# Em direção a um método para avaliações de impacto sobre a proteção de dados: entendendo as exigências do RGPD

Kloza, Dariusz; Van Dijk, Niels; Casiraghi, Simone; Vazquez Maymir, Sergi; Roda, Sara; Tanas, Alessia; Konstantinou, Ioulia

*Published in:*
d.pia.lab Policy Brief

*Publication date:*
2020

*Document Version:*
Final published version

# Em direção a um método para avaliações de impacto sobre a proteção de dados: entendendo as exigências do RGPD

**d.pia.lab Documento de Política n.º 1/2019**

Dariusz KLOZA, Niels VAN DIJK, Simone CASIRAGHI, Sergi VAZQUEZ MAYMIR,
Sara RODA, Alessia TANAS e Ioulia KONSTANTINOU
Laboratório de Avaliações de Impacto à Privacidade e à Proteção de Dados de Bruxelas (d.pia.lab)

Este documento de política ('policy brief'[1]) estabelece as bases para um método de elaboração de Avaliações de Impacto sobre a Proteção de Dados (AIPD) na União Europeia (UE). Primeiro, como um pré-requisito, propõe-se um método genérico para avaliação de impacto, que pode ser utilizado – quando ajustado a um contexto particular – em múltiplas áreas, como o meio ambiente, o desenvolvimento tecnológico ou a regulação (Seção 2). Depois, a partir desse método genérico e com base na interpretação das exigências estabelecidas pelo Regulamento Geral de Proteção de Dados (RGPD), delineia-se as bases de um método específico para a realização de Avaliações de Impacto sobre a Proteção de Dados[2] (AIPD) na UE, que também deverá ser adaptável de acordo com o contexto de aplicação (Seção 3). Em particular, este documento de política pretende esclarecer dois aspectos cruciais desse método específico, que até o momento se têm mostrado os mais controversos. Esses aspectos são as técnicas de avaliação (isto é, o teste de necessidade e proporcionalidade, e a avaliação de risco), e o envolvimento de *stakeholders*[3] (incluindo a participação pública) no processo de tomada de decisão. A Seção 4 resume as descobertas e demonstra a necessidade de maiores orientações, esclarecimentos e adaptações. Os resultados são direcionados principalmente a tomadores de decisão que são responsáveis por desenvolver métodos para avaliação de impacto, bem como demais profissionais que adaptam esses métodos a um determinado contexto de aplicação e quem avalia processos de forma geral com base nos métodos aqui descritos.

## 1 INTRODUÇÃO

### 1.1 CONTEXTO

O Regulamento Geral de Proteção de Dados (RGPD, ou Regulamento) é o principal instrumento da modernização do quadro regulatório de proteção de dados pessoais na União Europeia (UE). O Regulamento traz uma série de novas soluções, cujo objetivo é, *inter alia*, "assegurar um nível de proteção coerente e elevado das pessoas singulares" (Considerando 10[4]) em qualquer situação em que seus dados pessoais sejam tratados. Entre esas novidades está a obrigação do responsável pelo tratamento[5] de realizar uma Avaliação de Impacto sobre a Proteção de Dados (AIPD) antes de iniciar o tratamento de dados. Esse processo é exigido sempre que as operações de tratamento de dados pessoais sejam susceptíveis de implicar um "elevado risco[6] para os direitos e liberdades das pessoas singulares" (Artigo 35º, nº 1),

[1] "Um policy brief é um resumo conciso de um determinado assunto, as opções de políticas para lidar com esse assunto e algumas recomendações sobre a melhor opção. É direcionado a formuladores de políticas públicas e outros indivíduos que estejam interessados em formular ou influenciar políticas." Food and Agriculture Organization, *Food Security Communications Toolkit*, Rome 2011, p. 141. (Todas as citações utilizadas nesta tradução são tiradas da tradução oficial para o português do Regulamento Geral de Proteção de Dados [RGPD]. Como o padrão europeu é o português de Portugal, algumas expressões podem ser diferentes das utilizadas no direito brasileiro. Todas as notas de rodapé são provenientes do tradutor.)

[2] A Lei Geral de Proteção de Dados (LGPD) trabalha com o termo "relatório de impacto à proteção de dados pessoais", conceituado no Artigo 5º, XVII, enquanto o RGPD utiliza a expressão "avaliação de impacto sobre a proteção de dados pessoais" no seu Artigo 35º.

[3] Vd. Item 2, Fase IV.

[4] 'Recitals' ou 'Considerandos' são textos que contêm a fundamentação do dispositivo (artigo) do regulamento, cf.: http://publications.europa.eu/code/pt/pt-120200.htm.

[5] O Responsável pelo tratamento corresponde, na LGPD, à figura do controlador, um dos agentes de tratamento de dados pessoais. É aquele a que competem as decisões sobre o tratamento de dados pessoais (Artigo 5º, VI da LGPD) e em nome do qual o tratamento é realizado. No RGPD, essa figura está conceituada no Capítulo IV, Seção 1, Artigo 24º.

[6] Destaca-se que a LGPD fala em 'risco', mas não faz nenhuma diferenciação entre níveis ('alto risco'), cf.: "Artigo 5º, XVII – avaliação de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados

 ISSN 2565-9936

devendo ser realizado para "assegurar a proteção dos dados pessoais e demonstrar conformidade com o presente regulamento" (Artigo 35º nº 7, d).

A AIPD é uma forma de Avaliação de Impacto (*Impact Assessment*, *IA*) e – em grande medida – é uma variação da Avaliação de Impacto à Privacidade (AIP) (*Privacy Impact Assessment*, *PIA*). De uma forma geral, uma avaliação de impacto é uma ferramenta usada para a análise de possíveis consequências de uma iniciativa sobre um interesse ou interesses sociais relevantes (ou seja, sobre um assunto ou assuntos de interesse ou importantes), se essa iniciativa puder apresentar perigos a esses interesses. Essa ferramenta tem por objetivo apoiar um processo decisório informado sobre se se deve começar a iniciativa e sob quais condições, acabando por se traduzir – em primeiro lugar – num meio de proteção dos referidos interesses sociais.

A obrigação de conduzir uma AIPD reflete uma abordagem baseada no risco para a proteção de dados pessoais no novo regime jurídico da UE e no reforço do princípio da responsabilidade[7] (Artigo 5º nº 2). Aproveitando a experiência das técnicas de avaliação em outros campos (e.g. avaliação de impacto regulatório, tecnológico ou ambiental), espera-se que a AIPD possa se tornar um instrumento poderoso de cumprimento, e execução, das normas (leis de) proteção de dados pessoais.

