PARA ALÉM DA PROTEÇÃO DE DADOS: **UMA COLETÂNEA**

AUTORES

Anna Bentes
Bruno Bioni
Paula Guedes
Pedro H. Santos
Pedro Martins
Sinuhe Cruz

EDITORA
DATA PRIVACY BRASIL

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Para além da proteção de dados [livro eletrônico] : uma coletânea / Anna Bentes... [et al.]. -- São Paulo : Data Privacy Brasil Ensino, 2023. PDF

Outros autores: Bruno Bioni, Paula Guedes, Pedro H. Santos, Pedro Martins, Sinuhe Cruz.
Bibliografia.
ISBN 978-65-85344-00-5

1. Direito e tecnologia 2. Direito - Coletâneas 3. Proteção de dados - Direito - Brasil 4. Proteção de dados - Leis e legislação I. Bentes, Anna. II. Bioni, Bruno. III. Guedes, Paula. IV. Santos, Pedro H. V. Martins, Pedro. VI. Cruz, Sinuhe.

23-146358 CDU-34:6

Índices para catálogo sistemático:

1. Direito e tecnologia 34:6

Eliete Marques da Silva - Bibliotecária - CRB-8/9380

Organizadores
Anna Bentes
Paula Guedes
Pedro Martins
Pedro Henrique Santos
Bruno Bioni

Autores
Anna Bentes
Bruno Bioni
Paula Guedes
Pedro Martins
Pedro Henrique Santos
Sinuhe Cruz

Revisor
Sinuhe Cruz

Time de apoio
Gedeão França

Design
Roberto Junior

Sobre os autores

ANNA BENTES

Anna Bentes é Professora Adjunta na Escola de Comunicação, Mídia e Informação da Fundação Getúlio Vargas (ECMI-FGV). É Doutora e mestre em Comunicação e Cultura pela Universidade Federal do Rio de Janeiro (UFRJ) e formada em Psicologia pela UFRJ. É autora do livro "Quase um tique: economia da atenção, vigilância e espetáculo em uma rede social'', pela editora UFRJ (2021), e Membro do Conselho Diretivo da Rede Latino Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (LAVITS). É colunista do Terra Byte, onde fala sobre temas relacionados à tecnologia e comportamento. Atualmente, é *Fellow* da Derechos Digitales, liderando uma pesquisa sobre desinformação nas eleições brasileiras de 2022. Em suas pesquisas, está interessada na intersecção entre Comunicação, Psicologia e Mídias Digitais.

BRUNO BIONI

Doutor em Direito Comercial e Mestre em Direito Civil na Faculdade de Direito da Universidade de São Paulo - USP. Membro do Conselho Nacional da Autoridade Nacional de Proteção de Dados - CNPD, designado como titular dentre os representantes de organizações da sociedade civil. Foi *study visitor* do Departamento de Proteção de Dados Pessoais do *European Data Protection Board* - EDPB e do Conselho da Europa-CoE, pesquisador visitante no Centro de Pesquisa de Direito, Tecnologia e Sociedade da Faculdade de Direito da Universidade de Ottawa. É autor do livro "Proteção de Dados Pessoais: a função e os limites do consentimento'' e co-autor do livro "Proteção de dados: contexto, narrativa e elementos fundantes". É membro da Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade - LAVITS. É diretor fundador do Data Privacy Brasil, um espaço de intersecção entre uma escola de cursos e uma associação de pesquisa na área de privacidade e proteção de dados. É advogado, consultor e parecerista.

PAULA GUEDES

Doutoranda em Direito pela Universidade Católica Portuguesa – Centro Regional do Porto (bolsista da Fundação para a Ciência e Tecnologia) e Mestre em Direito Internacional e Europeu pela mesma instituição; especialista em Direito Digital pelo ITS-Rio em parceria com a UERJ. Pesquisadora do grupo de pesquisa em Direito e Tecnologia da PUC-Rio (Legalite) e membro do Grupo de Estudos em Novas Regulações de Serviços Digitais no Direito Comparado do *Legal Grounds Institute*.

PEDRO HENRIQUE SANTOS

Graduado em Direito pela Universidade Federal de Juiz de Fora. Advogado e colaborador externo do Centro de Referência em Direitos Humanos da Universidade Federal de Juiz de Fora - Campus Governador Valadares. É membro do setor acadêmico do Data Privacy Brasil Ensino.

