VI CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (VI CIDIA)

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES I

P961
Privacidade, proteção de dados pessoais e negócios inovadores II [Recurso eletrônico on-line] organização VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Alexandre Schmitt da Silva Mello, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato – Belo Horizonte: Skema Business School, 2025.

Inclui bibliografia
ISBN: 978-65-5274-361-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Perspectivas globais para a regulação da inteligência artificial.
1. GDPR. 2. Segurança da informação. 3. Compliance. I. VI Congresso Internacional de Direito e Inteligência Artificial (1:2025 : Belo Horizonte, MG).

CDU: 34

VI CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (VI CIDIA)

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES I

Apresentação

A SKEMA Business School é uma organização francesa sem fins lucrativos, com presença em sete países diferentes ao redor do mundo (França, EUA, China, Brasil, Emirados Árabes Unidos, África do Sul e Canadá) e detentora de três prestigiadas acreditações internacionais (AMBA, EQUIS e AACSB), refletindo seu compromisso com a pesquisa de alta qualidade na economia do conhecimento. A SKEMA reconhece que, em um mundo cada vez mais digital, é essencial adotar uma abordagem transdisciplinar.

Cumprindo esse propósito, o VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA), realizado nos dias 18 e 19 de setembro de 2025, em formato híbrido, manteve-se como o principal evento acadêmico sediado no Brasil com o propósito de fomentar ricas discussões sobre as diversas interseções entre o direito e a inteligência artificial. O evento, que teve como tema central a "Regulação da Inteligência Artificial", contou com a presença de renomados especialistas nacionais e internacionais, que abordaram temas de relevância crescente no cenário jurídico contemporâneo.

Profissionais e estudantes dos cursos de Direito, Administração, Economia, Ciência de Dados, Ciência da Computação, entre outros, tiveram a oportunidade de se conectar e compartilhar conhecimentos, promovendo um ambiente de rica troca intelectual. O VI CIDIA contou com a participação de acadêmicos e profissionais provenientes de diversas regiões do Brasil e do exterior. Entre os estados brasileiros representados, estavam: Alagoas (AL), Bahia (BA), Ceará (CE), Goiás (GO), Maranhão (MA), Mato Grosso do Sul (MS), Minas Gerais

Foram discutidos assuntos variados, desde a própria regulação da inteligência artificial, eixo central do evento, até as novas perspectivas de negócios e inovação, destacando como os algoritmos estão remodelando setores tradicionais e impulsionando a criação de empresas inovadoras. Com uma programação abrangente, o congresso proporcionou um espaço vital para discutir os desafios e oportunidades que emergem com o desenvolvimento algorítmico, reforçando a importância de uma abordagem jurídica e ética robusta nesse contexto em constante evolução.

A programação teve início às 13h, com o check-in dos participantes e o aquecimento do público presente. Às 13h30, a abertura oficial foi conduzida pela Prof.ª Dr.ª Geneviève Poulingue, que, em sua fala de boas-vindas, destacou a relevância do congresso para a agenda global de inovação e o papel da SKEMA Brasil como ponte entre a academia e o setor produtivo.

Em seguida, às 14h, ocorreu um dos momentos mais aguardados: a Keynote Lecture do Prof. Dr. Ryan Calo, renomado especialista internacional em direito e tecnologia e professor da University of Washington. Em uma conferência instigante, o professor explorou os desafios metodológicos da regulação da inteligência artificial, trazendo exemplos de sua atuação junto ao Senado dos Estados Unidos e ao Bundestag alemão.

A palestra foi seguida por uma sessão de comentários e análise crítica conduzida pelo Prof. Dr. José Luiz de Moura Faleiros Júnior, que contextualizou as reflexões de Calo para a realidade brasileira e fomentou o debate com o público. O primeiro dia foi encerrado às 14h50 com as considerações finais, deixando os participantes inspirados para as discussões do dia seguinte.

As atividades do segundo dia tiveram início cedo, com o check-in às 7h30. Às 8h20, a Prof.ª Dr.ª Margherita Pagani abriu a programação matinal com a conferência Unlocking Business Creativity Using Artificial Intelligence, apresentando insights sobre como a IA pode

Após um breve e merecido coffee break às 9h40, os participantes retornaram para uma manhã de intensas reflexões. Às 10h30, o pesquisador Prof. Dr. Steve Ataky apresentou a conferência Regulatory Perspectives on AI, compartilhando avanços e desafios no campo da regulação técnica e ética da inteligência artificial a partir de uma perspectiva global.

Encerrando o ciclo de palestras, às 11h10, o Prof. Dr. Filipe Medon trouxe ao público uma análise profunda sobre o cenário brasileiro, com a palestra AI Regulation in Brazil. Sua exposição percorreu desde a criação do Marco Legal da Inteligência Artificial até os desafios atuais para sua implementação, envolvendo aspectos legislativos, econômicos e sociais.

Nas tardes dos dois dias, foram realizados grupos de trabalho que contaram com a apresentação de cerca de 60 trabalhos acadêmicos relacionados à temática do evento. Com isso, o evento foi encerrado, após intensas discussões e troca de ideias que estabeleceram um panorama abrangente das tendências e desafios da inteligência artificial em nível global.