Simultaneamente, o processo de AIPD vem sendo progressivamente regulado por outros instrumentos do regime jurídico europeu de proteção de dados pessoais. Para além do RGPD, a obrigação de realizar uma AIPD está presente, até o momento, na Diretiva (UE) 2016/680 sobre a proteção de dados pessoais em matéria criminal (Artigo 27º), no Regulamento (UE) 2018/1725 sobre a proteção de dados pessoais tratados pelas instituições, órgãos, organismos e agências da União Europeia (Artigos 39º e 89º), e na Diretiva (EU) 2019/1024 relativa aos dados abertos e à reutilização de informações do setor público (Considerando 53). A proposta de Regulamento relativo à Privacidade e às Comunicações Eletrônicas (a 'ePrivacy Regulation'), se aprovada com sua atual redação, também irá exigir a realização de uma AIPD em determinadas situações (Artigo 6º). (Anteriormente, a UE também implementou regimes voluntários para a realização de AIP e AIPD no contexto de tecnologias de identificação por radiofrequência (IDRF) e de redes elétricas 'inteligentes'. Paralelamente, a Convenção 108+[8] do Conselho da Europa criou uma obrigação comparável por meio do Artigo 10º, nº 2. Para além da Europa, várias formas de AIP e AIPD têm sido praticadas na Austrália, no Canadá, no Japão, na África do Sul, na Coreia do Sul, nos Estados Unidos e na Nova Zelândia, entre outros países. Ao mesmo tempo, organizações internacionais, como o Comitê Internacional da Cruz Vermelha, exigem processos de avaliação semelhantes nos seus estatutos.

Essas obrigações de realização de AIPDs na UE suscitam uma série de questões. Novos conceitos-chave que nos quais a AIPD se baseia (e.g. risco para um direito), terminologias imprecisas utilizadas pela legislação (e.g. 'grande escala' ou 'sistemático') e a eventual imposição de multas elevadas em caso de não-conformidade e negligência, são algumas delas. Ademais, a estipulação de apenas aspectos-chave da AIPD dá lugar a uma enorme flexibilidade às custas da segurança jurídica, o que, por conseguinte, exige uma interpretação e orientação normativa. A Comissão Europeia, ao apresentar a proposta para reforma do regime jurídico relativo à proteção de dados pessoais, denominou esta abordagem de 'gancho legal', e indicou que o legislador apenas deveria legislar sobre os mínimo aspectos considerados essenciais[9]. Qualquer outra especificação, se necessária, deveria resultar, por exemplo, da indústria ou da administração pública. Apenas se esses esforços falharem ou forem insuficientes, deve o legislador intervir. Em 2017, o então Grupo de Trabalho do Artigo 29[10] emitiu recomendações sobre a AIPD na UE e sobre como determinar quando uma operação de tratamento de dados é suscetível de implicar um 'elevado risco'. As recomendações esclareceram alguns aspectos relativos tanto ao enquadramento como ao método (e.g. análise de limiar) para a avaliação de impacto, tratando no entanto outros aspectos de forma superficial (e.g. a avaliação da necessidade e da proporcionalidade ou o envolvimento de partes interessadas – '*stakeholders*'). As orientações acadêmicas e profissionais ainda não ofereceram igualmente esclarecimentos suficientes.

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

[7] Relevante destacar que tanto a LGPD, no Artigo 6º, X, quanto o RGPD, no Artigo 5º, nº 2 elencam a responsabilidade ('*accountability*') como princípio de proteção de dados pessoais. No caso brasileiro, optou-se por traduzir o termo '*accountability*' como responsabilidade e prestação de contas, o que evidencia o caráter duplo desse princípio – não basta estar em conformidade com as exigências regulatórias, mas é necessário desenvolver meios adequados para demonstrar tal conformidade.

[8] O "+" em Convenção 108+ refere-se à versão modernizada do documento, cf.: https://www.coe.int/en/web/data-protection/convention108/modernised.

[9] LGPD, a avaliação de impacto à proteção de dados é descrito em duas ocasiões, cf.: "Artigo 5º, XVII – avaliação de impacto à proteção de dados pessoais: 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" e "Artigo 38º, Parágrafo único. Observado o disposto no caput deste artigo, o avaliação deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados." Verifica-se, portanto, que não há procedimentalização alguma do avaliação de impacto, de forma que caberá à Autoridade Nacional de Proteção de Dados (ANPD) desenhar seus contornos e estipular parâmetros para sua condução.

[10] O Grupo de Trabalho do Artigo 29 esteve em operação até 25 de maio de 2018, ocasião em que foi substituído pelo Comité Europeu para a Proteção de Dados (CEPD) (*European Data Protection Board*, *EDPB*). O CEPD é o órgão da UE responsável pela aplicação do RGPD. Foi criado em 25 de maio de 2018, em substituição ao Grupo de Trabalho do Artigo 29. É composto pelos chefes de todas as Autoridades Nacionais de Proteção de Dados e o *European Data Protection Supervisor* (EDPS).

Um dos aspectos diz respeito ao método, isto é, ao conjunto das etapas para conduzir o processo de avaliação. O presente documento de política é dedicado a esse aspecto.

### 1.2 PANO DE FUNDO

A 'arquitetura' da avaliação de impacto tipicamente consiste em dois elementos principais, a 'estrutura' ('*framework*') e o 'método'. Um *framework* constitui uma "estrutura de suporte essencial" ou um arranjo organizacional para a política de avaliação de impacto, além de definir e descrever as suas condições e princípios. Por sua vez, um método, que é um "procedimento particular para realizar ou abordar algo", diz respeito à prática da avaliação de impacto e define os passos consecutivos e/ou iterativos que devem ser tomados para realizar tal processo. Um método corresponde a uma estrutura e pode ser encarado como um reflexo prático dela. Esta 'arquitetura' é costumeiramente suplementada por diretivas (manuais, guias) e modelos, que explicam mais profundamente o processo de avaliação e auxiliam na estruturação de todo o processo e na redação de um relatório final para documentá-lo.

Múltiplas estruturas e métodos para avaliação de impacto já existem, em várias áreas e com variadas aplicabilidades e qualidades. Uma necessidade constante de novos métodos e estruturas decorre do princípio da receptividade da avaliação de impacto, isto é, tanto a estrutura quanto o método devem ser constantemente melhorados para que a avaliação de impacto concretize seus objetivos de uma forma melhor (aprendendo com sua própria experiência ou com a experiência de outras técnicas de avaliação), responda melhor a mudanças sociais e se aplique a novas áreas de avaliação de impacto (e.g. a 'avaliação de impacto algorítmica', recentemente proposta).

### 1.3 ESTRUTURA

Esse documento de política apresenta as bases para um método para a realização de Avaliações de Impacto sobre a Proteção de Dados (AIPD) na União Europeia (UE). Primeiro, como um pré-requisito, ele propõe um método genérico para avaliação de impacto, que pode ser utilizado – quando ajustado a um contexto particular – em múltiplas áreas, como o meio ambiente, o desenvolvimento tecnológico ou a regulação (Seção 2).

O método genérico reflete uma estrutura de 16 princípios para avaliação de impacto em múltiplas áreas práticas, desenvolvidos no documento de política anterior do d.pia.lab (2017).[11] O segundo método apresentado no documento é específico para a proteção de dados pessoais e – mais concretamente – diz respeito ao processo de AIPD na UE. Ele é extraído de uma interpretação das disposições do RGPD à luz do método genérico (Seção 3). Esse método também deve ser ajustado ao contexto de utilização. Ao construir esse último método, focou-se em assuntos particularmente polêmicos como o envolvimento de *stakeholders* (inclusive por meio de participação pública) no processo de tomada de decisão, e assuntos menos debatidos que até o momento têm se provado difíceis na prática, como a avaliação de necessidade e proporcionalidade, e a avaliação de risco para os direitos e liberdades dos indivíduos. Esses dois métodos são construídos a partir de uma avaliação crítica e de uma análise comparativa das estruturas e métodos existentes para avaliação de impacto, e da sua experiência em várias áreas diferentes, em particular a privacidade, a proteção de dados pessoais ('privacidade informacional'), o desenvolvimento tecnológico, o meio ambiente, a regulação e os direitos humanos.

