem desempenhadas. Entretanto, o Encarregado substituto não precisa ser indicado no mesmo ato, logo isso ficará à escolha do agente de tratamento que poderá definir o momento mais oportuno para tanto (ex. na véspera das férias do Encarregado titular, ou em situações de conflito de interesse), desde que se garanta a ocupação constante do cargo para viabilizar o exercício dos direitos dos titulares de dados pessoais e/ou atendimento às comunicações da ANPD.

É preciso indicar o nome e os dados de contato do Encarregado?

Embora obrigação legal controversa por colocar em risco alguns direitos fundamentais, a Resolução exige e o Guia ratifica a necessidade da divulgação pública da identidade (nome completo) e as informações de contato do Encarregado e, no caso de o Encarregado ser uma pessoa jurídica, além da razão social desta, o nome completo da pessoa natural responsável também deve ser publicamente informado em local de destaque e fácil acesso, de forma clara e objetiva,

no website ou em qualquer outro meio de comunicação disponível e utilizado para contato com os titulares, a, incluindo quando o Encarregado for externo à organização (DPO as a Service). No caso de informações de contato, atende a exigência legislativa, a indicação de um e-mail ou telefone do Encarregado.

Portanto, enquanto vigente essa obrigação legal, os controladores devem cumpri-la. Inclusive, a ANPD, no final de 2024 divulgou notícia em seu website sobre a instauração de 20 (vinte) procedimentos fiscalizatórios contra controladores que teriam falhado em indicar Encarregado e em disponibilizar canal de comunicação direito e/ou efetivo com os titulares de dados [5].

3.2 O que é conflito de interesse e qual a sua importância para o Encarregado?

A ANPD, seguindo exemplo europeu no tema, ressalta que a inexistencia de "conflito de interesses" é pressuposto para acumulação de funções, visando assegurar a atuação independente e autonomia técnica do Encarregado.

O conceito de conflito de interesse é trazido pela Resolução nº 18/2024 e se configura em "situações que possam vir a comprometer, influenciar ou afetar, de maneira imprópria, a objetividade e o julgamento técnico do Encarregado no desempenho das suas atribuições". Sua análise, portanto, deve ser feita caso a caso.

Nesse sentido, para a ANPD e autoridade de dados e organismos europeus, algumas situações são exemplos de conflito de interesse, a saber:

- Conflito de interesse entre atribuições exercidas internamente pelo Encarregado em um agente de tratamento com funções/cargos:

1. Que envolvam decisões sobre proteção de dados na organização;
2. De alta direção, como Diretor Executivo, Diretor Operacional, Diretor Financeiro, Diretor Médico, Diretor de Marketing, Diretor de RH, Diretor de TI ou de Segurança da Informação, Diretor de Compliance, Auditoria e Riscos (WP29 e EDPB, autoridade de proteção de dados da Bélgica);
3. Inferiores na estrutura organizacional da empresa, quando o desempenho deles conduzir à determinação das finalidades e dos meios de tratamento de dados pessoais, como o caso de Gerente de TI, ou advogado do Departamento Jurídico de uma empresa que também a defende em causas sobre dados pessoais (WP29 e EDPB, CNIL, ICO);
4. Que tenham objetivos concorrentes e que coloquem a proteção de dados pessoais em segundo plano em relação aos interesses comerciais da empresa (ICO).

- Conflito de interesse no exercício da atividade de Encarregado em agentes de tratamento distintos:

1. comprometimento do desempenho eficaz das funções, levando em consideração a estrutura e dimensão dessas organizações;
2. ausência de recursos necessários para desenvolvimento de seu papel nas organizações e inexistência de apoio de uma equipe, quando necessário;
3. empresas com interesses divergentes;
4. impossibilidade de acesso ao Encarregado que atende um grupo de empresas (matriz e filiais) em virtude da falta de organização adequada.

Deste modo, embora o Encarregado não possa acumular suas funções com aquelas que envolvam decisões sobre proteção de dados na organização, o agente de tratamento, pela Resolução nº 18/2024 da ANPD, deve obrigatoriamente consultá-lo para fins de assistência e orientação quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

Sendo assim, além do cuidado do agente de tratamento para evitar o conflito de interesse é também dever do Encarregado, e igualmente do substituto, declarar ao agente de tratamento qualquer situação que possa configurá-lo, responsabilizando-se pela veracidade das informações prestadas.

3.3 É possível haver a indicação de um DPO Global ou DPO LATAM que funcione como Encarregado no Brasil?

