Diretrizes metodológicas para a elaboração do relatório de impacto a proteção de dados pessoais: uma proposta de atualização do modelo do governo federal.

Fernanda Carvalho

Em cumprimento à Agenda Regulatória para o biênio 2023/2024, a Autoridade Nacional de Proteção de Dados - ANPD elaborou, em abril de 2023, algumas diretrizes para a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), através de 15 (quinze) perguntas e respostas sobre o tema.[1]

Apesar das valiosas diretrizes existentes, na realidade, muitos controladores encontram dificuldades na elaboração do documento, tão relevante para a consolidação de boas práticas e mitigação de riscos.

A louvável flexibilidade metodológica estabelecida pela ANPD[2], pode, por vezes, fazer com que as instituições enfrentem dificuldades, num momento em que ainda é necessária a formação de uma cultura institucional de proteção de dados.

O Governo Federal, por meio do Programa de Privacidade e Segurança da Informação, disponibilizado pelo Ministério da Gestão e da Inovação em Serviços Públicos, propôs um Guia e *Template* para elaboração de RIPD[3]. Todavia a metodologia empregada pode ser aprimorada, evitando a descrição de informações repetidas em vários tópicos e melhor parametrizando todos os elementos de *compliance* à Lei. Sugerimos, portanto, a reformulação do *Template*, com o objetivo de orientar o controlador à análise crítica dos tratamentos de dados propostos e de seus riscos associados, à medida que se preenche o RIPD. Desta forma, por um lado reiteramos partes do *framework* e, por outro,

---

[1] ANPD. Relatório de Impacto à Proteção de Dados Pessoais. Perguntas e Respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais. Pulicado em: 6/4/2023 16h49. Atualizado em: 6/4/2023 17h14. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais

[2] Conforme se depreende no trecho de resposta da pergunta "Quais critérios e metodologias devem ser utilizados para a gestão de riscos?": "As diretrizes gerais do processo de gestão de risco de privacidade, além de estarem alinhadas à política de segurança do responsável, poderão considerar, entre outros aspectos, objetivos estratégicos, processos, estrutura organizacional, requisitos da LGPD e demais normativos aplicáveis." (ANPD, 2023). No mesmo sentido: "Enquanto a matéria não estiver regulamentada, controladores de dados têm flexibilidade para determinar as melhores estruturas e formatos de seu RIPD, da forma que mais se ajuste às práticas de trabalho existentes na organização, observadas as disposições pertinentes da LGPD." (ANPD, 2023).

[3] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-e-modelos. O guia/*template* pode ser especificamente acessado em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_template_ripd.docx

sugerimos modificações metodológicas ou classificatórias para direcionar o gestor na análise reflexiva sobre os riscos no tratamento de dados.

Nesse sentido, sugerimos a estruturação do RIPD a partir de 12 tópicos principais, quais sejam:

1- Definição dos agentes de Tratamento e do Encarregado
2- Partes Interessadas Consultadas
3- Justificativa da Necessidade de Elaborar o Relatório
4- Escopo do Relatório de Impacto
5- Finalidades: Delimitação e Justificativa dos propósitos com o tratamento de dados pessoais
6- Natureza dos Dados Tratados
7- Descrição do Tratamento
8- Base Legal do Tratamento
9- Avaliação Principiológica e Demais Requisitos Legais
10- Inventário e Análise de Riscos
11- Medidas, Salvaguardas e Mecanismos de Mitigação de Riscos
12- Aprovação

Abordaremos sucintamente cada um deles a seguir.

1- Definição dos agentes de Tratamento e Encarregado

Entendemos como acertada a iniciativa do Governo Federal, no *template* de referência, em estabelecer por ponto de partida para a confecção do RIPD, a identificação clara sobre os agentes de tratamento. A LGPD define como agentes de tratamento, o controlador e o operador, além de instituir a figura do encarregado como canal de comunicação entre os titulares, o controlador e a ANPD. Cabe destacar que a confecção do RIPD é atribuição do controlador, que é quem delimita de forma inequívoca, os propósitos os quais se almeja atingir com o tratamento. O controlador é o agente a quem competem as decisões referentes ao tratamento, cujos interesses estão sendo atendidos com a manipulação dos dados pessoais.

De fato, a identificação clara dos interesses atendidos com o tratamento deve ser vetor de orientação, auxiliando na identificação do controlador mesmo nos casos mais complexos. Por exemplo, em determinadas situações, os Entes Públicos poderão atuar exclusivamente como operadores de dados pessoais. É o caso do tratamento de dados de

funcionários terceirizados, quando o tratamento, embora realizado em alguma medida pelo ente público, se dá no interesse da empresa contratada, em questões trabalhistas, folha de ponto, atestados médicos etc.

Portanto, a definição do controlador está intimamente ligada à identificação dos interesses anelados com o tratamento de dados, separando assim o agente controlador daqueles que atuarão como operadores técnicos para a obtenção dos resultados pretendidos.

Com o objetivo de dirimir as dúvidas na classificação de cada agente, a ANPD elaborou recentemente um guia acerca dos agentes de tratamento[4]. A autoridade apontou a possibilidade de existir mais de um controlador no mesmo tratamento, desde que ambos os agentes de tratamento determinem conjuntamente as finalidades/propósitos e os meios a serem utilizados (em semelhança ao que prevê o art. 26 do Regulamento Europeu - RGPD, e o art. 42, § 1º, II da LGPD) (ANPD, 2022). Também apontou a possibilidade de existir subcontratação de operadores, resultando em sub-operadores, e apontou o caso atípico em que o órgão público responde como controlador, ainda que não exista personalidade jurídica propriamente dita.