Os GTs tiveram os seguintes eixos de discussão, sob coordenação de renomados especialistas nos respectivos campos de pesquisa:

a) Startups e Empreendedorismo de Base Tecnológica – Coordenado por Allan Fuezi de Moura Barbosa, Laurence Duarte Araújo Pereira, Cildo Giolo Júnior, Maria Cláudia Viana Hissa Dias do Vale Gangana e Yago Oliveira

b) Jurimetria Cibernética Jurídica e Ciência de Dados – Coordenado por Arthur Salles de Paula Moreira, Gabriel Ribeiro de Lima, Isabela Campos Vidigal Martins, João Victor Doreto e Tales Calaza

c) Decisões Automatizadas e Gestão Empresarial / Algoritmos, Modelos de Linguagem e Propriedade Intelectual – Coordenado por Alisson Jose Maia Melo, Guilherme Mucelin e

f) Regulação da Inteligência Artificial – III – Coordenado por Ana Júlia Silva Alves Guimarães, Erick Hitoshi Guimarães Makiya, Jessica Fernandes Rocha, João Alexandre Silva Alves Guimarães e Luiz Felipe Vieira de Siqueira

g) Inteligência Artificial, Mercados Globais e Contratos – Coordenado por Gustavo da Silva Melo, Rodrigo Gugliara e Vitor Ottoboni Pavan

h) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – I – Coordenado por Dineia Anziliero Dal Pizzol, Evaldo Osorio Hackmann, Gabriel Fraga Hamester, Guilherme Mucelin e Guilherme Spillari Costa

i) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – II – Coordenado por Alexandre Schmitt da Silva Mello, Lorenzzo Antonini Itabaiana, Marcelo Fonseca Santos, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato

j) Empresa, Tecnologia e Sustentabilidade – Coordenado por Marcia Andrea Bühring, Ana Cláudia Redecker, Jessica Mello Tahim e Maraluce Maria Custódio.

Cada GT proporcionou um espaço de diálogo e troca de experiências entre pesquisadores e profissionais, contribuindo para o avanço das discussões sobre a aplicação da inteligência artificial no direito e em outros campos relacionados.

Um sucesso desse porte não seria possível sem o apoio institucional do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, que desde a primeira edição do evento provê uma parceria sólida e indispensável ao seu sucesso. A colaboração contínua do CONPEDI tem sido fundamental para a organização e realização deste congresso, assegurando a qualidade e a relevância dos debates promovidos.

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Ms. Dorival Guimarães Pereira Júnior

Coordenador do Curso de Direito – SKEMA Law School

Prof. Dr. José Luiz de Moura Faleiros Júnior

Coordenador de Pesquisa – SKEMA Law School

IDENTIFICAÇÃO E AVALIAÇÃO DOS CRITÉRIOS DE ELEGIBILIDADE PARA ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

IDENTIFICATION AND ASSESSMENT OF ELIGIBILITY CRITERIA FOR PREPARING THE PERSONAL DATA PROTECTION IMPACT ASSESSMENT (RIPD)

Rainier Garacis

Resumo

O presente trabalho tem como objetivo analisar os critérios que tornam um tratamento de dados pessoais passível de requerer a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e sua relevância para a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). O RIPD é um instrumento essencial para a avaliação de riscos no tratamento de dados pessoais, permitindo que organizações identifiquem, mensurem e mitiguem potenciais impactos à privacidade e segurança dos titulares de dados.

Palavras-chave: Lei geral de proteção de dados pessoais (lgpd), Relatório de impacto à proteção de dados (ripd), Alto risco

Abstract/Resumen/Résumé

This study aims to analyze the criteria that determine whether personal data processing requires the preparation of a Data Protection Impact Assessment (DPIA) and its relevance for compliance with the Brazilian General Data Protection Law (LGPD). The DPIA is an essential tool for assessing risks in personal data processing, enabling organizations to identify, measure, and mitigate potential impacts on privacy and security.

Keywords/Palabras-claves/Mots-clés: General data protection law (lgpd), Data protection impact assessment (ripd), High risk

Introdução

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é uma ferramenta essencial no contexto da Lei Geral de Proteção de Dados (LGPD). Estabelecido pelo artigo 5º da LGPD, o RIPD se define como uma documentação detalhada dos processos de tratamento de dados que possam gerar riscos às liberdades civis e aos direitos fundamentais dos indivíduos. Este relatório não apenas descreve esses processos, mas também propõe medidas, salvaguardas e mecanismos de mitigação de risco apropriados ao caso concreto. A importância do RIPD se reflete em sua obrigatoriedade para os controladores de dados pessoais, destacando-se como um componente importante na governança de dados pessoais e na gestão de riscos associados ao seu tratamento, reforçando a confiança dos titulares de dados em relação ao manejo de suas informações pessoais. (GOMES, 2019)

Apesar da clareza conceitual oferecida pela LGPD, a implementação prática do RIPD apresenta diversos desafios. Entre eles, destaca-se a identificação correta e coerente dos critérios de elegibilidade para a elaboração do relatório. Estes critérios são cruciais para assegurar que os tratamentos de dados pessoais que envolvem alto risco estejam devidamente documentados e tenha seus riscos identificados e mitigados de maneira adequada. A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel fundamental na definição desses critérios, conforme descrito no artigo 55-J da LGPD. No entanto, a subjetividade e a falta de regulamentação detalhada têm gerado incertezas entre os controladores de dados sobre quando e como elaborar o RIPD. (GOMES, 2020)

Ainda, a implementação do RIPD exige uma adaptação constante por parte dos controladores de dados, principalmente diante de um cenário novo e não regulamentado.Com isso, o papel da ANPD na persecução da definição de parâmetros claros sobre quando e como o RIPD deve ser elaborado é crucial para minimizar as incertezas que ainda existem no cenário atual. Além disso, a capacitação das empresas e a promoção de uma cultura organizacional que valorize a proteção de dados pessoais são fundamentais para garantir que os RIPDs não sejam vistos apenas como um requisito legal, mas como uma ferramenta estratégica de governança e gestão de riscos. A abordagem europeia, por sua vez, serve de parâmetro para o tema no Brasil, apontando a necessidade de um amadurecimento na regulamentação nacional, para que os controladores de dados possam cumprir de forma mais clara e eficiente suas obrigações, garantindo a proteção dos direitos dos titulares de dados.