Esse documento de política tem dois principais destinatários. Considerando que os métodos para avaliação de impacto precisam ser adaptados ao seu respectivo contexto de utilização, os primeiros destinatários são tomadores de decisão, particularmente autoridades de controle sobre o tratamento) no nível da UE e dos Estados Membros, que precisam desenvolver métodos para que AIPDs sejam adaptáveis aos seus contextos nacionais. Este documento de política também é dirigido aos demais *stakeholders* que adaptam esses métodos de AIPD para um contexto específico de uso e, assim, potencialmente aos responsáveis pelo tratamento que conduzem o processo de avaliação. Ao mesmo tempo, também se espera que o método genérico de avaliação de impacto seja útil nas várias áreas em que a avaliação de impacto é praticada.

## 2 UM MÉTODO GENÉRICO PARA AVALIAÇÃO DE IMPACTO

O método genérico proposto para avaliação de impacto foi desenvolvido a partir de uma análise comparativa e de uma crítica aos passos recorrentes de métodos de avaliação praticados em múltiplas áreas, refinadas com as próprias experiências do d.pia.lab. Paralelamente, o método genérico reflete o regime de 16 princípios formulado no documento de política do d.pia.lab em 2017.

O método genérico fornece a base para métodos específicos de avaliação de impacto em diferentes áreas e práticas. O método genérico consiste em dez passos (seis passos consecutivos, três passos executados ao longo de todo o processo e um passo conduzido ao final), agrupados em cinco fases. Alguns desses passos seguem uma sequência lógica, enquanto outras são uma função dos princípios incorporados na estrutura. Os passos são os seguintes:

**Fase 1: Preparação do processo de avaliação**

1) *Triagem (análise de limiar).* Este passo determina se o processo de avaliação de impacto é necessário para uma determinada iniciativa planejada, ou uma série de iniciativas similares, em um dado contexto. A triagem é baseada

[11] Cf.: Dariusz Kloza, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani e Paul Quinn (2017) *Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos*, d.pia.lab Documento de Política n.º 1/2017, Vrije Universiteit Brussel (VUB): Bruxelas; https://cris.vub.be/files/49998404/dpialab_pb2017_1_final_PT.pdf.

em uma descrição inicial, embora suficientemente detalhada, dessa determinada iniciativa, tanto do ponto de vista contextual, quanto técnico. A decisão é tomada com base em critérios definidos, tanto internos (i.e., as próprias políticas da organização), quanto externos (i.e., aqueles provenientes de exigências legais/regulatórias), ou em critérios *ad hoc*, como pressão pública. Se um processo de avaliação não for necessário, nem justificável, todo o processo é concluído com uma declaração que fundamente a inexistência de um impacto significativo.

2) *Âmbito*. Este passo, baseado na descrição inicial, tem como objetivo identificar:
   a) uma questão social, ou questões sociais, como a privacidade, a proteção de dados pessoais, a ética (aplicada), ou o ambiente (biofísico) humano ou natural, que podem ser atingidas por uma iniciativa planejada, e as exigências legais ou regulatórias correspondentes; essas questões são a matriz de referência de todo o processo de avaliação;
   b) *stakeholders* que são ou (podem ser) afetados, preocupam-se ou se interessam, ou ainda possuem conhecimento sobre a iniciativa em questão, bem como seu nível de envolvimento;
   c) técnicas (métodos *stricto sensu*) para a avaliação de impactos e para o envolvimento de *stakeholders*, inclusive no que diz respeito à participação pública, no processo decisório, que serão utilizadas durante o processo de avaliação; e
   d) outras técnicas de avaliação, para além do processo de avaliação de impacto, que possam ser necessárias ou desejadas a fim de garantir, por exemplo, a completude da informação utilizada no processo de tomada de decisão (e.g. avaliação tecnológica ou avaliação de impacto ambiental).

   Nem todos esses elementos e pessoas podem ser identificáveis no início do processo de avaliação e, portanto, sua identificação pode precisar ser revisada periodicamente.

3) *Planejamento e preparação*. Este passo define os termos de referência para a realização do processo de avaliação. Esses termos incluem, dentre outros:
   a) os objetivos da avaliação;
   b) os critérios para a aceitação de impactos negativos;
   c) os recursos necessários (i.e., tempo, dinheiro, mão de obra, conhecimento, know-how, local e infraestrutura);
   d) os procedimentos e os cronogramas para o processo de avaliação;
   e) o(a) avaliador(a) ou time de avaliadores(as) (*in-house* ou terceirizados(as)), seus papéis e responsabilidades e a garantia de sua independência profissional; e
   f) a continuidade do processo de avaliação.

**Fase 2: Avaliação**

4) *Descrição*. Este passo, baseado na descrição inicial (cf. Passo 1), fornece um relato detalhado, em duas partes, da iniciativa planejada. Primeiro, há a descrição contextual, que tipicamente consiste em:
   a) um panorama da(s) iniciativa(s) prevista(s) e da organização que a(s) promove;
   b) o contexto de desenvolvimento da iniciativa;
   c) a necessidade da iniciativa;
   d) as possíveis interferências sobre interesses sociais; e
   e) os benefícios e desvantagens esperados.

   Em segundo lugar, há a descrição técnica. No caso de avaliações de impacto ambiental (AIA), esta etapa fornece uma descrição, por exemplo, dos componentes do ambiente biofísico afetados, e, no caso da AIPD, descreve, por exemplo, categorias de dados pessoais e seus fluxos dentro de uma operação de tratamento.

5) *Avaliação de impacto.* Neste passo, os impactos da iniciativa prevista são avaliados de acordo com as técnicas pré-selecionadas. Esses impactos dizem respeito aos interesses sociais que podem ser atingidos pela iniciativa planejada, e aos *stakeholders*, em maioria externos à organização promotora. Tipicamente, esta avaliação consiste em – ao menos – identificação, análise e avaliação detalhadas dos impactos. As técnicas de avaliação vão de análise de risco (gerenciamento de risco qualitativo ou quantitativo ou uma combinação dos dois) e análise de cenário (planejamento) e previsões tecnológicas, passam por verificação de conformidade legal e regulatória, técnicas de interpretação jurídica e avaliação de proporcionalidade e necessidade, até uma análise de custo-benefício e uma análise de forças, fraquezas, oportunidades e ameaças ('análise SWOT').