Alguns países latino-americanos também exigem a indicação do Encarregado, como a Colômbia e o México; outros o exigem apenas para alguns setores específicos e

se o tratamento de dados predominante do controlador tiver determinadas características, como o tratamento em larga escala e de dados pessoais sensíveis, como o Equador e o Uruguai.

Nesse contexto, não há vedação na legislação brasileira sobre a indicação de DPO Global ou DPO LATAM para também atuar como Encarregado e agente de tratamento situado no Brasil. Contudo, a Resolução nº18/2024, em seu artigo 13, exige expressamente que o Encarregado saiba se comunicar de forma clara e precisa em língua portuguesa. Logo, o DPO Global ou o DPO LATAM pode desempenhar tal papel no Brasil desde que se comunique em português.

Em não sendo possível a comunicação na língua portuguesa será necessária a indicação de representante aqui no Brasil para ser o Encarregado.

Importante ressaltar que o exercício da atividade de Encarregado não pressupõe a inscrição em entidade nem qualquer certificação ou formação profissional específica, porém é importante seu conhecimento especializado em proteção de dados, considerando as atividades do seu controlador.

3.4 Quais as principais medidas a serem adotadas pelo controlador com relação ao Encarregado?

Além da atenção com a análise do conflito de interesse, vale resumir os principais deveres dos controladores com relação à atuação do Encarregado:

i) prover-lhe os recursos humanos, técnicos e administrativos suficientes para o desempenho adequado de seu papel;

ii) envolvê-lo para assistência e orientação em decisões estratégicas sobre proteção de dados. Não cabe ao Encarregado a tomada de decisão;

iii) garantir sua autonomia técnica assegurando que não sofra interferências indevidas;

iv) assegurar meios para a boa comunicação; e

v) garantir acessos às pessoas de maior nível hierárquico, bem como às demais áreas da organização.

3.5 É possível a responsabilização do Encarregado?

A responsabilização civil pela conformidade dos agentes de tratamento com a LGPD recai sobre eles (controladores e operadores), e não sobre o Encarregado, de acordo com o expressamente previsto na LGPD, nos artigos 42 a 45. O Encarregado, por desempenhar funções estratégicas e técnicas, sem poder decisório sobre as operações de tratamento de dados, não pode ser punido pela atuação ilícita do controlador ou do operador. Por isso, eventuais sanções administrativas ou judiciais relacionadas a violações da LGPD são direcionadas aos agentes de tratamento.

No entanto, o Encarregado (prestador de serviços ou empregado celetista) assume obrigações legais e contratuais, cujo descumprimento doloso ou culposo, poderá vir a ensejar algum tipo de responsabilização indireta, de acordo com as regras do Direito Civil e da Consolidação das Leis do Trabalho (CLT). Essa situação é remota e poderá se materializar nas situações nas quais se comprove que o Encarregado agiu com má-fé (dolo) ou de forma negligente, imprudente ou com imperícia (culpa) no exercício de suas funções, nos termos do dos artigos 186, 187, 927 e 934, do Código Civil e 462, §1º da CLT. [6]

Para mais informações sobre o tema, acesse aqui a 2ª Edição do Guia do Encarrefado, elaborado plelo VLK.

4. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS (TID)

4.1 O que é transferência internacional e quais os Mecanismos de TID?

A transferência internacional de dados deve **necessariamente** envolver, no mínimo, **dois agentes de tratamento**: o exportador e o importador, localizados em países diversos do Brasil ou em organismos internacionais dos quais o Brasil seja membro.

Para viabilizar a transferência internacional de dados, a LGPD exige que agentes de tratamento adotem mecanismos específicos (artigo 33 da LGPD), sendo alguns regulamentados pela ANPD e outros autoaplicáveis. A Resolução CD/ANPD nº 19/2024 regulamentou instrumentos como decisões de adequação:

(i) cláusulas-padrão contratuais (detalhadas no Anexo II);

(ii) cláusulas-padrão contratuais equivalentes;

(iii) cláusulas contratuais específicas para determinada transferência; e

(iv) normas corporativas globais. Continuam pendentes de regulamentação específicas: selos, certificados e códigos de conduta.