Além disso, este artigo explora os desafios práticos enfrentados pelos controladores de dados na identificação dos critérios de elegibilidade para o RIPD, baseando-se em orientações atuais, como a Resolução nº 2 e a consulta pública do Guia Orientativo Tratamentos de Alto Risco, ambos documentos criados pela ANPD. Além disso, compara-se a abordagem brasileira com a europeia, destacando semelhanças e diferenças na regulamentação e na prática. Ao abordar essas questões, o artigo busca oferecer uma visão abrangente sobre as complexidades envolvidas na implementação do RIPD e as possíveis soluções para superar os desafios práticos que surgem no contexto da proteção de dados pessoais.

1. O que é Relatório de Impacto à Proteção de Dados Pessoais (RIPD)?

O conceito de Relatório de Impacto à Proteção de Dados Pessoais foi estabelecido na própria LGPD por meio do art. 5º, definindo-o como uma documentação do controlador de dados pessoais 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 (GOMES, 2020). Embora o conceito seja, relativamente, simples, o RIPD, por outro lado, apresenta atualmente inúmeras complexidades, tais como, quais os elementos necessários que devem compor, critérios de elegibilidade, publicidade do relatório, momento de elaboração, etc. (BRASIL, 2018)

Ainda, a LGPD em seu art. 38, define que, uma das medidas de governança de risco obrigatórias que os controladores de dados pessoais devem adotar é a criação de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD):

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório 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.

Este relatório deve ser composto com a (I) descrição dos processos de tratamento de

dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados envolvidos no respectivo tratamento, bem como (II) medidas, salvaguardas e mecanismos de mitigação dos riscos identificados ao longo da elaboração desse relatório. Por meio dele é possível demonstrar quais são os riscos existentes para os titulares dentro do contexto do processo analisado e quais foram as salvaguardas executadas pelo controlador para sua mitigação, preferencialmente, antes da realização do tratamento envolvendo dados pessoais, conforme dispõem a própria Autoridade Nacional de Proteção de Dados (ANPD), justamente para que se possa avaliar, de antemão, os possíveis riscos associados a esse tratamento (Privacy by Design). (LOHMANN, 2021)

Dessa forma, o controlador conseguirá, antes mesmo de usar os dados pessoais para aquela finalidade, identificar a probabilidade de ocorrência de cada fator de risco e o seu impacto sobre as liberdades e direitos fundamentais dos titulares e adotar as medidas, as salvaguardas e os mecanismos de mitigação de risco apropriados à hipótese ou, em última instância, não sequenciar com o tratamento. (ANPD, 2023)

É importante frisar que o risco associado ao relatório de impacto deve observar os direitos e liberdades do titular de dados pessoais como prisma fundamental da análise e não o risco de negócio ou conformidade em relação a tomada de decisão sobre o tratamento de dados. Conforme apresenta Maria Cecília Oliveira Gomes:

> "(...) este tipo de risco (de negócio), erroneamente associado ao relatório, é um risco muito mais focado em um aspecto de conformidade regulatória "*compliance risk*", do que em um risco associado aos direitos. Nesse sentido, vale reforçar essa diferença, uma vez que aparentemente muitos tem confundido o risco no processo de adequação com o risco indicado no relatório de impacto." (GOMES, 2020)

2. Critérios de elegibilidade de tratamento que necessitam do RIPD

Dada a importância da existência do RIPD trazida anteriormente, é necessário que os controladores identifiquem de forma correta e coerente, quais são os tratamentos cabíveis de realização do relatório. Visto que, embora a existência dele não garanta a plena conformidade ou mitigação total dos riscos inerentes aos tratamentos, ele é um dos principais mecanismos da LGPD para assegurar um nível de risco aceitável no tratamento de dados pessoais, tornando-

se elemento fundamental para demonstrar a conformidade, boa-fé e preocupação dos controladores com os dados dos titulares tratados.

Para identificação desses critérios, é necessário observar, primordialmente, o art. 55-J da LGPD que traz uma das competências da ANPD, consistindo na edição de regulamentos e guias acerca do RIPD, incluindo, mas não se limitando, quais os critérios necessários a serem observados pelos controladores de dados pessoais para a criação do relatório.

> Art. 55-J. Compete à ANPD: (...)
> XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei.

Observa-se por meio desse inciso a presença do elemento chave que será utilizado para identificar os critérios de elegibilidade: o alto risco à garantia dos princípios gerais de proteção de dados pessoais. É por meio desse conceito que a ANPD busca propor quais os critérios que compreendem serem centrais àqueles tratamentos tidos como alto risco. Critérios esses que serão apresentados e tratados ao longo desse artigo. (LOHMANN, 2021)

Além da premissa apresentada no art. 55-J da LGPD, o texto legal ainda exibe dois outros possíveis critérios que podem ensejar na necessidade de sequenciar com o procedimento de elaboração do RIPD. Embora pouco explorados na LGPD e pendentes de uma ação ativa da própria autoridade nacional. São esses os casos dos arts. 10º, §3º e art. 38 da LGPD, onde há a indicação que a ANPD poderá (não sendo uma regra) solicitar aos controladores a elaboração do RIPD para, respectivamente, alguns casos em que o tratamento tenha como hipótese legal o legítimo interesse e tratamentos que utilizam dados pessoais sensíveis1.