**Fase 3: Recomendações**

6) *Recomendações.* Neste passo, medidas concretas e detalhadas (controles, salvaguardas, soluções, etc.), seus destinatários, suas prioridades e os cronogramas para abordá-las são propostas para minimizar os impactos negativos da iniciativa planejada e, se possível, maximizar os impactos positivos. O(a) avaliador(a) deve justificar a distinção entre os impactos 'negativos' e 'positivos', na medida em que tal distinção é contextual e subjetiva. O(a) avaliador(a) deve fazer um balanço das medidas já implementadas. Dessa forma, após a conclusão da avaliação, a liderança da organização promotora tomará uma decisão quanto ao desenvolvimento da iniciativa e as condições para tal (entretanto, uma organização promotora pode implementar recomendações progressivamente, ainda durante o processo de avaliação). Uma iniciativa normalmente é cancelada se os impactos negativos são considerados inaceitáveis; continuar com tal iniciativa seria algo excepcional e requereria justificativa suficiente.

**Fase 4: Passos contínuos**

7) *Envolvimento de stakeholders, inclusive por meio de participação pública, no processo decisório.* Este é um passo contínuo e transversal que ocorre durante todo o processo, no qual *stakeholders*, inclusive o público ou seus representantes, participam do processo de avaliação.

   De forma ampla, um *stakeholder* é alguém que tem um interesse em algo, independente de ele ou ela estar ciente disso e de quão diretamente esse interesse está articulado. No contexto de avaliação de impacto, trata-se de alguém que questiona (agora) ou pode questionar (no futuro), que é (ou pode ser) afetado, que se preocupa ou se interessa pela iniciativa planejada, (potencialmente) positivamente e/ou negativamente. Ao mesmo tempo, um *stakeholder* pode ser alguém que possui conhecimentos específicos e *know-how* sobre a iniciativa, ou seja, um especialista. O conceito de *stakeholder* é, portanto, aberto e abrange o público (leigos, etc.), tomadores de decisão, especialistas, e daí por diante. *Stakeholders* podem ser indivíduos ou entidades coletivas, independente se formalmente (legalmente) constituídas (podem ser grupos sociais, comunidades, nações, o público como um todo, organizações da sociedade civil, etc.). Existem múltiplos (grupos de) *stakeholders* e, portanto, eles podem ser agrupados em: (i) internos (e.g. empregados, comitês de trabalho) e externos (e.g. organizações de consumidores ou organizações não-governamentais); (ii) primários (i.e., aqueles com um interesse direto na iniciativa, e.g. investidores) e secundários (i.e., aqueles com um interesse indireto, mas ainda assim influente, e.g. o Estado) ou, ainda; (iii) podem ser classificados de acordo com seus atributos; poder, legitimidade e urgência.

   O envolvimento de *stakeholders* constitui um componente integral do processo de avaliação e normalmente é eliminado apenas em situações excepcionais. Se o envolvimento de *stakeholders* não se justificar ou não for necessário, tal escolha deve ser explicada e documentada. Sempre que o envolvimento de *stakeholders* for obrigatório, eles poderão tomar medidas legais caso esse envolvimento seja excluído ou insuficiente na prática, proporcionalmente ao nível de envolvimento buscado em um determinado processo de avaliação. Em qualquer caso, o envolvimento de *stakeholders* não compromete nenhum segredo legítimo (e.g. segredo de Estado ou segredo comercial), nem traz quaisquer consequências negativas para os seus participantes (e.g. exploração).

   O nível de envolvimento de um *stakeholder* pode variar de: (a) meramente ser ensinado ou informado sobre uma iniciativa planejada (baixo nível); a (b) diálogo e consulta em que as visões dos *stakeholders* são ouvidas e levadas em consideração (nível médio); ou ainda (c) tratar-se de co-decisão pelos *stakeholders* e a organização promotora sobre o desenvolvimento da iniciativa em questão e, subsequentemente, firmar-se parceria com os *stakeholders* para sua implementação (nível alto).

   Existe um conjunto de técnicas para o envolvimento de stakeholders, que vão desde avisos, entrevistas, questionários e *surveys*, até grupos focais, mesas redondas, oficinas e painéis de cidadãos, incluindo técnicas estruturadas, como 'world café[12]' ou 'Delphi[13]'. Uma técnica, ou conjunto de técnicas apropriadas, é selecionada dependendo do nível de envolvimento de *stakeholders* desejado, da iniciativa planejada, do contexto de desenvolvimento da iniciativa e dos recursos à disposição da organização promotora.

   O envolvimento de *stakeholders* pode trazer vários benefícios para o processo de avaliação (e.g. aumentando sua qualidade, credibilidade e legitimidade), mas estes benefícios devem ser contrastados com as desvantagens, que incluem a questão de representatividade (sobre ou sub representatividade), justiça (e.g. manipulação, *'astroturfing'*[14]), relutância, barreiras de comunicação, conflito entre interesses públicos e privados e a necessidade de utilização intensiva de recursos que marca o processo de envolvimento de *stakeholders*.

8) *Documentação.* Este é um passo contínuo, transversal, que ocorre durante todo o processo, em que registros inteligíveis são mantidos, em forma escrita ou outra forma permanente, de todas as atividades desempenhadas durante o processo de avaliação. Esse passo inclui a preparação de um relatório final do processo de avaliação (ou uma declaração de impacto não-significativo, quando aplicável). O espectro completo de documentação de um determinado processo de avaliação, preferencialmente em formato eletrônico, pode ser tornado público, registrado de forma centralizada, e/ou apresentado para inspeção mediante requerimento (com o devido respeito à confidencialidade legítima).

9) *Controle de qualidade.* Este é um passo contínuo, transversal, que ocorre durante todo o processo, em que a aderência a um padrão de performance é verificada, ou internamente (e.g. pelo monitoramento de progresso ou uma revisão pela organização promotora) ou externamente (e.g. por uma autoridade reguladora independente por meio de uma

[12] O 'world café' é um método de livre acesso para todas as pessoas, engendrada por Juanita Brown e David Isaacs. Tratase de um processo criativo que visa gerar e fomentar diálogos entre os indivíduos, a partir daí criando uma rede viva de diálogo colaborativo que acessa e aproveita a inteligência coletiva para responder questões de grande relevância para organizações e comunidades. Cf.: http://www.theworldcafe.com.

[13] O método Delphi é um método de tomada de decisão em grupo que se caracteriza pelo facto de cada membro do grupo apresentar as suas ideias mas nunca face a face com os restantes elementos (como acontece por exemplo no método do grupo nominal ou no brainstorming). Cf.: https://knoow.net/cienceconempr/gestao/metodo-ou-tecnica-delphi.

[14] '*Astroturfing*' é a prática enganosa de apresentar uma campanha de marketing ou relações públicas orquestrada como se fosse uma série de comentários espontâneos de membros do público. Cf.: Oxford Dictionary of English (tradução); https://www.lexico.com/definition/astroturfing.

auditoria, ou por um tribunal), ou ambos. O controle de qualidade pode igualmente ocorrer durante ou depois do processo de avaliação, ou ambos.

**Fase 5: Revisitando**

10) *Revisitando*. Neste passo, uma decisão é tomada sobre se se deve conduzir o processo novamente, integralmente ou em parte. Esse passo pode ocorrer toda vez que a iniciativa prevista for alterada (antes ou depois do seu desenvolvimento) ou toda vez em que o contexto em que ela vai ser desenvolvida, ou já foi desenvolvida, mudar. Essa etapa também garante a continuidade do processo de avaliação em casos como a transferência/terceirização da iniciativa para uma outra organização.