Decisões de adequação

Apesar de as Cláusulas-Padrão Contratuais serem o mecanismo mais utilizado mundialmente, as decisões de adequação se destacam por promover a integração econômica com parceiros estratégicos, como a União Europeia (UE), e alinhar o Brasil aos padrões globais de proteção de dados. Essa harmonização regulatória fortalece a segurança jurídica, atrai investimentos estrangeiros e impulsiona o comércio internacional, elementos essenciais para o crescimento sustentável do país. A ANPD está negociando com a UE para viabilizar decisões mútuas de adequação e é provável que em meados de 2025 o Brasil e a União Europeia reconheçam mutuamente adequados ao grau de proteção de dados pessoais exigido pelas legislações respectivas.

4.2 Há prazo para aplicação da Resolução nº 19/2024?

A Resolução nº 19/2024 entrou em vigor na data de sua publicação, ou seja, em 23.08.24, estabelecendo o prazo de **12 meses** para os agentes de tratamento que decidirem adotar as **Cláusulas-Padrão Contratuais** (Anexo II, da Resolução nº 19/2024) para, nesse prazo, incorporá-las aos seus respectivos instrumentos contratuais.

Os demais mecanismos sobre transferência internacional, portanto, já são aplicáveis desde **agosto de 2020**, com a vigência da LGPD, ou passaram a ser em **23.08.2024**, com a Resolução nº 19/2024, ressalvadas :**(i)** as Cláusulas-Padrão Contratuais cujo prazo para completa adoção se finda no dia **23.08.25**; e

(ii) os selos, certificados e códigos de conduta que ainda não foram regulamentados.

Assim, é possível resumir esses prazos da seguinte forma:

Mecanismos previstos no artigo 33, III a IX da LGPD

Aplicável e exigível desde **agosto de 2020**

Decisão de adequação (art. 33, I)

Aplicável desde **23.08.2024** com procedimento para adoção previsto na Resolução nº19/2024

Cláusulas-Padrão Contratuais (Anexo II da Resolução nº 19/2024)

Aplicável desde 23.08.2024 e exigível a partir

de **23.08.25**

Cláusulas-padrão contratuais equivalentes

Aplicável desde **23.08.2024** com procedimento para adoção previsto na Resolução nº19/2024

Cláusulas contratuais específicas para determinada transferência

Aplicável desde **23.08.2024** com procedimento para adoção previsto na Resolução nº19/2024

Normas Coorporativas Globais

Aplicável desde **23.08.2024** com procedimento para adoção previsto na Resolução nº19/2024

Selos, certificados e códigos de conduta

Inaplicável (pendente de regulamentação pela ANPD)

4.3. Quais os mecanismos de transferência mais adequados? Qual a sua diferença para a base legal?

Os mecanismos de transferência internacional de dados pessoais são uma previsão legal (artigo 33 da LGPD) cuja adoção adequada torna lícita a TID. Já as bases legais são hipóteses legais que a LGPD exige seja adotada para tornar lícita a própria operação de tratamento de dados pessoais e estão elencadas nos artigos 7º, 11 e 14 da LGPD.

No entanto, a LGPD elegeu algumas bases legais como mecanismos de transferência internacional, o que gera certa confusão. Isso ocorre no artigo 33, incisos:

IV (proteção da vida ou da incolumidade física do titular ou de terceiro);

VII (execução de política pública ou atribuição legal de serviço público);

VIII (consentimento específico e em destaque);

IX apenas para dados pessoais não sensíveis **(cumprimento de obrigação legal ou regulatória; execução de contrato e procedimentos preliminares da qual o titular seja parte; exercício regular de direitos em processo judicial, administrativo ou arbitral).**

Assim, o controlador poderá adotar qualquer um dos mecanismos de TID previstos no artigo 33 da LGPD. A decisão sobre a adoção do mecanismo de transferência mais adequado cabe ao agente e tratamento, mais precisamente ao controlador-exportador e conforme suas atividades de tratamento. Logo, cabe a ele definir qual melhor mecanismo adotar para atender a legislação brasileira de proteção de dados.

Execução de Contrato e Procedimentos Preliminares (artigo 33, V c/c artigo 7º inciso V da LGPD)

O mecanismo de TID fundado na base legal de execução de contrato e procedimentos preliminares relacionados a contrato possui alguns condicionantes para ser aceita, como

(i) o titular tem que ser parte do contrato;

(ii) o tratamento de dados deve ocorrer a pedido do titular dos dados;

(iii) só pode ser usada se o tratamento em questão for imprescindível para a execução do contrato firmado entre o agente de tratamento e o titular de dados, segundo precedentes europeus.