Embora os textos dos dispositivos sejam claros e diretos, ou seja, caso tenha como base legal o legítimo interesse ou trate dados pessoais sensíveis deve-se elaborar RIPD, o legislador optou por não tratar esses critérios como absolutos ou objetivos e, nem sequer, tratou-os como critérios obrigatórios, podendo ser uma necessidade a depender do pedido do regulador ao controlador. (DOZZA, 2023) Sendo necessário aguardar regulamentação específica sobre o

[1] Dado pessoal sensível é, com base no art. 5º, II da LGPD, dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

tema advinda da autoridade nacional, conforme reforçado pela Maria Cecília Oliveira Gomes:

> "A LGPD não previu expressamente em quais situações o relatório de impacto seria obrigatório, o que a LGPD indica é em quais situações a ANPD, dentro de suas competências, pode ou deve solicitar o relatório de impacto a um Controlador de maneira ampla ou em contextos específicos de tratamento. Assim como, a LGPD não indicou o que é uma operação de tratamento de alto risco, apenas indicou que compete à ANPD elaborar diretrizes sobre o assunto."

Como consequência dessa indefinição objetiva trazida pelo legislador, Matheus Sturari ressalta, a título exemplificativo, as inúmeras inseguranças apresentadas pelos agentes de tratamentos na prática:

> Constata-se, por dedução da definição do art. 5º, XVII, que o DPIA[2] será exigido para atividades de tratamento que gerem riscos às liberdades civis e direitos fundamentais. Entretanto, são várias as dúvidas que permanecem, por exemplo: (i) toda hipótese de tratamento fundamentado em legítimo interesse deve ser acompanhada de um DPIA?; (ii) quais são os tratamentos que serão considerados como geradores de riscos a ponto de demandarem um DPIA?; (iii) a despeito de uma lista, quais critérios devem ser considerados para analisar a existência de risco e considerar a necessidade de um DPIA?; (iv) todo e qualquer risco deve ensejar um DPIA ou apenas "alto" risco, como no inciso XIII do art. 55-J?
> (...) Acontece que, a existência de tais dúvidas e de um cenário de incertezas envolvendo o tema, tem gerado um efeito que, a meu ver, pode não ser positivo: a possível banalização do DPIA e consequente excessiva oneração dos agentes de tratamento.". (STURARI, 2020)

Nesse sentido pode-se observar concordância do Felipe Fontes Cabral acerca dessa ausência de critérios objetivos:

> "(...) há o risco de que o RIPD se torne um instrumento de controle em casos isolados ou, pior, que seja um documento elaborado para fins formais, porém sem guiar uma atividade real de gerenciamento de riscos, o que pode comprometer a eficácia do sistema de proteção aos dados pessoais no Brasil." (CABRAL, 2019)

Ainda, importante mencionar que a ANPD, ao estabelecer os critérios em futura

[2] DPIA é a sigla traduzida para o inglês do RIPD.

regulamentação, deve possuir cautela e garantir proporcionalidade entre a necessidade formal do RIPD e o real objetivo do relatório. Uma vez que, caso "erre a mão", poderá onerar excessivamente os controladores e operadores com uma possível obrigação legal meramente formal, sem qualquer importância prática para controle de riscos de privacidade, o que vai na contramão da sistemática preventiva trazida pela LGPD. (GRASSO, 2021)

2.1 Resolução nº2/ANPD e Guia de Alto Risco

Com base nas premissas informadas no capítulo anterior, a ANPD até o momento, não elegeu os critérios de elaboração do RIPD. Todavia, por meio de consulta pública a sociedade acerca do novo Guia Orientativo Tratamentos de Alto Risco para, mas não somente, Agentes Tratamento de Pequeno Porte (ATPP) apresentou proposta de quais critérios poderão ser considerados relevantes para essa identificação.

Embora a Resolução nº 2 da ANPD de 2022 não possua, à primeira vista, correlação direta com o tema do RIPD, uma vez que trata sobre a definição e parâmetros de Agentes de Tratamentos de Pequeno Porte (ATPP), é por meio desse dispositivo que o regulador decidiu apresentar o que seria considerado tratamentos de alto risco e qual a metodologia de avaliação dos critérios de elegibilidade.

A metodologia em questão indica que o controlador de dados pessoais deverá avaliar a existência, no tratamento de dados pessoais, de, pelo menos, um critério geral cumulado com um critério específico, conforme estabelecido no art. 4º da referida Resolução.

> Art. 4º Para fins deste regulamento, (...) será considerado de alto risco o tratamento de dados pessoais que atender cumulativamente a pelo menos um critério geral e um critério específico, dentre os a seguir indicados:
> I - critérios gerais:
> a) tratamento de dados pessoais em larga escala; ou
> b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;
> II - critérios específicos:
> a) uso de tecnologias emergentes ou inovadoras;
> b) vigilância ou controle de zonas acessíveis ao público;
> c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os

> aspectos da personalidade do titular; ou
> d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos. (ANPD, 2022)

Com isso, ainda que a metodologia de cálculo de alto risco tenha sido originada para atender uma resolução sem envolvimento direto com o tema central tratado nesse artigo, é por meio da consulta pública do Guia Orientativo Tratamentos de Alto Risco que a ANPD confirma a recomendação de utilizar esses critérios e metodologia para eleger quais tratamentos deverão possuir RIPD enquanto não houver a existência de resolução específica para o tema[3]. Inclusive, antes da consulta pública do guia, a ANPD, por meio do FAQ sobre RIPD, já havia recomendado aos controladores utilizarem os mesmos critérios dispostos para identificação de tratamentos de alto risco da Resolução nº 2 da ANPD de 2022 (ANPD, 2023). Porém, até aquele momento, não havia clareza sobre como avaliar na prática os elementos dos critérios dispostos no art 4º dessa resolução e nem mesmo existia documentação criada pelo Órgão Regulador que formalizasse essa recomendação.