Vale a observação de que, para a Autoridade, quando há uma relação de subordinação institucional entre o controlador e o empregado/funcionário que lida com os dados, então esses agentes não podem ser caracterizados como operadores. Nesses casos, o tratamento de dados seria realizado exclusivamente pelo controlador, inexistindo operadores de dados para um tratamento exclusivamente realizado pelo Ente, internamente.

2- Partes Interessadas Consultadas

A ANPD sugere que sejam indicadas também as partes interessadas/envolvidas na elaboração do RIPD, orientando o controlador a informar eventuais consultas na elaboração do RIPD e pareceres emitidos. O *template* proposto pelo Governo Federal contempla esse quesito, que deve ser preservado também nesta proposta.

3- Justificativa da Necessidade de Elaborar o Relatório

[4] ANPD, Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. VERSÃO 2.0 ABR. 2022.

É importante que conste do relatório o motivo que justificou a elaboração do RIPD. Este aspecto também é contemplado pelo *template* do Governo Federal. A LGPD aborda casos em que a ANPD pode solicitar a elaboração do Relatório, mas existem outras situações que podem justificar a escolha pela elaboração do RIPD. A própria ANPD apontou como recomendável a elaboração do Relatório nos casos que envolvam tratamento de alto risco, nos termos do art. 4º da Resolução nº 2/2022 da ANPD. O controlador também pode estipular diretrizes ou estabelecer casos em que o RIPD seja obrigatório ou recomendável. Sugerimos como especialmente recomendável a elaboração do RIPD em tratamentos de dados pessoais que envolvam a anonimização de dados em grande escala ou destinados a disponibilização pública de dados, como forma de desdobramento do princípio da responsabilização e prestação de contas.[5] Por fim, destacamos que esse tópico se encontra em conformidade com o item 6.2 da ABNT NBR ISO/IEC 29134:2020, acerca da análise de pertinência, ou determinação da necessidade da realização da PIA (Privacy Impact Analysis).[6]

4- Escopo do Relatório de Impacto

Entendemos por Escopo o conjunto de atividades que serão abrangidas pelo RIPD em elaboração. Este aspecto não é diretamente tratado no *template* de referência que menciona apenas o escopo do tratamento (e não do relatório), dentro da descrição do tratamento.

É muito comum que, para se atingir um único propósito, o controlador precise de diversos tratamentos distintos, dentre aqueles determinados pela LGPD (como coleta, classificação, utilização, reprodução etc.). Também é possível, como vimos, que exista mais de um controlador, tratando os dados de formas diversas para o alcance de um mesmo interesse. Nesse sentido, o RIPD deve conter as informações claras sobre o seu escopo, ou seja, deve explicitar a abrangência do alcance do relatório, apontando se ele abarca todos os tratamentos relacionados ao propósito, se ele abarca apenas os processos de trabalho internos; se ele envolve apenas um determinado tratamento de dados ou um conjunto de tratamentos diversos etc.

---

[5] Nos termos sugeridos na obra: Carvalho, Fernanda Potiguara. Desafios da Anonimização: Um framework dos requisitos e boas práticas para compliance à LGPD. 1. ed. São Paulo: Thomson Reuters Brasil, 2022.
[6] ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg. 4/5.

Portanto, este tópico esclarece de forma clara o objeto do RIPD, e sobre qual processo será realizada a análise de riscos. Destacamos que essa descrição se encontra em conformidade com o item 7.3.1.1 da ABNT NBR ISO/IEC 29134:2020, o qual orienta que sejam especificados os limites da avaliação, com declaração sobre o que é considerado dentro ou fora do escopo da PIA.[7]

5- Finalidades: Delimitação e Justificativa dos propósitos com o tratamento

Os propósitos do tratamento de dados pessoais compõem elemento central na elaboração do RIPD, pois são vetores de diversas variáveis de *compliance*. O princípio da Finalidade (art. 6º, I, LGPD) determina que os propósitos do tratamento devem ser legítimos, específicos, explícitos e informados ao titular. Também o princípio da adequação correlaciona as finalidades ou os propósitos informados e o tratamento em si para averiguar se o tratamento é considerado adequado com as expectativas geradas no titular. Desta forma a delimitação dos propósitos é importante para análise da legitimidade do tratamento, para fiel notificação do titular e para identificação de riscos excessivos e de medidas alternativas.

No *template* proposto pelo Governo Federal, a finalidade do tratamento é compreendida como sinônimo da base legal para o tratamento. Não recomendamos essa equiparação pois ela pode gerar equívocos. Basta a análise, por exemplo, da base legal do consentimento, que representa apenas a hipótese legal autorizativa do tratamento, mas não compreende os propósitos, ou seja, as finalidades que levaram à decisão pelo tratamento de dados pessoais.

Ademais, mesmo as hipóteses legais que contenham alguma diretriz quanto à finalidade do tratamento devem esclarecer a chamada "finalidade específica", apontando qual obrigação legal se propõe a cumprir, qual política pública será realizada, qual estudo, etc. A mesma questão se observa no tratamento de dados de crianças e adolescentes, que contém a diretriz finalística de que o mesmo deve ser feito no interesse da criança/adolescente (art. 20) e no tratamento de dados pelo poder público, que deve visar o interesse público (art. 23, caput). Também nesses casos, o propósito que garante o interesse do menor e o interesse público deve ser devidamente especificado.

[7] ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg. 33.

Nesse contexto, propomos a alteração do *template*, de forma que os dois aspectos (base legal e finalidade institucional) estejam claramente identificados. É necessário que os propósitos sejam pontuados expressamente para que, na análise principiológica e de riscos existam subsídios para avaliação do tratamento proposto na descrição do tratamento. É com base nos propósitos elencados neste tópico que será possível a análise do tratamento de dados pessoais esquematizado, respondendo a perguntas como: se o tratamento é necessário, se é suficiente ou se extrapola os propósitos institucionais pretendidos e justificando-os.