O método supramencionado para avaliação dos impactos de uma iniciativa sobre interesses sociais é de natureza genérica e deve ser adaptado para as especificidades e necessidades de uma determinada área, dos *stakeholders* (inclusive o público em geral) envolvidos e do contexto de cada uso. Por exemplo, a avaliação de impacto na área de proteção de dados pessoais na UE implica uma abordagem específica, no mínimo, dos passos de *Triagem* (*análise de limiar*), *Âmbito* (e.g. uma lista de interesses sociais), *Avaliação de impacto* (e.g. técnicas para a avaliação e uma lista de possíveis impactos), *Envolvimento de stakeholders*, inclusive por meio de participação pública, no processo decisório (e.g. *stakeholders* e técnicas para envolvê-los) e *Recomendações*.

**DISPOSIÇÕES RELEVANGTES DO RGPD**

**Artigo 35º**

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação. [...]

7. A avaliação inclui, pelo menos:

   a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

   b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;

   c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o nº 1; e

   d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa. […]

9. Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento.

**Artigo 36º**

1. O responsável pelo tratamento consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados [...] indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.

2. Sempre que considerar que o tratamento previsto [...] violaria o disposto no presente regulamento, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controlo [...] dá orientações, por escrito, ao responsável pelo tratamento e, se o houver, ao subcontratante[15] e pode recorrer a todos os seus poderes [...]

## 3 UM MÉTODO PARA AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS NA UNIÃO EUROPEIA

O método específico para AIPD exigido pelo RGPD na UE e descrito abaixo foi extraído com base na interpretação das disposições densamente formuladas nos Artigos 35º-36º e à luz do método genérico. O RGPD obriga que um responsável pelo tratamento conduza um processo de avaliação e que um subcontratante, quando aplicável, dê assistência ao responsável. É o responsável pelo tratamento que deve prestar contas sobre o processo de avaliação[16].

O Regulamento prevê sete passos a serem tomados, especificamente:

[15] Na LGPD, 'subcontratante' traduz-se em 'operador', figura descrita e regulada pelo Artigo 5º, VII e Artigo 39º.
[16] A responsabilidade na LGPD é, em regra, solidária (Artigo 42º). É discutido, entretanto, se o regime é de responsabilidade subjetiva, objetiva ou uma terceira espécie.

1) *Triagem (análise de limiar)*: a fim de determinar se um processo de AIPD é exigido por lei, as operações de tratamento de dados previstas, com base em uma descrição inicial dessas operações e em uma avaliação de risco rudimentar, deverão ser examinadas a partir dos seis critérios a seguir:
   - *Critério 1 – probabilidade de elevado risco (geral)*: no nível mais geral, o Regulamento exige que um processo de AIPD seja conduzido para operações de tratamento suscetíveis de implicar um elevado risco para direitos e liberdades de pessoas naturais, levando em consideração quatro critérios qualitativos – a natureza, o âmbito, o contexto e a finalidade do tratamento de dados pessoais. Particularmente, operações de tratamento de dados que envolvem novas tecnologias constituem um gatilho específico para o processo de avaliação (Artigo 35º, nº 1). Esses critérios, entretanto, não são mais detalhados. Eles podem incluir, por exemplo, o tratamento de dados sensíveis, dados relacionados a condenações criminais e infrações ou dados relacionados a medidas de segurança ou dados biométricos (i.e., a natureza das operações de tratamento), a quantidade de dados tratados, o alcance geográfico e o número de pessoas afetadas (i.e., o âmbito), o uso de um determinado tipo de tecnologia ou a área de uso (e.g. publicamente acessível) (i.e., o contexto), ou dados para *profiling* ou tomada de decisões automatizadas (i.e., a finalidade) (cf. Considerando 91). O então Grupo de Trabalho do Artigo 29, na sua opinião sobre como determinar se é provável que um tratamento "resulte em um elevado risco" (2017), recomendou que nove critérios sejam considerados para determinar se o risco está em um nível elevado; exemplos dos critérios são se as bases de dados estão sendo associadas ou combinadas e se o tratamento de dados pessoais diz respeito a titulares vulneráveis. De qualquer forma, cabe ao responsável pelo tratamento determinar se o nível do risco é elevado.
   - *Critério 2 – probabilidade de elevado risco (enumeração)*: o Regulamento prevê três tipos de operações de tratamento de dados para as quais uma AIPD é exigida, porque é provável que tais operações impliquem um elevado risco para os direitos e liberdades de pessoas naturais. Em outras palavras, as operações de tratamento de dados a seguir são consideradas pela lei como altamente arriscadas; a lista não é taxativa.
     - "avaliação sistemática e completa de aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar";
     - operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e
     - "controlo sistemático de zonas acessíveis ao público em grande escala" (Artigo 35º, nº 3).
   - *Critério 3 – probabilidade de elevado risco (enumeração positiva por autoridades de controle sobre o tratamento de dados)*: uma autoridade de controle nacional ou regional tem a prerrogativa de determinar, para sua própria jurisdição, outros tipos de operações de tratamento de dados para as quais uma AIPD é exigida (Artigo 35º, nº 4)[17].
   - *Critério 4 – probabilidade de elevado risco (enumeração negativa por autoridades de controle sobre o tratamento de dados)*: as mesmas autoridades podem determinar, para suas próprias jurisdições, outros tipos de operações de tratamento de dados para as quais uma AIPD não é exigida (Artigo 35º, nº 5). Ambas as listas, caso envolvam – de forma geral – operações transfronteiriças de proteção de dados, devem ser comunicadas, pelo mecanismo de consistência, ao Comité Europeu para a Proteção de Dados (CEPD)[18] para sua opinião (Artigo 35º, nº 4-6). O CEPD tem emitido estas opiniões desde 2018.
   - *Critério 5 – prévia avaliação de impacto regulatória*: a não ser que Estados Membros decidam de outra forma, para dados pessoais tratados para o cumprimento de uma obrigação jurídica (Artigo 6º, nº 1, c) ou tratados em razão do interesse público (Artigo 6º, nº 1, e), com base em lei da UE ou do Estado Membro, quando o tratamento já tenha sido avaliado dentro de algum processo de avaliação no contexto da adoção daquela base legal, o processo de AIPD não é mais exigido, desde que este outro processo de avaliação essencialmente satisfaça as condições descritas no RGPD (Artigo 35º, nº 10).
   - *Critério 6 – exceções para profissões específicas*: se as operações de tratamento dizem respeito a "dados pessoais de pacientes ou clientes de um médico em particular, outros profissionais de saúde ou um advogado", estas operações não são consideradas de grande escala (cf. e.g. Artigo 35º, nº 3, b) e, desta forma, para tais operações de tratamento o processo de AIPD não é exigido (Considerando 91).

   Se qualquer um dos três primeiros critérios for satisfeito, o processo de AIPD é obrigatório. Inversamente, se qualquer um dos três últimos critérios for satisfeito, o responsável pelo tratamento está isento de conduzir o processo de avaliação.