Mesmo que o guia de alto risco seja o documento elaborado pela ANPD mais próximo daquilo que seria recomendável levar em consideração, deve-se recordar que o próprio regulador indica que esses critérios e metodologia não substituirá nova regulamentação específica sobre o tema ou sequer esgotará a aplicabilidade frente aos casos práticos. Cabendo aos controladores o dever de identificar a necessidade de sequenciar o RIPD mesmo que o tratamento não possua a presença dos critérios mencionados[4].

2.1.1 Adentrando os Critérios de Alto Risco

Ante ao exposto, o guia em questão tem como objetivo principal trazer maiores detalhes acerca de como identificar, por exemplo, se determinado tratamento possui a presença

[3] O item 5 da Resolução nº 11 da ANPD de 2023 indica que o tema de RIPD está sendo tratado pela autoridade com previsão de nova regulamentação para o biênio de 2023-2024. Não tendo o tema esgotado com o guia de alto risco e larga escala.

[4] "Ressalte-se que, para fins de elaboração do RIPD, esses critérios não devem ser considerados exaustivos, de modo que o controlador poderá verificar a existência de alto risco em situações diferentes das indicadas. Assim, em conformidade com o princípio da responsabilização e prestação de contas, cabe ao controlador avaliar as circunstâncias relevantes do caso concreto, a fim de identificar os riscos envolvidos e as medidas de prevenção e segurança apropriadas, considerando os possíveis impactos às liberdades e direitos fundamentais dos titulares e a probabilidade de sua ocorrência" (ANPD, 2023).

dos critérios gerais de elegibilidade do RIPD, ou seja, se possui elementos de larga escala ou que afete significativamente os direitos e liberdades dos titulares.

Em relação a esses critérios, cabe mencionar que a análise de larga escala observará apenas elementos quantitativos dos tratamentos, por sua vez, o critério que possibilita avaliar os impactos significantes aos titulares observará apenas elementos qualitativos, referindo-se à magnitude dos impactos que a atividade de tratamento de dados pessoais poderá representar sobre interesses e direitos fundamentais dos titulares dos dados pessoais. Com isso, exige-se uma avaliação detalhada e fundamentada sobre as suas possíveis consequências negativas, isto é, os possíveis impactos que podem ser gerados pelo tratamento dos dados dos titulares. (ANPD, 2024)

A ANPD estabeleceu ainda que, para avaliação do critério de larga escala, é necessário aplicação de uma formula matemática que considerará os seguintes elementos: quantidades de titulares afetados pelo tratamento, volume médio de dados tratados (para identificar o volume médio de dados tratado o controlador deverá dividir a quantidade de titulares envolvidos no tratamento com o total de registro de dados tratados), frequência (quantidade de vezes que o tratamento é realizado ao longo do tempo), duração (extensão de tempo em que o tratamento perdura até a eliminação dos dados pessoais) e extensão geográfica (identificação da abrangência e alcance da operação de tratamento). Essa formula matemática atrela pesos diferentes para cada um desses elementos, afetando o resultado final a depender do caso concreto. Importante mencionar que a quantidade de titulares afetados é o elemento principal da formula, possuindo, consideravelmente, maior peso na identificação da larga escala em relação aos outros. (ANPD, 2024)

A fórmula, por si só, não apresenta grande complexidade de desenvolvimento: com base na identificação dos elementos do caso prático, cada um deles possuirão pesos específicos (apresentados por meio da tabela de valores presente no guia) que serão somados ao final da análise do controlador e, caso a somatório dos pesos resulte em um valor maior que vinte e cinco (25), o tratamento avaliado deve ser classificado como larga escala5.

Já em relação ao critério geral qualitativo de alto risco: afetar significativamente

[5] A ANPD estabeleceu que os casos de tratamentos de dados pessoais que envolva mais de dois milhões de titulares já são considerados de alto risco, ou seja, já atingirão o valor objetivo do alto risco (vinte e cinco). Sendo necessário a avaliação dos demais elementos de larga escala (frequência, duração, extensão geográfica e volume médio de dados) apenas nos casos em que o volume de titulares envolvidos no tratamento for inferior a dois milhões.

direitos e liberdades fundamentais, ele deverá ser avaliado de forma subjetiva pelo controlador com base nos seguintes elementos: possibilidade da operação de tratamento causar dano moral ou material, impedir exercício de direitos fundamentais ou impedir a utilização de serviços essenciais.

O conceito chave que deve ser utilizado para avaliação dos critérios indicados acima é a identificação de gravidade e probabilidade de um impacto ilegítimo e desarrazoado ocorrer sobre os interesses e direitos dos titulares envolvidos no tratamento. Eventuais impactos limitados, proporcionais ou necessários para o atendimento de fins legítimos ou para o exercício de direitos não devem ser levados em consideração para classificado do tratamento nesse critério. Inclusive, em relação aqueles tratamentos que podem causar dano moral ou material, a ANPD apresenta alguns exemplos práticos do que pode ser considerado para avaliação da existência desse elemento no tratamento em questão, sendo eles: possibilidade de causar discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade. (ANPD, 2024)

Tratando-se dos critérios específicos, embora sejam significativamente mais objetivos do que a análise dos critérios gerais apresentados anteriormente, ainda assim paira certo grau de subjetividade que deverá ser endereçada pelos controladores de forma justificada, sendo o caso do critério de tecnologias emergentes ou inovadoras, por exemplo.