Portanto, é necessário que o controlador descreva os benefícios esperados com os tratamentos de dados pessoais, seja para a instituição, para os titulares, para a sociedade como um todo etc., e como o propósito específico atingirá a diretriz finalística descrita na lei. Por fim, destacamos que esse tópico se encontra em conformidade com o item 6.1 da ISO/IEC 29134:2020, o qual orienta que sejam especificados os objetivos gerais previstos no escopo da PIA[8]

6- Natureza dos Dados Tratados

A especificação da natureza dos dados que serão tratados também recebe destaque na identificação dos riscos do tratamento. Isso porque o art. 4º da Resolução nº 2/2022 da ANPD estabelece por parâmetro para definição do tratamento de alto risco elementos como a categoria dos titulares (se envolve dados de crianças, adolescentes ou idosos), a natureza sensível dos dados ou o volume de dados tratados.

Portanto, sugerimos a criação de um tópico específico no RIPD para descrição detalhada dos dados, com informações sobre a categoria dos titulares; o tipo de dado tratado (exemplo: nome, telefone, matrícula etc.), especificando se envolve dados sensíveis ou dados pessoais com potencial de revelar dados pessoais sensíveis, nos termos do art. 11, § 1º; o volume dos dados pessoais a serem coletados e tratados; o número de titulares de dados afetados pelo tratamento; a fonte de dados (dados pré-existentes? Dados coletados no decorrer do tratamento?); o formato dos dados (planilha eletrônica, arquivo xml, formulário em papel etc.).

Deve ser mencionado se o tratamento envolve dados pseudonimizados, dados de perfil comportamental de pessoa identificada (art. 12, § 2º) ou se envolve dados

[8] ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg. 4/5.

anonimizados. Cabe mencionar ainda o nível de relacionamento dos titulares com o controlador, por exemplo, se são clientes, funcionários do controlador, terceiros prestadores de serviços etc.

No *template* do Governo Federal, há um subtópico acerca da natureza do tratamento, dentro do tópico de descrição do tratamento. Muitas das informações acerca da natureza dos dados estão espalhadas por diversos subtópicos (como o volume dos dados, categoria dos titulares, se os dados são sensíveis ou não etc.). Desta forma, sugerimos que estas informações sejam descritas em tópico específico, que permita a análise de forma minuciosa sobre os dados que serão objeto de tratamento. Esse agrupamento de informações é intencional, objetivando viabilizar, posteriormente, a correlação entre todos os dados descritos com o propósito institucional, de forma a justificar a necessidade do tratamento de cada dado.

7- Descrição do Tratamento

A descrição dos tratamento compõe o modelo operacional do projeto, que especificará o passo a passo pretendido, dentro do escopo definido para o RIPD no tópico 4.

Nesse sentido, a disponibilização para os titulares do RIPD, como sugerido pela ANPD[9], pode se dar de forma mitigada quanto à descrição do tratamento, como forma de proteção dos segredos comercial ou industrial, nos termos do princípio da transparência (art. 6º, VI, da LGPD) e da limitação dos direitos do titular explicitada no art. 9º, II da Lei. Em todo caso, para a elaboração do RIPD, ainda que exista a mitigação na publicidade dada à descrição do tratamento é necessário que todas as etapas estejam explicitadas, sempre que possível por meio de documentação que demonstre os fluxos de dados da instituição. A análise de riscos depende da especificação do passo a passo do tratamento para que possíveis brechas sejam detectadas em cada etapa.

Portanto, nesta seção, o RIPD deve conter informações como: quais as modalidades de tratamento serão realizadas, com base no art. 5º, X, da LGPD; como será realizada cada uma dessas modalidades de tratamento, com quais dados especificados no

[9] Conforme exposto pela ANPD: "Embora a divulgação do RIPD não seja, em regra, obrigatória, permitir o acesso ao público em geral pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas, previstos, respectivamente, pelo art. 6º, incisos IV, VI e X, da LGPD." disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd

tópico anterior e quais agentes de tratamento estarão envolvidos em cada etapa (se houver mais de um controlador ou operador); se as decisões serão tomadas por meio de tratamento automatizado; se haverá compartilhamento de dados, quais os dados compartilhados e com quais agentes; a extensão e frequência em que os dados serão tratados; a duração do tratamento; a política de armazenamento dos dados; a abrangência da área geográfica do tratamento.

No *template* apresentado pelo Governo Federal, a descrição do tratamento se subdivide em tópicos que fragmentam o fluxograma e a compreensão sobre a totalidade do procedimento pretendido para obter o propósito institucional. Por isso, sugerimos que toda a descrição sobre o tratamento de dados seja reunida em um tópico único, que descreva as minúcias do fluxo de dados na instituição, desde a coleta até a exclusão dos dados. Ressaltamos, todavia, a possibilidade de divisão da descrição em subtópicos, à critério do controlador, nos casos em que a segmentação for importante para a melhor compreensão do processo, como por exemplo, no caso em que escopo do RIPD envolva mais de uma frente de tratamentos. Ademais, cada etapa deve ser exposta com descrição minuciosa, conforme prevê a ISO/IEC 29134:2020:

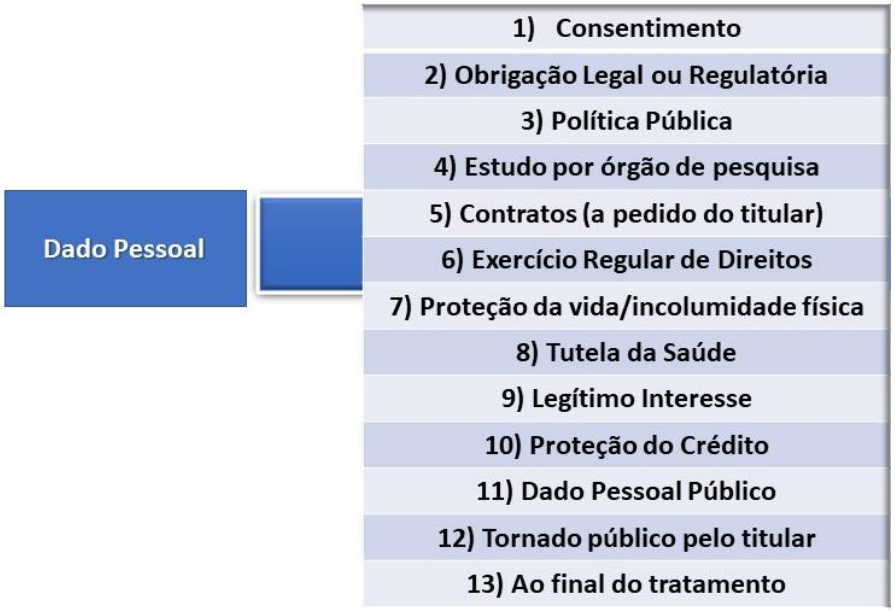
> "Convém que organização, como uma entrada da PIA, descreva o fluxo de informações da maneira mais detalhada possível para ajudar a identificar os possíveis riscos de privacidade. Convém que o avaliador considere os impactos não apenas na privacidade das informações, mas também na conformidade com os regulamentos relacionados à privacidade, por exemplo, atos de telecomunicações. Convém que todo o ciclo de vida dos DP seja considerado."[10]

8- Base Legal do Tratamento

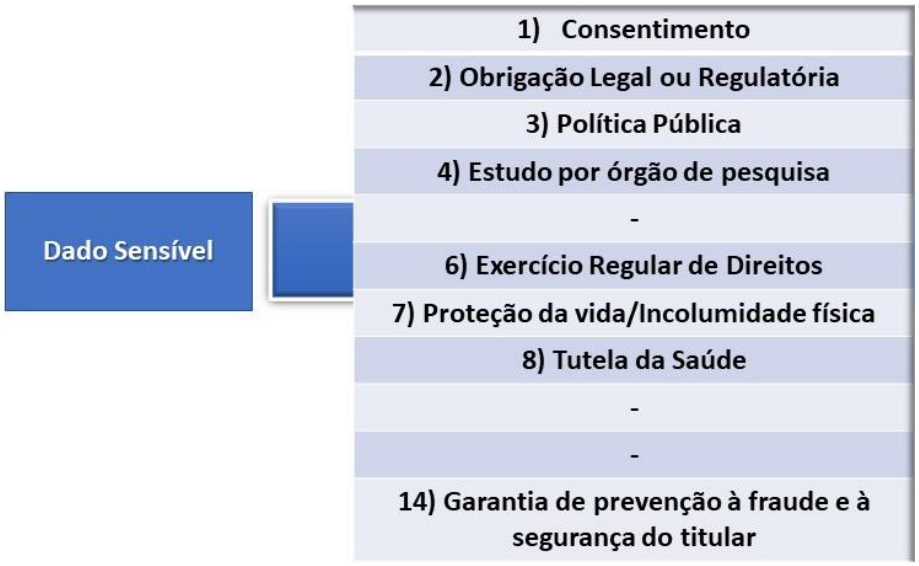
A base legal se refere à hipótese em que a Lei permite o tratamento de dados pessoais. Ela deve ser explicitada no RIPD pois se trata do parâmetro que legitima o tratamento de dados pessoais. É através de sua especificação que o titular pode exercer o controle do tratamento, exercendo a autodeterminação no uso de seus dados. Desta forma, deve ser expresso o inciso, alínea ou parágrafo do art. 7º, do art. 11 ou de outro artigo da LGPD que justifique o tratamento.

[10] ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg. 17.

De fato, cabe destacar que as hipóteses legais não estão subordinadas aos art. 7º e 11, como detalhamos no livro "Desafios da Anonimização: Um *framework* dos requisitos e boas práticas para compliance à LGPD"[11]. Aproveitamos para mencionar suscintamente as principais hipóteses de tratamento estipuladas pela Lei e mencionadas na obra de forma esquematizada:



Fonte: Adaptado de Carvalho, Fernanda Potiguara. Desafios da Anonimização: Um framework dos requisitos e boas práticas para compliance à LGPD. 1. ed. São Paulo: Thomson Reuters Brasil, 2022.



[11] Carvalho, Fernanda Potiguara. Desafios da Anonimização: Um framework dos requisitos e boas práticas para compliance à LGPD. 1. ed. São Paulo: Thomson Reuters Brasil, 2022.

Fonte: Adaptado de Carvalho, Fernanda Potiguara. Desafios da Anonimização: Um framework dos requisitos e boas práticas para compliance à LGPD. 1. ed. São Paulo: Thomson Reuters Brasil, 2022.

Acrescentamos ainda a base legal do art. 14, § 3º, que se refere à hipótese de dispensa de consentimento para o tratamento de dados de crianças.

Cabe pontuar que existem casos em que a LGPD exige que a base legal seja complementada por uma **hipótese autorizativa**. Podemos apontar algumas situações em que isso ocorre:

- ✓ Nos casos de compartilhamento de dados de saúde com o objetivo de obter vantagem econômica, que só poderá ocorrer nas hipóteses do art. 11, § 4º e incisos I, II;
- ✓ Nos casos de compartilhamento de dados pelo Poder Público com entidades públicas, que deve respeitar as hipóteses do art. 26, caput;
- ✓ Nos casos de compartilhamento de dados com entidades privadas, que só poderá se dar nos casos autorizativos dos incisos do art. 26, § 1º da LGPD. Esse é um caso em que as próprias exceções também podem se constituir em base legal propriamente dita, que dispensa o consentimento (e não apenas em hipótese autorizativa), nos termos do art. 27, III da LGPD;
- ✓ Nos casos em que o tratamento envolve a transferência internacional de dados, nos quais a base legal deve ser complementada com uma das hipóteses autorizativas, especificadas no art. 33 da LGPD.