[17] As Autoridades Nacionais de Proteção de Dados (APDs) dos Estados Membros da UE elaboraram listas individuais, chamadas '*white lists*', para tratar de atividades que não requerem AIPD e '*blacklists*' para atividades que devem ser precedidas pelo avaliação, cf.: https://iapp.org/resources/article/eu-member-state-DPIA-whitelists-and-blacklists. Posteriormente, o CEPD emitiu uma opinião para cada uma das listas, com o objetivo de uniformizar o entendimento em torno da necessidade de AIPD, cf.: https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en.

[18] Vd. nota 10.

2) *Descrição*: o Regulamento exige que a avaliação comece com "uma descrição sistemática das operações de tratamento previstas" (Artigo 35º, nº 7, a). Tal descrição inclui, em particular:

   a) uma descrição *contextual* das operações de tratamento de dados previstas, particularmente sua natureza, âmbito, contexto e finalidade, o legítimo interesse do responsável pelo tratamento (se aplicável)[19] e os *stakeholders* envolvidos (titulares de dados, responsáveis pelo tratamento, subcontratantes, terceiros e autoridades públicas);

   b) uma descrição técnica contendo os fluxos de dados pessoais e – possivelmente – uma visualização deles.

   A descrição das operações de tratamento de dados previstas pode ser baseada na descrição inicial que foi utilizada para determinar se o processo de avaliação era necessário (cf. Passo 1).

3) *Avaliação da operação de tratamento prevista, ou de um grupo de operações similares*: o Regulamento exige o uso, consecutivo ou paralelo, de ao menos duas técnicas de avaliação distintas (métodos *stricto sensu*), especificamente a avaliação de necessidade e proporcionalidade e a avaliação de risco. Ambas as técnicas constituem, em grande medida, novidades nas leis de proteção de dados pessoais. Seguindo a abordagem do 'gancho legal' a definição do RGPD é genérica e não especifica exatamente como essas técnicas devem ser usadas.

   a) A avaliação de "necessidade e proporcionalidade das operações de tratamento em relação aos objetivos"[20] (Artigo 35º, nº 7, b).

      O teste de necessidade e proporcionalidade refere-se à observância dos princípios relativos ao tratamento de dados pessoais (Artigo 5º, nº 1). Particularmente, diz respeito ao princípio da limitação das finalidades – isto é, ele primeiro pergunta sobre a finalidade da operação de tratamento de dados, se "o tratamento poderia ser razoavelmente realizado por outros meios" (Considerando 39) e se os dados pessoais seriam "coletados para fins específicos, explícitos e legítimos e não tratados posteriormente" de uma incompatível com aquelas finalidades[21] (Artigo 5º, nº 1, b). Ademais, a avaliação diz respeito ao princípio da licitude do tratamento (Artigo 6º), e aos princípios de minimização de dados, exatidão e limitação da conservação. Em outras palavras, pergunta se os dados pessoais seriam "tratados de forma lícita, leal e transparente", se o tratamento seria "adequado, pertinente e limitado ao necessário em relação às finalidades", se os dados pessoas seriam "exatos e atualizados sempre que necessário" e se seriam conservados "apenas durante o período necessário" (Artigos 5º, nº 1, a-e).

      Tal avaliação deve ser realizada a partir de uma análise dos fatos baseada em evidências suficientes, claramente descritas e verificáveis. O conteúdo da avaliação de necessidade e proporcionalidade difere entre o setor privado e o setor público. Além disso, quanto ao último é necessária uma maior diferenciação entre a criação e a aplicação da lei.

   b) A avaliação dos "riscos para os direitos e liberdades dos titulares" (Artigo 35º, nº 7, c).

      Avaliação de risco, no contexto de AIPD, tipicamente refere-se a uma identificação, análise e avaliação detalhadas das futuras possíveis consequências negativas das operações de tratamento de dados, e, mais concretamente, dos danos causados por tais operações. A sua avaliação diz respeito a "danos físicos, materiais ou imateriais" e inclui, por exemplo, discriminação, roubo de identidade e fraude, perda financeira ou dano à reputação, perda de confidencialidade, reversão não-autorizada de pseudonimização, qualquer desvantagem social ou econômica considerável, perda de controle sobre os dados pessoais, e tratamento não-autorizado de dados sensíveis ou dados de pessoas naturais vulneráveis, em especial crianças (o Considerando 75 apresenta uma lista maior de exemplos desses possíveis danos; sua identificação ocorre durante o processo de avaliação). A decisão sobre se uma operação de tratamento envolve um risco e – subsequentemente – se o nível do risco é elevado, é tomada pelo responsável pelo tratamento com base em uma avaliação objetiva (Considerando 76).

      Os riscos que devem ser avaliados no processo de AIPD se relacionam a pessoas naturais, inclusive titulares de dados e a sociedade como um todo, e não a responsáveis pelo tratamento ou subcontratantes. Esses riscos relacionam-se ao gozo de direitos e liberdades por indivíduos e, portanto, eles não são (meramente) riscos de conformidade. Considerado o objetivo do Regulamento, esses riscos têm um âmbito mais amplo do que simplesmente o direito à proteção de dados pessoais e se estendem para outros direitos e liberdades de forma aberta. (O Considerando 4 indica direitos como privacidade, direito a um recurso judicial efetivo, julgamento justo, diversidade linguística, religiosa e cultural, direitos como a liberdade de pensamento, consciência e religião, liberdade de expressão e informação, e liberdade de conduzir um negócio.)

      Riscos a direitos e liberdades são em grande parte avaliados qualitativamente, por meio de avaliação da sua severidade (a magnitude do risco) e probabilidade (viabilidade da ocorrência, e.g. baixa, média ou alta), medidas com referência à "origem", "particularidade" (Considerando 84) e "natureza, âmbito, contexto e finalidades do tratamento" (Considerandos 75-76). Certos riscos à proteção de dados, como riscos de segurança de dados, podem ser avaliados quantitativamente (e.g. calculando sua severidade e probabilidade). A avaliação de riscos

[19] O único dispositivo que traz previsão semelhante na LGPD é o Artigo 38º, Parágrafo único: "Observado o disposto no caput deste artigo, o avaliação deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados".

[20] Finalidade, na LGPD.

[21] Vale destacar que, diferente do contexto normativo brasileiro, na UE a noção de limitação à finalidade ('*purpose limitation*') é o resultado de dois vetores – a finalidade e a adequação – que na LGPD são princípios autônomos (Artigo 6º, I e II).