2.2 Comparação dos critérios recomendados no Brasil e aqueles estabelecidos na Europa

A base construída na LGPD foi inspirada na legislação europeia, com algumas adequações para o cenário do Brasil. Essa inspiração trouxe diversas obrigações e instrumentos presentes também na GDPR (regulamento europeu de proteção de dados pessoais). É o caso do RIPD ser equivalente ao *Data Protection Impact Assessmesnt* (DPIA) europeu. (GRASSO, 2021)

O Relatório de Impacto à Proteção de Dados pessoais, embora seja um tema recente no Brasil, na Europa já possui um cenário mais robusto e maduro. Dessa forma, nesse subcapítulo, o objetivo central será explorar alguns dos critérios estabelecidos na Europa frente aos que temos atualmente no Brasil, trazendo a perspectiva europeia do tratamento "suscetível de implicar um elevado risco para os direitos e liberdades do titular dos dados".

No cenário europeu, assim como no Brasil, a legislação local não detalhou quais seriam os critérios para que os agentes de tratamento tenham noções claras de quais tratamentos poderiam gerar alto risco aos titulares e, por consequência, devessem realizar o Relatório de Impacto à Proteção de Dados. Motivo esse que, antes mesmo da publicação da GDPR, o extinto Grupo de Trabalho do Artigo 29 (WP29)6 elaborou um dos *guidelines* mais antigos e relevantes sobre o tema. Trata-se do documento "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" elaborado em 2017 e endossado pelo atual Comitê Europeu de Proteção de Dados (EDPB, 2018).

Diferente do Brasil que possui apenas um regulador (ANPD), o cenário Europeu é formado por inúmeros países e, por óbvio, reguladores diferentes entre eles. Dessa forma, o *guideline* em questão apresenta racional amplo e comum para que os países membros do bloco europeu tenham, minimamente, critérios semelhantes e basilares para avaliação do alto risco, podendo serem detalhados conforme entendimento dos inúmeros Reguladores existentes e realidades dos países.

Ao compararmos ambos os guias elaborados para o alto risco, podemos identificar inúmeras correlações entre os critérios e racionais adotados para análise dos tratamentos. O primeiro que pode ser identificado é a indicação de que, embora os critérios de ambos os guias sejam um norte amplo para as análises dos agentes de tratamentos, são apenas exemplos e não se esgotam, em outras palavras, podem existir outros tratamentos, inclusive que não possua nenhum dos critérios de elegibilidade e que mesmo assim será necessário a elaboração do relatório pelos controladores. Existindo a necessidade dos controladores avaliarem cada caso concreto com cautela e, se identificado a pertinência de elaborar o relatório, execute-o.

Outros aspectos de semelhança, é em relação aos próprios critérios de elegibilidade, embora a metodologia de avaliação seja diferente.

Ao observar os critérios europeus, pode-se identificar que seis (6) dos nove (9) critérios presentes no *guideline* possuem relevante sinergia aos recomendados pela ANPD, inclusive pelo racional que deverá ser levado em consideração para avaliação deles, sendo eles: impedir

[6] O Grupo de Trabalho do Artigo 29 foi um Órgão Consultivo instituído pelo artigo 29º da Diretiva 95/46/CE, composto por um representante da autoridade de proteção de dados de cada Estado-Membro da União Europeia até 25 de maio de 2018, sendo substituído pelo atual EDPB (*European Data Protection Board*).

os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato, utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais, dados relativos a titulares de dados vulneráveis, dados tratados em larga escala (com exceção da ausência de análise do elemento de frequência, todos os demais estão presentes na identificação do critério de larga escala), dados sensíveis e controle sistemático, mas não apenas de zonas acessíveis ao público.

Já acerca dos critérios que não possuem correlação direta, são eles: avaliação ou classificação (elaboração de perfis e previsão dos titulares), decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar (embora o critérios de afetar significativamente os titulares seja uma premissa presente nos critérios nacionais, o cenário europeu delimita essa premissa para aquelas decisões que são tomadas automaticamente) e estabelecer conjunto ou combinação de dados coletados para finalidades distinta da qual se almeja realizar a operação de tratamento. (WP29, 2017)

Sobre a metodologia de avaliação, no cenário europeu não existe a subdivisão dos critérios gerais e específicos, todos possuem o mesmo peso e deverão ser avaliados de forma apartada, cabendo a realização do DPIA caso o mesmo tratamento possua mais de dois critérios de elegibilidade, sejam eles quais forem. Quanto maior a quantidade de critérios presentes no tratamento, maior a probabilidade de ser necessário realizar o RIPD.

Já no Brasil, pelo guia de alto risco, o tratamento poderá, em tese, conforme metodologia de análise, ter todos os critérios específicos presentes e mesmo assim não ter a obrigatoriedade de realizar o RIPD. Tendo em vista que os critérios gerais são os principais elementos para eleger um tratamento como alto risco (larga escala ou alta probabilidade e gravidade de afetar significativamente os direitos e liberdades dos titulares).

3. Desafios práticos da identificação dos critérios recomendados pela ANPD

A identificação dos critérios de elegibilidade no Brasil apresenta desafios significativos devido à falta de regulamentação detalhada e à natureza subjetiva de alguns dos critérios estabelecidos pela LGPD, conforme apresentado ao longo desse artigo.