Por vezes, uma mesma finalidade/propósito institucional pode envolver tratamentos com mais de uma base legal. É o caso, por exemplo do tratamento de um conjunto de dados que contenha dados pessoais e dados pessoais sensíveis tratados de forma simultânea. Nesse caso, deve ser especificada a base legal que autoriza o tratamento de cada conjunto de dados.

Pontue-se que, para orientar acerca da base legal aplicável ao setor público, a ANPD elaborou um guia orientativo em que descreve algumas das bases legais mais utilizadas no setor[12]. Segundo o guia, "é recomendável que, em geral, órgãos e entidades públicas evitem recorrer ao legítimo interesse, preferindo outras bases legais, a exemplo de execução de políticas públicas e cumprimento de obrigação legal, para fundamentar os tratamentos de dados pessoais que realizam nessas condições."

9- Avaliação principiológica e Demais Requisitos Legais

[12] O Guia Orientativo para Tratamento de Dados Pessoais pelo Poder Público pode ser consultado pelo site: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf

Esta é uma importante etapa que antecede e viabiliza a especificação dos principais riscos encontrados no tratamento proposto. Neste ponto do RIPD o controlador é convidado à análise e conferência das informações prestadas em comparação com as principais exigências de *compliance* definidas pela Lei. É uma etapa de revisão e identificação de falhas nas etapas anteriormente percorridas, e, portanto, sugerimos que seja realizada em tópico próprio.

Aqui, o controlador deve ser levado a refletir sobre todo o fluxo de tratamento e a compará-lo com os objetivos institucionais, com a base legal elencada, com os princípios legais e outros requisitos trazidos pela LGPD para o tratamento de dados pessoais.

Para isso, sugerimos a análise dos requisitos principiológicos e legais sob 3 perspectivas, de acordo com o ente ou instituto mais diretamente afetado pelo tratamento de dados, quais sejam: o propósito institucional, os direitos dos titulares e as demais obrigações de *compliance*.

A classificação é sugerida para que a análise dos impactos se dê por perspectiva, e oriente a identificação dos riscos como veremos adiante. Por exemplo, podemos identificar que, para cumprimento do princípio da adequação, precisamos analisar:

1) quanto ao titular, se ele foi devidamente informado acerca do propósito institucional do tratamento;
2) quanto ao propósito institucional, se a atividade desenvolvida é compatível com o propósito informado.

Desta forma, para cumprimento de um único princípio, temos que observar a exigência legal sob duas perspectivas diferentes. Nesse sentido, podemos destacar:

a) Análise do propósito institucional: Neste tópico, o controlador deve vistoriar o propósito institucional, verificando, por exemplo:

- ✓ se o propósito é legítimo (princípio da finalidade);
- ✓ se ele é específico o suficiente para parametrizar o tratamento de dados pessoais (princípio da finalidade);
- ✓ se há compatibilidade entre o propósito pretendido e o informado ao titular, (princípio da finalidade)
- ✓ se há possibilidade de alteração fundamental desse propósito durante a operação, ocasionando finalidade divergente da informada (princípio da finalidade);

- ✓ se há compatibilidade entre o tratamento de dados e o propósito institucional informado aos titulares (Princípio da Adequação);
- ✓ se os dados pessoais tratados são suficientes, adequados ou excessivos para atender o objetivo institucional com o tratamento de dados pessoais? (Princípio da Necessidade);
- ✓ se tratamento proposto é o mínimo necessário para o atingimento dos propósitos institucionais? (Princípio da Necessidade);
- ✓ se serão utilizados apenas aqueles dados pertinentes, proporcionais e não excessivos ao atingimento do propósito institucional? (Princípio da Necessidade);
- ✓ se os dados são claros, relevantes e atuais de forma suficiente para o atingimento do propósito institucional (Princípio da qualidade dos dados);
- ✓ se o propósito institucional envolve fins discriminatórios ilícitos ou abusivos (Princípio da Não-Discriminação).

b) Análise dos Direitos dos Titulares: Neste tópico, o controlador deve vistoriar se os Direitos dos Titulares estão sendo atendidos. Nesse sentido, deve existir a reflexão sobre os seguintes aspectos:

- ✓ se as informações prestadas aos titulares são suficientes para gerar a legítima expectativa sobre todas as etapas do(s) tratamento(s) (Princípio da Adequação);
- ✓ se está viabilizada a consulta facilitada e gratuita sobre a forma, a duração do tratamento e os tipos de dados tratados (Princípio do livre acesso);
- ✓ se as informações prestadas ao titular são claras, precisas, facilmente acessíveis (Princípio da transparência), adequadas e ostensivas e contemplam as informações descritas no art. 9º da LGPD;
- ✓ se é prestada garantia aos titulares acerca da exatidão, clareza, relevância e atualização dos dados, de acordo com o propósito institucional do tratamento (princípio da qualidade dos dados)
- ✓ se são utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão? (Princípio da Segurança);[13]
- ✓ se, nos casos em que a base legal é o consentimento, o controlador obteve consentimento específico para a comunicação ou compartilhamento de dados (art. 7º § 5º)
- ✓ se é viabilizada a revogação de consentimento pelo titular por procedimento gratuito e facilitado? (art. 8º, 5º)
- ✓ se nos casos em que a base legal é o consentimento, as alterações quanto a finalidade (propósito), forma, duração, alteração do controlador ou compartilhamento de dados foram informadas ao titular de forma destacada? (art. 8º, § 6º e art. 9º §2º)
- ✓ se os titulares são informados com destaque quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, além de serem