Logo, não é aceitável a escolha do controlador (ex. optou por usar um serviço de armazenamento em nuvem no exterior), mas deve ser necessária para a execução do contrato do qual faça parte o titular (ex. contrato realizado no Brasil de aluguel de carro em viagem ao exterior: os dados pessoais do titular precisam ser transferidos para o país onde o carro será retirado, caso contrário a execução do contrato fica impossibilitada).

Consentimento

O mecanismo de TID que trata do consentimento, conforme previsto no artigo 33 inciso VIII, deve atender suas condições legais logo, deve ser:

(i) específico;

(ii) em destaque para a transferência e só pode ser utilizado desde que;

(iii) tenha havido informação prévia sobre o caráter internacional da operação; e

(iv) as finalidades tenham sido claramente diferenciadas de outras finalidades para as quais consentimento foi coletado.

4.4. Além do mecanismo de transferência internacional de dados, é preciso indicar uma base legal autônoma para a transferência internacional?

Embora a LGPD não exija expressamente essa indicação, a ANPD em sua Resolução nº19/2024 assim determinou em seu artigo

4º III c/c artigo 9º I e II. Logo, o agente de tratamento deve respaldar sua transferência internacional de dados em um dos mecanismos de transferência internacional de dados e indicar a base legal independente para a transferência de dados pessoais.

Isso burocratizará a transferência internacional e tem como efeito praticamente impossibilitar a transferência de dados pessoais sensíveis já que a base legal do legítimo interesse, que respalda a maioria das decisões estratégicas das organizações em termos de transferência internacional de dados, não poderá ser usada para essa categoria de dados pessoais.

De toda forma, nos casos em que o mecanismo de TID reproduzir base legal, tanto o mecanismo como a base legal para aquela TID específica serão iguais. (Ex. Contrato de locação de veículo firmado no Brasil para retirada do carro em Paris, França). Haverá necessidade de transferência dos dados pessoais coletados do titular para execução deste contrato., do qual o titular é parte. Logo, o mecanismo de TID será **execução de contrato (artigo 33 IX da LGPD),** assim como a base legal para a transferência internacional de dados será **execução de contrato (artigo 7º V).**

4.5 O que fazer se eu já adoto Clausulas-Padrão Contratuais de outro país ou de organismo internacional?

É possível formular perante a ANPD pedido de reconhecimento de equivalência (artigos 18 a 20 da Resolução nº 19/2024), pelo qual a ANPD vai analisar as Cláusulas-Padrão Contratuais e verificar:

(i) são compatíveis com as disposições da LGPD e da Resolução nº 19/2024;

(ii) se asseguram nível de proteção de dados equivalente ao garantido pelas cláusulas-padrão contratuais nacionais;

(iii) os riscos e os benefícios proporcionados pela aprovação, considerando, entre outros aspectos, a garantia dos princípios, dos direitos do titular e do regime de proteção de dados da legislação nacional; além dos

(iv) impactos sobre o fluxo internacional de dados, relações diplomáticas, comércio internacional e cooperação internacional do Brasil com outros países e organismos internacionais.

4.6 Qual o melhor mecanismo de transferência internacional de dados para os EUA e para a União Europeia?

União Europeia (UE)

Para a transferência internacional de dados entre agentes de tratamento situados no Brasil (exportador) e na União Europeia (importador) as Cláusulas-Padrão Contratuais da ANPD também podem ser imediatamente adotadas, contudo, se os agentes de tratamento já regularizaram essa transferência via Cláusulas-Padrão Contratuais europeias (EU´s Standard Contractual Clauses - EU´s SCCs), a Resolução nº 19/2024 permite que sejam submetidas a um procedimento de reconhecimento de equivalência perante a ANPD. Há notícias de que já existe um pedido nesse sentido em curso na ANPD, portanto, uma vez reconhecida a equivalência das EU´s SCCs, os agentes de tratamento brasileiros poderão aproveitá-las validamente também para fins de transferência internacionais de dados que partem do Brasi para a UE.

De toda forma, uma vez sendo proferida a decisão de adequação da União Europeia pelo Brasil (ANPD), essa decisão será suficiente para respaldar as transferências internacionais de dados.

Estados Unidos da América (EUA)

Para a transferência internacional de dados entre agentes de tratamento situados no Brasil (exportador) e nos EUA (importador), a princípio, o melhor mecanismo a ser adotado são as Cláusulas-Padrão Contratuais da ANPD. Isso porque o Brasil não possui decisão de adequação com os EUA semelhante à decisão da União Europeia com os EUA, o "USA-EU Data Privacy Framework", adotado em 10 de julho de 2023[1], nem existem Cláusulas-Padrão Contratuais norte-americanas.