Com isso, uma das dificuldades que os controladores poderão enfrentar na prática é em relação ao critério de larga escala. Embora a fórmula ofereça uma estrutura objetiva, a aplicação

dos elementos quantitativos e a atribuição de pesos podem gerar dúvidas e dificuldades, especialmente em contextos que não se encaixam perfeitamente nos parâmetros estabelecidos. Essa dificuldade relaciona-se com a maturidade do controlador em relação a clareza e detalhamento do mapeamento dos seus processos e bases de dados, incluindo a ausência de ferramentas aptas para mapear dados não estruturados. Nesse cenário, atividades simples, como atendimento ao cliente (SAC/Ouvidoria), poderão apresentar complexidades em levantar, de forma precisa, as informações necessárias para avaliar esse critério. Questionamentos como: "Qual a quantidades de dados pessoais tratados, inclusive, por e-mail?" ou "Qual a extensão geográfica dos titulares (aumentando a complexidade caso a informação de localização não seja coletada no atendimento aos titulares)?" podem ser levantados por esses agentes de tratamento caso não possuam processos maduros e/ou ferramentas de mapeamento de dados pessoais[7] que auxiliarão na identificação precisa daqueles dados estruturados e, principalmente, não estruturados[8].

Ainda em relação aos critérios gerais, avaliar se o tratamento pode afetar significativamente os titulares dos dados pessoais, por si só, trata-se de um procedimento que pairam inúmeras dúvidas acerca do racional que os controladores deverão desenvolver para chegar em uma conclusão. Inclusive, o Guia Orientativo de Alto Risco, até o momento, não apresenta, demonstra ou desenvolve uma linha racional clara para guiar as análises dos elementos que definem esse critério, meramente, apresentam alguns poucos exemplos. Com isso, um dos possíveis controles para demonstrar a boa-fé e responsabilidade dos controladores é desenvolver procedimentos de governança para que as análises qualitativas do tratamento sejam registradas e façam parte do registro dos tratamentos de dados pessoais, possibilitando apresentar, de forma fundamentada, quais foram os pontos argumentativos que concluíram a

[7] "O processo de mapeamento dos dados pessoais é fundamental para apoiar o processo de gestão de riscos de privacidade e de segurança da informação. Ele envolve tanto a identificação dos dados dos clientes, dos fornecedores quanto dos colaboradores. O mapeamento visa prover as informações iniciais para que a organização possa alcançar e manter sua conformidade com a lei.
Esse processo tem como objetivo identificar quais dados estão em posse (...) e assegurar sua privacidade, salvaguardando a instituição se porventura vir a enfrentar problemas com vazamentos, denúncias e afins." (LCNN, 2024)

[8] Dado estruturado é o dado que é representado por números, tabelas, linhas, colunas, atributos e assim por diante. Como o nome implica, dado estruturado é geralmente disciplinado, bem comportado, previsível e repetível. Dado textual não-estruturado é simplesmente um conjunto de caracteres como por exemplo dados encontrados em e-mails, relatórios, documentos, registros médicos e planilhas. Este tipo de dado não possui formato, nem estrutura e nem há repetição. (BARBOSA, 2016)

existência ou não da presença desse critério.

Vale mencionar que o critério de definição de uso de tecnologias emergentes ou inovadores possuem a mesma dificuldade teórica da avaliação dos impactos significativos. Não há centralização de uma lista, por exemplo, pela ANPD com a definição de um rol de tecnologias nessa esfera. Cabendo aos controladores realizar esse tipo de análise com base em suas próprias avaliações e convicções do mercado, o que pode gerar insegurança para o ecossistema nacional de proteção de dados pessoais.

Outro ponto passível de questionamentos trata-se da inovação apresentada pela ANPD que buscou a equiparação de idosos às crianças e adolescentes. Analisando esse critério com base no guia elaborado, a mera disponibilização para venda de produtos ou serviços no mercado, por sua vez, já poderá qualificar esse critério como existente no tratamento, uma vez que para realizar os procedimentos de venda e envio do produto ou prestação do serviço é necessário tratar dados pessoais e, via de regra, não há qualquer tipo de controle que impeça, por óbvio, idosos de consumir quaisquer produtos e serviços expostos amplamente no mercado.

Conforme esse critério está estabelecido hoje, qualquer empresa de grande porte que comercialize produtos ou serviços para mais de dois milhões de clientes, provavelmente, possuirá a necessidade de realizar um RIPD para aqueles tratamentos envolvidos na execução dos contratos de compra e venda, independentemente, da noção de riscos de privacidade atrelados a eles, distorcendo o próprio objetivo do guia e a definição de alto risco.

Com os exemplos endereçados anteriormente, fica claro que a falta de diretrizes claras sobre quando exatamente o RIPD se torna obrigatório adiciona certo nível de incerteza para os controladores de dados que devem determinar se a elaboração do relatório é necessária com base na sua própria interpretação das circunstâncias.

A dificuldade é ainda mais exacerbada pela ausência de uma regulamentação específica que trate do RIPD, levando os controladores a dependerem de orientações gerais e de melhores práticas estabelecidas por outros regulamentos e diretrizes. A recomendação da ANPD para o uso dos critérios da Resolução nº 2 como referência, embora útil, não substitui a necessidade de uma regulamentação dedicada e específica para o RIPD, o que poderia proporcionar uma maior clareza e segurança jurídica ao cenário nacional de privacidade e proteção de dados pessoais.