[13] Observe que essas medidas deverão ser descritas no tópico 11, acerca das "Medidas, Salvaguardas e Mecanismos de Mitigação de Riscos".

informados sobre os meios pelos quais poderão exercer os direitos do titular elencados no art. 18? (Art. 9º, § 3º);

- ✓ se há publicidade para a dispensa de consentimento no tratamento de dados sensíveis nas hipóteses de cumprimento de obrigação legal ou regulatória e políticas públicas (art. 11, § 2º);
- ✓ se há demonstração de que o tratamento de dado de criança e adolescente está sendo realizado em seu melhor interesse (art. 14);
- ✓ se as informações sobre tratamento de crianças e adolescentes foram prestadas de maneira simples, clara e acessível, adequado ao entendimento da criança (art. 14, § 6º)
- ✓ se há mecanismo simplificado de obtenção de informações sobre dados, retificação de dados ou solicitação de tratamento pelo titular, mediante requisição (art. 18 e 19);
- ✓ se é viabilizada aos titulares a revisão das decisões tomadas em tratamento automatizado? (art. 20).
- ✓ se são prestadas, mediante requisição, informações claras e adequadas sobre os critérios e os procedimentos utilizados para decisão automatizada, observados os segredos comercial e industrial (art. 20, § 1º)
- ✓ se o tratamento de dados de idosos foi efetuado de maneira simples, clara, acessível e adequada ao seu entendimento (art. 55-J, XIX)

c) Análise das demais obrigações de *Compliance:* neste tópico, o controlador deve vistoriar as demais obrigações de *compliance*, não enquadradas nos tópicos anteriores, verificando, por exemplo:

- ✓ se há a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (Princípio da Prevenção)
- ✓ se existe o risco de que o tratamento de dados gere, de forma colateral, efeitos discriminatórios, ilícitos ou abusivos; (Princípio da Não-Discriminação),
- ✓ se existem medidas técnicas e administrativas contra acessos não autorizados aos dados? (Princípio da Segurança)[14]
- ✓ se são utilizadas medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados (Princípio da Segurança e art. 46) e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (art. 46)[15];
- ✓ se as medidas supramencionadas são adotadas desde a concepção do produto ou serviço até sua execução (art. 46, § 2º)

[14] Observe que essas medidas deverão ser descritas no tópico 11, acerca das "Medidas, Salvaguardas e Mecanismos de Mitigação de Riscos.

[15] Observe que essas medidas deverão ser descritas no tópico 11, acerca das "Medidas, Salvaguardas e Mecanismos de Mitigação de Riscos".

- ✓ se há a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (Princípio da responsabilização e prestação de contas)[16];
- ✓ se há a demonstração, pelo agente, da eficácia das medidas tomadas para observância e cumprimento das normas de proteção de dados pessoais (Princípio da responsabilização e prestação de contas);[17]
- ✓ se foram atendidos os requisitos do consentimento previstos no art. 8º, quando esta for a base legal (art. 8º);
- ✓ se foram tomadas precauções contra vícios de consentimento, quando esta for a base legal? (art. 8º, § 3º);
- ✓ se a participação em jogos e aplicações de internet foi condicionada ao fornecimento de informações pessoais pelo titular além do estritamente necessário à atividade? (art. 14, § 4º)
- ✓ se o controlador empregou esforços razoáveis para verificar se o consentimento foi dado pelo responsável pela criança (art. 14, § 5º),
- ✓ se os dados foram devidamente eliminados ao final do tratamento, ou conservados nos limites do art. 16 da LGPD;
- ✓ se, no caso de compartilhamento de dados, as alterações das bases foram comunicadas aos demais agentes de tratamento (art. 18, § 6º);
- ✓ se controlador mantém o registro das operações de tratamento, em especial quando a base legal é o legítimo interesse (art. 37);
- ✓ se controlador exerce mecanismo de verificação acerca da atuação dos operadores (art. 39);
- ✓ se estão publicamente divulgadas, preferencialmente em sítio eletrônico do controlador, a identidade e as informações de contato do encarregado (art. 41, § 1º)

Cabe ressaltar que, segundo a ABNT NBR ISO/IEC 29134:2020, a análise de *compliance* deve ser um dos itens da avaliação de impactos, concorrendo para a demonstração de boas práticas da instituição:

> "Embora convenha que uma PIA seja mais que simplesmente uma verificação de compliance, ela, entretanto, contribui para uma demonstração da organização quanto ao seu *compliance* com requisitos pertinentes de privacidade e proteção de dados na eventualidade de uma reclamação subsequente, auditoria de privacidade ou investigação de *compliance*."[18]

[16] Observe que essa demonstração pormenorizada deverá ser realizada no tópico 11, acerca das "Medidas, Salvaguardas e Mecanismos de Mitigação de Riscos".
[17] Observe que a comprovação pormenorizada da eficácia dessas medidas deverá ser realizada no tópico 11, acerca das "Medidas, Salvaguardas e Mecanismos de Mitigação de Riscos".
[18] ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg. 4/5.

A reflexão sobre esses pontos intenta direcionar o controlador na constatação dos riscos e de sua criticidade, de acordo com os parâmetros de *compliance* da lei e nos limites do contexto do tratamento proposto.