PEDRO MARTINS

Mestre em Direito pela Universidade Federal de Minas Gerais. Desenvolve pesquisa na área de proteção de dados pessoais e profiling. É autor do livro “Profiling na Lei Geral de Proteção de Dados: O livre desenvolvimento da personalidade em face da governamentalidade algorítmica” pela editora Foco (2022). Pesquisador do grupo de pesquisa Persona e Coordenador Acadêmico do Data Privacy Brasil.

SINUHE CRUZ

Bacharel em Direito pela Universidade de São Paulo e pesquisador nas áreas de privacidade, proteção de dados e regulação de novas tecnologias. Colaborou como Analista Acadêmico do Data Privacy Brasil entre 2020 e 2022

Sumário

5

O risco como elemento do sistema normativo de proteção de dados pessoais

Paula Guedes Fernandes da Silva

Com as constantes mudanças tecnológicas, que permitem intensa coleta de dados pessoais e aumento do uso de técnicas algorítmicas de perfilização, criação de inferências e predições de comportamentos e tomada de decisões automatizadas sobre os titulares de dados, o tratamento de dados pessoais é visto como uma atividade intrinsecamente de risco. Consequentemente, há uma clara ligação entre o direito à proteção de dados pessoais e a regulação do risco, o que é observado nas mais recentes leis de proteção de dados pessoais mundialmente[15], tendo como exemplo o Regulamento Europeu de Proteção de Dados Pessoais (GDPR) e a Lei Geral de Proteção de Dados Pessoais (LGPD).

Neste capítulo, nosso objetivo é ressaltar a relação entre o risco e o tratamento de dados pessoais, explorando a noção de avaliação de impacto e o instrumento do relatório de impacto como uma medida prática adequada para a proteção de direitos fundamentais dos titulares dos dados pessoais tratados. Além de artigos acadêmicos, traremos modelos de relatório de impacto vindas do direito comparado, assim como documentos de autoridades, dentre outros materiais, que te ajudarão a adentrar a noção de proteção de dados pessoais como uma atividade intrinsecamente de risco. Vamos lá?

---

15 ZANATTA, Rafael A. F. Proteção de *Dados Pessoais como Regulação de Risco: uma nova moldura teórica?* I Encontro da Rede de Pesquisa em Governança da Internet. Novembro de 2017.

O risco e a proteção de dados pessoais

a. Ideias iniciais sobre o conceito geral de risco

Segundo Raphaël Gellert, o risco pode ser compreendido como uma ferramenta auxiliar para a tomada de decisões, já que torna algo incerto como certo, englobando uma dupla noção: trata-se da tentativa de prever eventos futuros (positivos ou negativos) e, a partir disso, facilita e orienta a tomada de decisões[16]. Em outras palavras, não falamos da existência ou não do risco, mas presumimos a sua existência. Ele é inerente, variando apenas o nível de risco que um determinado agente consegue assumir e mitigar[17].

SAIBA MAIS

- BECK, Ulrich. **Sociedade de Risco: rumo a uma outra modernidade**. Tradução de Sebastião Nascimento. Editora 24, 2ª Edição, 2011.
- BERNSTEIN, Peter L. **Against the Gods: The Remarkable Story of Risk**. John Wiley & Sons, 1998.
- GOMES, Maria Cecília O. **Entre o método e a complexidade: compreendendo a noção de risco na LGPD**. *In: Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

b. Ideias iniciais sobre o conceito geral de risco

A narrativa de se controlar riscos de uma atividade econômica não é nova, utilizada há anos, por exemplo, para a regulação do setor automobilístico, de medicamentos e de alimentos[18]. No campo da privacidade e da proteção de dados pessoais, não é diferente: o

---

16 GELLERT, Raphaël. *Understanding the risk-based approach to data protection: an analysis of the links between law, regulation, and risk*. PhD Thesis. Faculty of Law and Criminology, Vrije Universiteit Brussel, 2017. p. 35.

17 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: Direito Digital: Debates Contemporâneos*, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

18 ZANATTA, Rafael A. F. *Proteção de Dados como Regulação de Risco: uma nova moldura teórica?* I Encontro da Rede de Pesquisa em Governança da Internet, Novembro de 2017. Disponível em: **https://www.researchgate.**

risco sempre foi um dos elementos presentes na narrativa e justificativa da necessidade de leis de proteção de dados pessoais, desde o primeiro momento, na década de 60-70, quando se criaram as primeiras leis, com a constatação de que a atividade de tratamento de dados pessoais geraria um risco, principalmente de o Estado usurpar esse poder[19].