Considerações finais

A elaboração de um RIPD é uma prática indispensável para garantir a conformidade com a LGPD e a proteção dos direitos dos titulares de dados. No entanto, a identificação dos critérios de elegibilidade para o RIPD apresenta desafios significativos, principalmente devido à falta de regulamentação específica e à subjetividade de alguns critérios estabelecidos pela ANPD. A metodologia recomendada, que se baseia na composição de critérios gerais e específicos fornece uma base, mas também exige dos controladores esforço para realizar uma análise criteriosa e fundamentada de seus processos de tratamento de dados, o que pode causar dificuldades práticas aos controladores que não possuam maturidade acerca do tema.

A ausência de diretrizes claras e detalhadas aumenta a complexidade das avaliações dos critérios e pode gerar incertezas para os controladores de dados. No entanto, a adoção de práticas robustas de governança de dados, incluindo o mapeamento detalhado dos processos de tratamento, pode ajudar a mitigar essas dificuldades.

A comparação com a abordagem europeia, mais madura e detalhada, revela a necessidade de evolução na regulamentação brasileira. A criação de regulamentações específicas e a definição clara dos critérios de elegibilidade para o RIPD são passos fundamentais para fortalecer a proteção de dados pessoais no Brasil. Com essas medidas, espera-se que os controladores de dados tenham mais segurança jurídica e clareza para cumprir suas obrigações e proteger os direitos dos titulares de dados de maneira eficaz.

Além disso, é essencial que a Autoridade Nacional de Proteção de Dados (ANPD) promova diretrizes mais objetivas e incentivos à adoção de boas práticas relacionadas ao RIPD. A criação de guias orientativos, a realização de consultas públicas, a publicação de uma regulamentação específica para o tema e o incentivo à troca de experiências entre os agentes de tratamento e a autoridade podem contribuir para a consolidação de um entendimento mais uniforme sobre o tema. Paralelamente, as organizações devem investir na capacitação de seus profissionais e no aprimoramento de suas estruturas de governança de dados, garantindo que o RIPD não seja apenas um requisito formal, mas um instrumento eficaz na gestão de riscos e na proteção da privacidade dos titulares. A evolução da regulamentação e da cultura organizacional em torno do RIPD será determinante para que o Brasil alcance um nível de maturidade compatível com os desafios e avanços tecnológicos no tratamento de dados

pessoais.

Referências

ANPD. Consulta pública – Guia Orientativo Tratamento de Dados Pessoais de Alto Risco. 2024. Gov.br.. Disponível em: <https://www.gov.br/participamaisbrasil/blob/baixar/48651>.

ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Gov.br.. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd>.

ANPD. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Gov.br.. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022>.

ANPD. Resolução CD/ANPD nº 11, de 27 de dezembro de 2023. Gov.br.. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-11-de-27-de-dezembro-de-2023-534947737>.

BARBOSA, Elaine Muniz. Integração de Dados de Redes Sociais a Armazém de Dados. 2016. Disponível em: <http://hdl.handle.net/1843/ESBF-AKUNG3>.

BRASIL. Lei Geral de Proteção de Dados – Lei nº 13.709, de 14 de agosto de 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.

CABRAL, Filipe Fonteles. O Relatório de Impacto à Proteção de Dados Pessoais como um instrumento para o gerenciamento de riscos na Lei Geral de Proteção de Dados Pessoais. Caderno Especial: Lei Geral de Proteção de Dados (PGPD). São Paulo: Revista dos Tribunais, 2019. p. 200-211.

DOZZA, Eleonora Coelho. Uso secundário de dados pessoais e seu fundamento no legítimo interesse no Brasil pós-LGPD. 2023. Disponível em: <https://lume.ufrgs.br/bitstream/handle/10183/264345/001173367.pdf?sequence=1&isAllowed=y>.

EDPB. Aprovação das orientações do Grupo de Trabalho 29 sobre o RGPD pelo EDPB. 2018. Disponível em: <https://www.edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en>.

GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In: LIMA, Ana Paula; HISSA, Carmina; SALDANHA, Paloma Mendes (Org.). Direito Digital: Debates Contemporâneos. São Paulo: Revista dos Tribunais, 2019. p. 141-153.

GOMES, Maria Cecília O. Relatório de Impacto à Proteção de Dados: obrigatório para o tratamento de dados sensíveis? In: DALLARI, Analluza Bolivar; MONACO, Gustavo Ferraz (Coord.). LGPD na Saúde. 1. ed. São Paulo: Thomson Reuters Brasil, 2021. p. 263-275.

GOMES, Maria Cecília O. Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. Disponível em: <https://mariaceciliagomes.com.br/wp-content/uploads/2022/01/Relatorio_de_Impacto_a_Protecao_de_Dados.pdf>.

GRASSO, Ian Matiello. Relatório de Impacto à Proteção de Dados Pessoais na Lei Geral de Proteção de Dados: Uma Banalização? Cadernos Jurídicos da Faculdade de Direito de Sorocaba. Direito Digital, Ano 3, n. 1, 2021. p. 142-174.

LCNN – Laboratório Nacional de Computação Cientifica. O que é mapeamento de dados pessoais? 2024. Disponível em: <https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/o-que-e-mapeamento-de-dados-pessoais>.

LOHMANN, Pedro A.; ALBUQUERQUE, Raphael Carlos. Revisão Sistemática para o Processo de Avaliação de Impacto sobre a Proteção de Dados Pessoais e à Privacidade. [S.l.: s.n.], 2021.

STURARI, Matheus. O DPIA na LGPD: interpretação nacional ou banalização do instrumento? Perfil do Linkedin, 2020. Disponível em: <https://www.linkedin.com/pulse/o-dpia-na-lgpd-interpreta%C3%A7%C3%A3o-nacional-oubanaliza%C3%A7%C3%A3o-do-matheus/>.

WP29. 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. 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236>.