4.7. Qual o meio disponibilizado pela ANPD para realizar os requerimentos previstos na Resolução nº 19/2024?

A ANPD lançou em setembro de 2024 em seu site, página específica para transferência internacional de dados pessoais. Os pedidos relacionados à aprovação ou revisão de mecanismos de transferência internacional de dados devem ser submetidos à ANPD por meio do Sistema Eletrônico de Informações (SEI), que busca garantir a eficiência e a segurança na instrução e tramitação dos processos, permitindo que as empresas acompanhem o andamento de suas solicitações. [2]

Para mais informações visite nosso Q&A no tema em nosso site aqui.

5. CIBERSEGURANÇA E RESPOSTA A INCIDENTES

Cibersegurança e Resposta a Incidentes figuram entre os temas de maior prioridade para a ANPD. Dos 10 processos sancionadores instaurados pela Autoridade até o momento, oito estão diretamente relacionados a essa temática [1].

Diante desse cenário, apresentamos os principais aspectos que merecem atenção ao tratar de cibersegurança no contexto da proteção de dados pessoais.

5.1 Quais medidas de segurança adotar?

Não existe "solução única" para responder a essa questão. As medidas de segurança devem sempre ser proporcionais ao risco e ajustadas ao caso concreto, conforme o art. 44 da LGPD, o qual exige que o tratamento atenda ao que é “razoavelmente esperado” pelo titular.

Mas o que significa "razoavelmente esperado"?

Apesar de essa análise depender dos riscos de cada atividade específica, as medidas indicadas pela ANPD no Checklist para Agentes de Tratamento de Pequeno Porte representam o mínimo esperado de qualquer agente de tratamento, incluindo[1]:

- **Política de Segurança da Informação:** estabelecer e revisar periodicamente;
- **Contratos:** incluir cláusulas específicas de proteção de dados e segurança;
- **Treinamento e conscientização:** promover capacitação sobre privacidade e segurança, incluindo prevenção a ameaças comuns, como vírus e engenharia social;
- **Controles de acesso:** limitar permissões de acesso ao mínimo necessário, implementar troca periódica de senhas e autenticação multifator (MFA);
-
- **Minimização de dados:** reduzir o tratamento de dados pessoais ao necessário e remover dados expostos desnecessariamente em ambientes públicos;
- **Criptografia:** proteger dados armazenados, incluindo dispositivos externos, e em trânsito;
- **Segurança de Dispositivos externos:** controlar, inventariar e minimizar seu uso;
- **Backups:** realizar cópias offline periódicas e armazená-las de forma segura;
- **Descarte de mídias físicas:** formatar, sobrescrever ou destruir mídias antes do descarte. Garantir registro de descarte/ destruição ao contratar terceiros, por meio de contrato.
- **Firewall ou WAF:** instalar e manter Firewall ou Web Application Firewall;
- **Proteção de E-mails:** implementar

filtros antispam e integração com software antivírus;

- **Atualizações de segurança:** manter sistemas atualizados para corrigir falhas de segurança;

- **Softwares de proteção:** instalar, atualizar e realizar varreduras periódicas com antivírus e antimalware;

- **Segurança de dispositivos móveis:** segregar dispositivos institucionais de particulares, proteger com MFA e possibilitar deleção remota;

- **Segurança de Serviços em nuvem:** garantir conformidade com requisitos de segurança, controles de acesso robustos e acordos adequados de nível de serviço.

Ainda é importante destacar que, a LGPD faculta à ANPD a possibilidade de determinar padrões-técnicos mínimos de segurança da informação – os quais tendem a ser mais robustos que aqueles voltados aos agentes de pequeno porte. Há expectativa de que esses padrões serão expedidos pela ANPD ainda em 2025, já que é uma das atividades previstas na fase 1 da Agenda Regulatória da autoridade para o biênio 2025-2026[2].

Por fim, muitos setores regulados possuem normas específicas de segurança cibernética ou requisitos relacionados, que também devem ser considerados como parte do "mínimo razoavelmente esperado" pelos titulares de agentes de tratamento integrantes desses setores. Logo, é fundamental observar as regulamentações setoriais porque seu descumprimento tende a configurar irregularidade no tratamento. Exemplos de normas setoriais incluem:

Setor Financeiro

Normativo: Resolução CMN n° 4.893/2021 (atualizada em janeiro de 2024) – Dispõe sobre a política de segurança cibernética, inclusive controles mínimos a serem adotados, e serviços em nuvem [3].