Nos últimos anos, com os progressivos avanços tecnológicos, que impulsionaram a criação de leis gerais de proteção de dados pessoais mais modernas, como o GDPR, a tutela do direito à proteção de dados pessoais enfrentou um processo de transformação. A partir de uma lógica regulatória prévia (*ex-ante*), baseada na prevenção e mitigação de riscos, o Regulamentou diferenciou-se da antiga Diretiva 95/46/CE. Nesse novo modelo, a salvaguarda dos direitos fundamentais é complementada pela implementação de análises de risco, licenças, processos de documentação, registro de processos e prestação de contas (*accountability*) por parte dos agentes de tratamento de dados pessoais[20].

Nesse cenário de aumento dos fluxos informacionais e uso cada vez mais intenso de técnicas algorítmicas, Claudia Quelle[21] e Raphaël Gellert[22] ressaltam uma clara ligação entre a proteção de dados e regulação do risco, a partir da noção de "risquificação" do direito de proteção de dados pessoais que ganhou força principalmente no cenário europeu[23]. A abordagem baseada no risco (*risk-based approach*), trazida pelo GDPR, busca identificar, calibrar e mitigar potenciais riscos envolvidos nos tratamentos de dados pessoais

---

net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica. p. 181.

19 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: Direito Digital: Debates Contemporâneos*, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

20 ZANATTA, Rafael A. F. *Proteção de Dados como Regulação de Risco: uma nova moldura teórica?* I Encontro da Rede de Pesquisa em Governança da Internet, Novembro de 2017. Disponível em: **https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica**. p. 176 e 181.

21 QUELLE, Claudia. Does the risk-based approach to data protection conflict with the protection of fundamental rights on a conceptual level? *Tilburg Law School Research Paper* , pp. 1-36, 2015.

22 GELLERT, Raphaël. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law , Vol. 5, pp. 3-20, 2015.

23 ZANATTA, Rafael A. F. *Proteção de Dados como Regulação de Risco: uma nova moldura teórica?* I Encontro da Rede de Pesquisa em Governança da Internet, Novembro de 2017. Disponível em: **https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica**. p. 182.

que possam causar violações a direitos e liberdades fundamentais dos titulares, como uma espécie de gestão de riscos[24].

Assim, fica claro que o risco é um ponto central para as atividades regulatórias, já que é elemento inerente e sempre presente nas atividades de tratamento. Por isso, nos processos envolvendo dados pessoais, deve-se levar em consideração o quanto de risco um determinado agente de tratamento é capaz de assumir e o quanto de risco ele consegue mitigar[25].

No contexto brasileiro, a Lei Geral de Proteção de Dados do Brasil (LGPD) aproxima-se também na lógica de "risquificação" da proteção de dados pessoais. Apesar de trazer instrumentos de controle a posteriori, como a figura da responsabilidade civil, em que o risco é impulsionador das obrigações de reparar possíveis danos, a LGPD aposta também na prevenção de danos, evitando a ocorrência de violações de direitos fundamentais, a partir de instrumentos de regulação *ex-ante*[26], como vemos na tabela abaixo.

Obrigação de elaboração de relatórios de impacto, com a eventual descrição dos processos potencialmente causadores de riscos às liberdades civis e direitos fundamentais pela ANPD, além da imposição de mecanismos de mitigação desses riscos.	Art. 5º, XVII; art. 10, § 3º; art. 38 da LGPD.
Princípio da prevenção	Art. 6º, VIII da LGPD.
Obrigação de adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais	Art. 6º, VII; art. 46 da LGPD.
Adoção de boas práticas de modelos de gestão de risco	Art. 50 da LGPD.
Criação de autoridade de proteção de dados com alta expertise técnica para fiscalizar a boa aplicação da lei e, eventualmente, sancionar	Capítulo IX da LGPD.

24 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: Direito Digital: Debates Contemporâneos*, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

25 GOMES, Maria Cecília O. *Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In:* Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

26 ZANATTA, Rafael A. F. *Proteção de Dados como Regulação de Risco: uma nova moldura teórica?* I Encontro da Rede de Pesquisa em Governança da Internet, Novembro de 2017. Disponível em: **https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica**. p. 188-189.