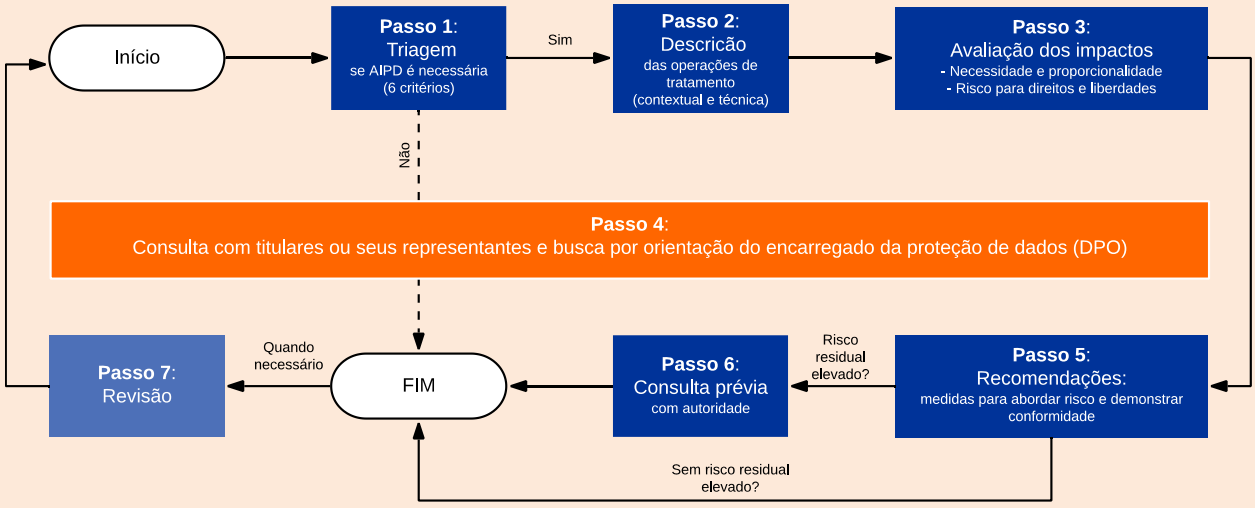
pode ser baseada na avaliação inicial que é utilizada para determinar se o processo de avaliação é necessário (cf. Passo 1).

4) *Envolvimento de stakeholders (inclusive por meio de participação pública)*: O Regulamento prevê, "quando apropriado", consultas com titulares de dados ou seus representantes, com o devido respeito a segredos legítimos (i.e., a "proteção de interesses públicos ou comerciais ou a segurança de operações de tratamento") (Artigo 35º, nº 9). A expressão "quando apropriado" não deve ser entendida como se a consulta fosse 'opcional'. Exceções podem ser abertas se, por exemplo, nenhuma nova ideia puder ser obtida pelo envolvimento de *stakeholders*, ou se o esforço para tal superar os resultados. A decisão de não envolver *stakeholders*, ou de desviar dos resultados de uma consulta, deve ser justificada e documentada. Paralelamente, o encarregado da proteção de dados (*Data Protection Officer*, *DPO*), caso designado e mediante requerimento, deve ser consultado e deve oferecer orientação (Artigos 35º, nº 2 e 39º, nº 1, c); não obstante, o encarregado da proteção de dados não pode conduzir o processo de avaliação.
5) *Recomendações*: O Regulamento exige que o processo de avaliação seja concluído com uma lista de recomendações concebidas para:
   a) abordar os riscos, "incluindo salvaguardas, medidas de segurança e mecanismos para garantir a proteção de dados pessoais" e
   b) garantir conformidade com o Regulamento, "levando em consideração os direitos e os legítimos interesses dos titulares de dados e outras pessoas em causa" (Artigo 35º, nº 7, d).

   O resultado do processo de avaliação "deve ser levado em conta para determinar as medidas apropriadas que serão tomadas a fim de demonstrar que o tratamento de dados pessoais está conforme o Regulamento" (Considerando 64).
6) *Consulta prévia a uma autoridade supervisora*: O Regulamento conecta o processo de AIPD com uma eventual consulta prévia. No caso de um risco residual elevado, isto é, quando o processo de avaliação demonstrar um risco de nível elevado que permanece mesmo após o responsável pelo tratamento implementar as recomendações extraídas do processo de avaliação, o responsável pelo tratamento é obrigado a consultar uma autoridade de controle antes do início do tratamento de dados pessoais e de acordo com um procedimento prescrito (Artigo 36º).
7) *Revisão*: Quando "necessário", "o responsável pelo tratamento procede a um controle para avaliar se o tratamento é realizado em conformidade com a [AIPD], pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam" (Artigo 35º, nº 11). Essa revisão pode ocorrer, portanto, após um certo período de tempo, para finalidade de monitoramento, ou quando houver uma mudança que torne a avaliação anterior obsoleta (parcial ou totalmente). No entanto, o Regulamento não estipula as consequências de tal revisão; dada a possibilidade de mudança do risco, o processo de avaliação pode precisar ser conduzido novamente (em parte ou integralmente).

O método específico para AIPD, proposto acima, oferece as bases para que, posteriormente, seja ajustado para se adequar a um contexto de uso específico, como telecomunicações ou redes elétricas 'inteligentes', ao mesmo tempo em que garante a "proteção de dados pessoais" e demonstra "conformidade com [o] Regulamento" (Artigo 35º, nº 7, d).

**O PROCESSO DE AIPD CONFORME INTERPRETAÇÃO DOS ARTIGOS 35º-36º DO RGPD**




De acordo com esta interpretação, o RGPD não aborda todos os dez passos do método genérico. Alguns passos não necessariamente precisam ser regulados por lei, mas eles emergem de razões pragmáticas durante o processo de avaliação. Particularmente, o Regulamento não aborda o passo do *Âmbito*. (Na prática, o âmbito determinaria, por exemplo, quais aspectos do direito à proteção de dados pessoais são mais prováveis de ser afetados por uma operação de tratamento

prevista e quem seria um titular, ou o representante de um titular, em tal operação de tratamento). Outros passos do método genérico podem, em grande medida, ser interpretados a partir de outros dispositivos do Regulamento. No que se refere ao *Planejamento e à preparação*, o Regulamento estipula apenas que, por exemplo, um único processo de avaliação pode abordar um conjunto de operações de tratamento similares (Considerando 92) ou que um subcontratante pode auxiliar um responsável pelo tratamento na condução do processo de avaliação (Artigo 28º, nº 3, f). Quanto à *Documentação*, um responsável pelo tratamento é, por exemplo, obrigado a demonstrar que suas operações de tratamento são realizadas em conformidade com o Regulamento (Artigo 24º, nº 1)[22]. Sobre o *Controle de qualidade*, por exemplo, um encarregado da proteção de dados (DPO) é incumbido de controlar[23] a realização do processo de avaliação (Artigo 39º, c) e uma autoridade de controle sobre o tratamento de dados é encarregada de realizar auditorias (Artigo 58º, nº 1, b)[24]. Entretanto, em comparação com o método genérico, o RGPD inclui o passo adicional de *Consulta prévia a uma autoridade supervisora*.

## 4 CONSIDERAÇÕES FINAIS

No presente documento de política, o d.pia.lab constrói as bases para dois métodos de avaliação de impacto: primeiro, um método genérico, que reflete a estrutura do seu documento de política anterior e pretende constituir uma base para métodos de avaliação que são, posteriormente, adaptados para áreas e contextos de uso específicos; segundo, um método para AIPD na UE, baseado no método genérico e extraído da interpretação do RGPD.

O processo de AIPD na UE é baseado em uma série de novos conceitos-chave, como o de risco para um direito e – como consequência da abordagem de 'gancho legal' – esse processo é minimamente regulado no texto da lei e requer interpretação e orientação. Assim, o d.pia.lab. buscou extrair um método para AIPD dos Artigos 35º-36º do RGPD, focando em assuntos pouco debatidos ou polêmicos. (Já que a obrigação de conduzir o processo de AIPD está presente em alguns dispositivos legais da UE para além do RGPD, estas observações aplicam-se *mutatis mutandis*.) Não obstante, questões como as técnicas para a avaliação de necessidade, proporcionalidade e riscos para direitos e liberdades de pessoas naturais, bem como o envolvimento de *stakeholders*, incluindo o público em geral, merecem mais atenção profissional e acadêmica e o d.pia.lab pretende retornar a essas questões em futuras contribuições.