10- Inventário e Análise de Riscos

O inventário parte da análise acerca dos riscos imediatamente identificados e dos riscos prováveis, tendo em consideração o contexto do tratamento. Nesse sentido, o controlador pode ter um catálogo pré-estabelecido que aponte os riscos mais recorrentes. O *template* proposto pelo Governo Federal abarca, na versão 2.0, a identificação não exaustiva de 14 riscos, que incluem aqueles descritos pela ABNT NBR ISO/IEC 29134:2020, quais sejam: *R01) Acesso não autorizado; R02) Modificação não autorizada; R03) Perda; R04) Roubo; R05) Remoção não autorizada; R06) Coleção Excessiva; R07) Informação insuficiente sobre a finalidade do tratamento; R08) Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente); R09) Falha em considerar os direitos do titular de dados pessoais (Ex.: Perda do direito de acesso); R10-Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais; R11-Retenção prolongada de dados pessoais sem necessidade; R12-Vinculação/associação indevida, direta ou indireta dos dados pessoais do titular; R13-Falha/erro de processamento (Ex. execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.);R14-Reidentificação de dados pseudonimizados*.[19]

Entendemos que uma melhor classificação dos riscos poderia ajudar o controlador no momento da análise do tratamento de dados. Por isso, sugerimos que os riscos, ao menos no que se refere aos fatores legais vinculados, sejam classificados nas mesmas três categorias que usamos para a "Avaliação Principiológica e Demais Requisitos Legais", correspondente à perspectiva do ente ou instituto mais afetado. Nesse sentido os riscos poderiam ser assim classificados:

a) Riscos relacionados ao propósito institucional
b) Riscos diretamente relacionados ao titular
c) Riscos relacionados ao *compliance*

[19] Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_template_ripd.docx

Antes de especificar a classificação é necessário esclarecer alguns pontos. O objeto de RIPD é a identificação de riscos às liberdades civis e aos direitos fundamentais[20], tendo, portanto, como enfoque os riscos relacionados ao titular. A mencionada classificação não se olvida do expresso conceito legal, mas o destrincha em objetos imediatos de afetação.

De fato, todo tratamento de dados em contrariedade à lei é potencialmente prejudicial ao titular de dados, ainda que não exista um risco imediato. É o que acontece, por exemplo, quando é identificada uma brecha para acesso não autorizado, para citar um dos riscos elencados pelo *template* do Governo Federal. Se considerarmos um acesso interno por um funcionário que não deveria dispor dessa atribuição, por exemplo, não temos propriamente um vazamento de dados. Todavia, temos um processo de trabalho que apresenta falha pelos requisitos da LGPD porque permite um acesso irregular, e, portanto, promove um tratamento de dados que não se limita ao mínimo necessário, nos termos que prevê o princípio da necessidade.

Nesse caso, podemos inferir que o risco afeta de forma imediata as obrigações de *compliance* e apenas de forma mediata o titular de dados. Da mesma forma, existem riscos que afetam com maior intensidade os interesses da controladora do que os do titular de dados ao promover um tratamento de dados, por exemplo, infrutífero.

Portanto, podemos conceituar os itens desta classificação da seguinte forma:

a) Riscos relacionados ao propósito institucional

São aqueles diretamente relacionados ao propósito institucional, que afetem diretamente o tratamento de dados, e, indiretamente, os titulares dos dados pessoais. Deve-se observar os parâmetros estabelecidos na "Avaliação Principiológica e Demais Requisitos Legais". A partir deles, delimitar os riscos que se aplicam ao escopo do RIPD.

Por exemplo, digamos que o controlador, na Avaliação Principiológica, faça a análise deste quesito do propósito institucional:

- ✓ "se há possibilidade de alteração fundamental desse propósito durante a operação, ocasionando finalidade divergente da informada (princípio da finalidade);"

Ao promover o exame, o controlador detecte a possibilidade de alteração substancial do propósito institucional no decorrer do tratamento. Nesse caso ele deve registrar o "risco de tratamento excessivo" e deve suscitar também, como "risco diretamente relacionado ao titular" (que veremos a seguir), o risco de que as informações

[20] Nos termos do art. 5º, XVII, da LGPD.

prestadas aos titulares se tornem desatualizadas ou insuficientes com o novo propósito institucional. Da mesma forma, deve ser conferido se os métodos de armazenamento, a metodologia de tratamento, a qualidade dos dados, ou seja, as decisões institucionais para o tratamento de dados são adequadas para o propósito institucional com o tratamento de dados, em concordância com o princípio da adequação, apontando as lacunas ou inadequações como riscos; e assim sucessivamente.

b) Riscos diretamente relacionados ao Titular

O RIPD tem por principal enfoque a análise dos riscos às liberdades civis e aos direitos fundamentais dos titulares. De fato, como principais interessados, os titulares devem poder fiscalizar os riscos e, posteriormente, as eventuais medidas mitigatórias. Nesse sentido, deve-se observar os parâmetros avaliados na avaliação principiológica, observando se há falhas na garantia dos direitos dos titulares dentro do processo de tratamento pretendido.

c) Riscos relacionados ao *Compliance*

Geralmente, tanto os riscos relacionados ao propósito institucional quanto os relacionados ao titular estarão em certa medida, incorporados àqueles relacionados ao *compliance*, ou seja, à possibilidade de que o tratamento de dados não esteja em conformidade com a Lei. Mas existem riscos que atingem os titulares e os objetivos institucionais apenas indiretamente, sendo, portanto, prioritariamente tratados neste tópico da classificação. Da mesma forma, a análise desses riscos decorre da constatação de falhas ou limites de *compliance*, descrito no tópico acerca da Avaliação Principiológica e Demais Requisitos Legais.