SAIBA MAIS

- ZANATTA, Rafael A. F. Proteção de Dados como Regulação de Risco: uma nova moldura teórica? I Encontro da Rede de Pesquisa em Governança da Internet, Novembro de 2017. Disponível em: **https://www.researchgate.net/publication/322804864_Protecao_de_dados_pessoais_como_regulacao_do_risco_uma_nova_moldura_teorica**.

- COSTA, Luiz. Privacy and the precautionary principle. Computer Law & Security Review, Vol. 28, 2012, pp. 14-24. Disponível em: **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000702**.

- BIONI, Bruno Ricardo; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? Disponível em: **https://brunobioni.com.br/home/wp-content/uploads/2019/09/Bioni-Luciano_O-PRINCÍPIO-DA-PRECAUÇÃO-PARA-REGULAÇÃO-DE-INTELIGÊNCIA-ARTIFICIAL-1.pdf**.

- QUELLE, Claudia. The 'risk revolution' in EU data protection law: We can't have our cake and eat it, too. Tilburg Law School Legal Studies Research Paper Series No. 17/2017. Disponível em: **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000382**.

Gestão de Risco no campo da proteção de dados pessoais

Atualmente, não existe uma definição universal consensual para a noção de risco no campo da proteção de dados pessoais, já que o risco pode significar coisas diferentes para pessoas diferentes[27]. De certo, embora existam variadas definições de risco nesta área, tanto o GDPR como a LGPD priorizam o risco adverso para os titulares de dados e toda a coletividade, em contraposição aos riscos para a organização ou negócio, como os riscos de oportunidade, financeiros, reputacionais e de litígio[28]. O referencial primordial desta definição deve ser o titular de dados, isto é, suas liberdades civis e direitos fundamentais[29].

---

27 Centre for Information Policy Leadership (CIPL). Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. CIPL GDPR Interpretation and Implementation Project, Dezembro de 2016. Disponível em: **https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf**, p. 13.

28 Ibid. p. 14.

29 GOMES, Maria Cecília Oliveira. *Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In:* Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

Porém, o risco continua sendo uma noção abstrata que precisa de metodologias, modelos e processos que o implementem concretamente[30]. Nesse contexto, muito se fala da gestão de riscos, isto é, processo mediante o qual se identifica, analisa e valoriza a probabilidade e o impacto da ocorrência de ameaças que, através da exploração de alguma vulnerabilidade, possam materializar um risco para os direitos e liberdades fundamentais das pessoas. Assim, o objetivo é identificar as hipóteses de risco e avaliá-las para, em seguida, definir o plano necessário para minimizá-los[31].

a. Avaliação de risco

Dito isso, dentro da gestão de riscos, a avaliação busca identificar os riscos existentes, sob o referencial escolhido, e mitigá-los o máximo possível até um patamar aceitável. Em outras palavras, o propósito da avaliação não é eliminar todos os riscos existentes, já que isso não é um objetivo alcançável, mas eliminar riscos inaceitáveis e reduzir riscos altos o quanto possível[32]. Consequentemente, os agentes de tratamento, ao realizarem a avaliação do risco de suas atividades de tratamento, não devem limitar-se à checagem de sua conformidade com a LGPD e demais regulações (não deve ser apenas um "*checklist de compliance*"), mas deve incluir também uma análise mais profunda, em que seja possível mensurar os possíveis efeitos adversos aos titulares de dados[33].

Para esta avaliação, é imprescindível a escolha de um método adequado, o que inclui a escolha de metodologia e sua justificativa, assim como o desenvolvimento de uma matriz de risco com indicadores mínimos de análise, como contexto, volume, espécie e natureza dos dados e tipos de titulares[34].

---

30 GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, Volume 34, Issue 2, 2018, pp. 279-288. Disponível em: **https://doi.org/10.1016/j.clsr.2017.12.003**.

31 Agencia de Acceso a la Información Pública de Argentina (AAIP); Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay. Guía de Evaluación de Impacto en la Protección de Datos. Janeiro 2020.

32 Centre for Information Policy Leadership (CIPL). Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. CIPL GDPR Interpretation and Implementation Project, Dezembro de 2016. Disponível em: **https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf**, p. 14.