Ao mesmo tempo, o método para AIPD interpretado a partir das exigências do RGPD também requer mais estudos, orientações e adaptações. Particularmente, o CEPD, em conjunto com autoridades nacionais e regionais da UE, é o órgão mais bem situado para oferecer tal suporte, com vistas a contribuir para maior segurança jurídica e tornar-se 'centro de referência' sobre esse e outros tipos de avaliação de impacto. Por exemplo, modelos para AIPD, ajustados às circunstâncias de um determinado Estado Membro e um determinado contexto de uso (e.g. indústria ou setor de governança) merecem atenção especial.

---

[22] Na LGPD, esta obrigação está disposta no Artigo 37º: "O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse".
[23] Aqui, 'controlar' tem sentido de 'monitorar', 'inspecionar'.
[24] A LGPD estipula como uma das atribuições da Autoridade Nacional de Proteção de Dados a realização de auditorias. "Artigo 55º – J, Compete à ANPD (...) XVI – auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público".

## FONTES RELEVANTES SELECIONADAS


Arnstein, Sherry R. (1969) "A Ladder of Citizen Participation," Journal of the American Institute of Planners, 35(4), pp. 216–224. doi: 10.1080/01944366908977225.

De Hert Paul, Dariusz Kloza and David Wright (2012) "Recommendations for a Privacy Impact Assessment Framework for the European Union," Brussels – London. https://piafproject.files.wordpress.com/2018/03/piaf_d3_final.pdf.

Gellert, Raphaël (2018) "Understanding the notion of risk in the General Data Protection Regulation", Computer Law & Security Review 34(2), pp. 279–288. doi: 10.1016/j.clsr.2017.12.003.

Kloza, Dariusz, Niels van Dijk, Raphaël Gellert, István Böröcz, Alessia Tanas, Eugenio Mantovani and Paul Quinn (2017) "Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals," d.pia.lab Policy Brief 1/2017, VUB: Brussels. https://cris.vub.be/files/32009890/dpialab_pb2017_1_final.pdf.

van Dijk Niels, Raphaël Gellert and Kjetil Rommetveit (2016) "A risk to a right? Beyond data protection risk assessments", Computer Law & Security Review, 32(2), pp. 286–306. doi: 10.1016/j.clsr.2015.12.017.

Oxford Dictionary of English; https://www.lexico.com/en.


## LEITURAS SUGERIDAS


Grupo de Trabalho do Artigo 29º (2017) *Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679*, WP248 rev. 01, Bruxelas. https://www.cnpd.pt/home/rgpd/docs/wp248rev.01_pt.pdf.

International Organization for Standardization [ISO] (2018), *Risk management – Guidelines*, ISO 31000:2018, Geneva. https://www.iso.org/iso-31000-risk-management.html.

Jasanoff, Sheila (2012) *Science and Public Reason*. London: Routledge. doi: 10.4324/9780203113820.

European Data Protection Supervisor [EDPS] (2017) *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. Brussels. https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

EDPS (2017) *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* [draft]. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.

EDPS (2019) *Accountability on the ground. Part II: Data Protection Impact Assessments & Prior Consultation*. Brussels. https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_ii_en.pdf.

Grunwald, Armin (2018) *Technology Assessment in Practice and Theory*. Abingdon: Routledge. doi: 10.4324/9780429442643.

Mays, Claire (2004) *Stakeholder Involvement Techniques. Short Guide and Annotated Bibliography*. Organisation for Economic Co-operation and Development (OECD), Paris. http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf.

Noble, Bram F. (2015) *Introduction to Environmental Impact Assessment. A Guide to Principles and Practice*. Toronto: OUP Canada.

## SOBRE O D.PIA.LAB

O **Laboratório de Avaliações de Impacto à Privacidade e à Proteção de Dados de Bruxelas**, ou **d.pia.lab**, conecta pesquisa básica, metodológica e aplicada, oferece treinamentos e fornece assessoramento sobre políticas relacionadas a avaliações de impacto nas áreas de inovação e desenvolvimento tecnológico. Apesar de os aspectos jurídicos da privacidade e proteção de dados pessoais constituírem o nosso foco principal, o Laboratório inclui outras disciplinas como ética, filosofia, estudos sobre vigilância e estudos na área de ciências, tecnologia e sociedade. Criado em novembro de 2015, o Laboratório constitui parte, e se baseia na experiência, do Grupo de Pesquisa em Direito, Ciência, Tecnologia e Sociedade (LSTS) da Vrije Universiteit Brussel (VUB; Universidade Livre de Bruxelas), Bélgica.

O Laboratório desenvolveu seu conhecimento baseado em avaliações de impacto provenientes de múltiplos projetos, concluídos e em andamento, como PERSONA, HR-RECYCLER e SYSTEM (co-financiados pela UE), e PARENT (co-financiado pela UE e Innoviris). A visão expressa neste documento de política não reflete as visões de nenhuma destas agências de financiamento.

Nós agradecemos – em ordem alfabética – Alexandra Aslanidou, Jonas Breuer, Alessandra Calvi, Roger Clarke, Katerina Demetzou, Catherine Jasserand-Breeman, Anna Johnston, Gianclaudio Malgieri, Anna Mościbroda, Kjetil Rommetveit, Julien Rossi, Juraj Sajfert, Laurens Vandercruysse, Heidi Waem, Ine van Zeeland e um revisor anônimo pelo seu feedback sobre uma versão anterior do presente documento de política.

**dpialab.org** | **dpialab@vub.ac.be**

## SOBRE O DATA PRIVACY BRASIL (ENTIDADE PARCEIRA DA TRADUÇÃO)

O **Data Privacy Brasil** é um centro de produção e difusão de conhecimento que tem como objetivo criar, analisar e compartilhar conteúdo sobre o impacto das tecnologias da informação e comunicação (TICs) sobre a privacidade e proteção de dados pessoais, a fim de subsidiar o debate público sobre os desafios de uma sociedade e economia cada vez mais movida e orientada por dados. Para concretizar esses fins, atualmente o Data Privacy (i) oferece cursos e *workshops* sobre aspectos teóricos e práticos relativos à privacidade e proteção de dados, com especial foco na Lei Geral brasileira de Proteção de Dados (LGPD) e sua relação com normativas diversas vigentes no ordenamento jurídico brasileiro e em outras jurisdições (e.g. Regulamento Europeu de Proteção de Dados Pessoais); (ii) promove palestras, reuniões, seminários e outros eventos a fim de reunir especialistas em privacidade e proteção de dados (e temas correlatos) e suscitar avanços no debate sobre o assunto no Brasil, além de propiciar sua difusão para um público mais amplo; (iii) reúne, produz e contribui com a produção de pesquisa aplicada e conteúdo diverso, como ensaios, análises, estudos e artigos científicos.

**dataprivacy.com.br** | **contato@dataprivacy.com.br**