Setor Telecomunicações.

Normativo: Resolução ANATEL n° 740/2020 (atualizada em agosto de 2024) – Regulamenta as condutas e procedimentos para a promoção da segurança nas redes e serviços de telecomunicações, incluindo a Segurança Cibernética [4].

Setor Saúde:

Normativo Resolução CFM n° 1.821/2007 e Resolução COFEN n° 754/2024 – Preveem regras para o prontuário eletrônico, estabelecendo a necessidade de conformidade com os requisitos de segurança aplicáveis ao NGS2, do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde [5][6].

Também é importante considerar a aplicação de normas de outras jurisdições. Por exemplo, o Digital Operational Resilience Act (DORA)[7], da União Europeia, estabelece diversas obrigações para instituições financeiras europeias, incluindo a gestão de riscos relacionados a fornecedores de TIC. Assim, fornecedores que prestam serviços, especialmente os considerados críticos, a essas instituições devem se adequar para atender ao nível de segurança exigido por essa regulamentação.

5.2 O que devo ajustar em meu Plano de Resposta à Incidentes?

Parte significativa dos processos sancionadores na ANPD decorre da ausência de comunicação de incidentes aos titulares e à própria Autoridade. Por isso, é essencial que as organizações ajustem seus **Planos de Resposta a Incidentes** aos requisitos previstos no **Regulamento de Comunicação de Incidentes à Segurança** [1].

Sobre o tema, leia o E-Book de Comunicação de Incidentes de Segurança (clique aqui). O qual inclui as seguintes ações simultâneas, no caso de resposta a incidentes de segurança envolvendo dados pessoais/sensíveis:

5.3 É necessário pagar ao titular indenização?

A responsabilidade civil tipicamente requer a presença de três elementos básicos: ato ou omissão ilícita do agente de tratamento, dano ao titular e nexo de causalidade entre o ato e o dano.

Em acórdão recente proferido no Recurso Especial n° 2147374 – SP, a **Terceira Turma do Superior Tribunal de Justiça (STJ)** chegou a entendimento que o regime de responsabilidade não se enquadra nos regimes tradicionais de responsabilidade subjetiva e objetiva, mas em um novo regime de “responsabilidade proativa” [1].

Nesse regime, não basta cumprir a lei para afastar a responsabilização. É também

necessário demonstrar a eficácia das medidas adotadas quanto à prevenção dos danos potenciais decorrentes de suas atividades. [2].

Assim, o agente de tratamento que sofreu incidente e não adotou e/ou não demonstrou medidas de segurança suficientes que o titular poderia razoavelmente esperar, ele poderá ser responsabilizado pelos danos decorrentes do incidente.

Em relação aos danos, eles podem ser classificados como materiais (relacionados a perdas patrimoniais) ou morais (ligados a aspectos não patrimoniais, como honra, imagem e dignidade). No caso dos danos morais, eles podem ser presumidos *(in re ipsa)* ou depender de comprovação da violação de direitos da personalidade.

Com relação aos danos morais, no Agravo em Recurso Especial n° 2130619/22 – SP[3], que tratou do vazamento de dados cadastrais, a **Segunda Turma do STJ** distinguiu entre dados pessoais sensíveis [4] e outros dados pessoais. Para **dados sensíveis**, entendeu-se haver **presunção de danos morais** devido à forte ligação desses dados com a intimidade da pessoa afetada. No caso dos demais dados pessoais, a comprovação do dano é necessária.

Já quanto aos danos materiais, com base em precedentes sobre vazamento de dados bancários, como o Recurso Especial 2077278/23 – SP[5], **a Terceira Turma do STJ** entendeu que o agente de tratamento pode ser responsabilizado não apenas pelos **danos materiais diretos** decorrentes do vazamento, mas também pelos prejuízos causados por práticas facilitadas por ele, como fraudes financeiras decorrentes de engenharia social, ou seja, responsabilizou o agente de tratamento por **danos indiretos.**

[4] “Dados pessoais sensíveis são dados sobre a 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” (V. artigo 5º II da LGPD).

AUTORES

RONY VAINZOF
rony@vlklaw.com.br

CAIO LIMA
caio@vlklaw.com.br

VERÔNICA BARROS
veronica.barros@vlklaw.com.br

JEAN SANTANA
jean.santana@vlklaw.com.br

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

Direito,
Inovação
& Tecnologia

E-book "O Futuro da privacidade: como se preparar para 2025", de 28 de janeiro de 2025.