Cabe ressaltar que a construção de uma lista exaustiva de riscos possíveis é pouco provável, e que, portanto, cada controlador deve levantar os riscos encontrados nas reflexões sobre o tópico 9 (“Avaliação principiológica e Demais Requisitos Legais”) e somá-los aos demais riscos encontrados no contexto específico do tratamento. A classificação que indicamos tem, nesse sentido, a pretensão apenas de direcionar o controlador na identificação dos riscos relacionados a fatores legais. Vale lembrar ainda que, conforme destacado pela ABNT NBR ISO/IEC 29134:2020, os riscos não se limitam aos fatores legais. Neste caso, extrapolando as exigências da LGPD e se estendendo a fatores externos, predeterminados em casos específicos e outros fatores que possam afetar “o *design* de sistemas de informação e os requisitos de proteção de privacidade

associados,"[21]. Isto inclui, por exemplo, vulnerabilidades suscitadas pelos próprios usuários. A ABNT NBR ISSO/IEC também orienta que sejam especificados os critérios de riscos, deixando evidente a metodologia utilizada na análise e que os riscos sejam avaliados de acordo com sua probabilidade e com os impactos que podem exercer quanto à privacidade, de acordo com a metodologia adotada e em conformidade com a ISO/IEC 27000:2018[22].

11- Medidas, Salvaguardas e Mecanismos de Mitigação de Riscos

O controlador deve apontar as medidas, salvaguardas e mecanismos de mitigação para os riscos inventariados, relacionados ao tratamento de dados proposto. Este tópico do RIPD busca especificar as ações relacionadas aos princípios da segurança, da prevenção, da responsabilização e prestação de contas previstos pela LGPD, além das Boas Práticas e Governança[23] adotadas pela instituição e especificamente relacionadas ao escopo do relatório. Nele devem ser descritos os procedimentos já adotados, aqueles em vias de adoção e os projetados para mitigação de cada risco identificado. Sugere-se que sejam respondidas, dentre outras, as seguintes perguntas:

- ✓ Quais são as garantias prestadas aos titulares acerca da exatidão, clareza, relevância e atualização dos dados, de acordo com o propósito institucional do tratamento? (princípio da qualidade dos dados)
- ✓ Quais são as medidas técnicas e administrativas utilizadas aptas a proteger os dados pessoais de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão? (Princípio da Segurança)
- ✓ Quais as medidas técnicas e administrativas utilizadas aptas a proteger os dados pessoais de acessos não autorizados (Princípio da Segurança) e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito? (art. 46)
- ✓ Demonstrar se essas medidas supramencionadas são adotadas desde a concepção do produto ou serviço até sua execução. (art. 46, § 2º)
- ✓ Quais são as medidas adotadas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais? (Princípio da responsabilização e prestação de contas)
- ✓ Quais são as medidas adotadas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; (Princípio da Prevenção)

[21] ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg.9.
[22] Conforme item 7.3.2 da ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg.34-35.
[23] Nos termos do que dispõe o art. 50 da LGPD.

- ✓ Existem experiências anteriores com esse tipo de tratamento de dados?
- ✓ Quais avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais e estejam diretamente relacionados ao escopo do RIPD?
- ✓ Quais mitigações foram propostas para amenizar o risco de adoção de nova tecnologia ou de novo método de tratamento que envolva dados pessoais?
- ✓ Demonstrar os mecanismos de controle sobre o operador: Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).
- ✓ Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais e se haverá alguma restrição de acesso alguma informação ou alguma mitigação na publicidade do RIPD, com a respectiva justificativa.
- ✓ Quais são as salvaguardas para as transferências internacionais de dados? (art. 33)
- ✓ Existem mecanismos adicionais de segurança: como termo de confidencialidade, ou gestão de identidades e usuários?
- ✓ Os benefícios esperados para o órgão, entidade ou para a sociedade como um todo são compatíveis com os riscos assumidos?

O objetivo é a reavaliação da criticidade dos riscos encontrados após a aplicação das medidas mitigatórias. Deve ser feita a análise se os benefícios esperados com o propósito institucional são compatíveis com os riscos assumidos. Caso positivo, para que sejam realizados os ajustes necessários e a filtragem dos riscos residuais, de acordo com a metodologia adotada. A ABNT NBR ISO/IEC 29134:2020 traz interessante diretriz para o estabelecimento de controles de riscos, identificando uma escala progressiva: 1) controle para impedir violação de dados (anonimização, minimização, informação aos titulares etc.); 2) controle para impedir que o risco ocorra, ou limitar seus efeitos; 3) controle para impedir que a fonte de risco identificada se torne um risco real; 4) controle para impedir exploração de vulnerabilidades, e de restauração da normalidade, caso o risco ocorra.[24]

Cabe mencionar ainda que o controlador, da mesma forma que ocorre na descrição do tratamento, deve observar se a ampla publicidade do inventário e análise dos riscos e das medidas de mitigação pode, em alguma medida, aprofundar vulnerabilidade ou enfraquecer medidas. Nesse sentido, a publicidade pode ser excepcionalmente mitigada, desde que devidamente justificada.

[24] ABNT NBR ISO/IEC 29134:2020. Tecnologia da informação — Técnicas de segurança — Avaliação de impacto de privacidade — Diretrizes. Primeira edição 26.11.2020. Pg.26.

12- Aprovação

Por fim, o RIPD será aprovado pelo controlador e assinado.

Conclusão

O modelo apresentado foi elaborado como um direcionador, para que o controlador, ao percorrer as etapas do documento, reflita sobre o processo, propondo, ao final, as alterações no projeto ou as medidas mitigatórias necessárias para contenção de riscos.

Nesse contexto, sem a pretensão de esgotar o tema, e partindo das recomendações já suscitadas pela ANPD, apresentamos essas sugestões para aprimoramento do modelo disponibilizado pelo Governo Federal.

A definição de um esboço acerca das principais informações que devem ser prestadas pelo controlador, seguindo uma lógica contínua na análise dos requisitos legais pode ser útil para a adaptação das metodologias usuais de riscos às exigências da Lei.