33 GOMES, Maria Cecília Oliveira. *Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In:* Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

34 Ibid.

Baseada em riscos *(risk-based approach)*	**ICO-UK** - **Guia para elaboração de DPIA com checklist para avaliação do processo**; **dpia.lab** - **Data protection impact assessment in the European Union: developing a template for a report from the assessment process**; **Secretaria do Governo Digital (BR)** - **Template sobre relatório de impacto à proteção de dados pessoais**
Baseada em riscos e benefícios	**Berkman Klein Center** - **Open Data Privacy Playbook** (2017); **Future Privacy Forum** - **City of Seattle: Open Data Risk Assessment**.
Baseada em direitos	**Berkman Klein Center** - **Principled Artificial Intelligence: mapping consensus in ethical and rights-based approaches to principles for AI** (2020)

A fórmula mais conhecida e aceita para avaliar riscos é formada por probabilidade x impacto, onde a probabilidade é determinada com base nas possibilidades existentes de materialização da ameaça e o impacto é determinado com base no dano (material ou moral) que pode ocorrer no caso desta materialização[35].

Risco = Probabilidade x Impacto

Nesse contexto, por mais que seja possível escrever esta fórmula para a avaliação do risco, ele não é quantificável, já que é um elemento normativo de características qualitativas e valorativas apenas. Por isso, podemos falar em classificações de risco como (muito) alto, médio e baixo, mas não em termos de quantificação[36], de forma a definir os níveis adequados, aceitáveis e inaceitáveis. Abaixo, exemplos de descrição dos níveis de probabilidade e impacto e, em seguida, de uma matriz de risco:

35 Agencia de Acceso a la Información Pública de Argentina (AAIP); Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay. Guía de Evaluación de Impacto en la Protección de Datos. Janeiro 2020.

36 GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In: Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

	BAIXA	MÉDIA	ALTA	MUITO ALTA
PROBABILIDADE	Pode acontecer apenas em circunstâncias excepcionais	É um evento raro e pouco frequente, embora não improvável	É possível que ocorra uma vez ao ano	É possível que ocorra várias vezes ao ano
	BAIXA	**MÉDIA**	**ALTA**	**MUITO ALTA**
IMPACTO	Os titulares dos dados não serão afetados ou sofrerão apenas alguns inconvenientes, que poderão resolver sem muitas dificuldades	Os titulares dos dados serão afetados de forma significativa, podendo superar a situação com alguma dificuldade	Os titulares dos dados serão afetados de forma significativa e só poderão superar a situação com grandes dificuldades	Os titulares dos dados serão afetados com consequências gravíssimas e irreversíveis que talvez não possam superar

Agencia de Acceso a la Información Pública de Argentina (AAIP); Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay. Guía de Evaluación de Impacto en la Protección de Datos. Janeiro 2020.

PROBABILIDADE				
Muito alta (4)	**4**	**8**	**12**	**16**
Alta (3)	**3**	**6**	**9**	**12**
Média (2)	**2**	**4**	**6**	**8**
Baixa (1)	**1**	**2**	**3**	**4**
	Baixa (1)	Média (2)	Alta (3)	Muito alta (4)
				IMPACTO

Agencia de Acceso a la Información Pública de Argentina (AAIP); Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay. Guía de Evaluación de Impacto en la Protección de Datos. Janeiro 2020.

b. Mitigação de riscos

Com tais exemplificações, é possível compreender que, considerando o nível identificado pela matriz de risco de probabilidade x impacto, o controlador pode determinar quais riscos precisam indiscutivelmente de mitigação, quais devem ser monitorados e quais não representam risco significativo para a os direitos e liberdades fundamentais dos titulares (e para a organização). O risco inerente, após implementação das medidas de mitigação, torna-se residual. Em outras palavras, o risco inerente é aquele existente sem a aplicação de medidas ou controles, enquanto o residual considera tais aplicações, o que permite verificar na prática a eficácia de tais medidas na redução e mitigação de riscos[37].

Em resumo, a partir do nível identificado pela matriz de risco, é possível pensar quais podem ou não ser assumidos. Por vezes, por exemplo, o nível de risco é alto, mas pode ser reduzido até um ponto aceitável com a implementação de medidas de mitigação. Lembrando que é impossível reduzir os níveis de risco ao zero, principalmente devido à complexidade do cenário de proteção de dados pessoais[38], de forma que a decisão a ser tomada é se o nível de risco é suficientemente baixo para ser tomado e se há medidas eficientes para a redução concreta desse risco, o que é feito na fase de gerenciamento ou mitigação de riscos[39].

Nesse contexto de proteção de dados pessoais, compreende-se como mitigação de riscos todas as ações afirmativas assumidas pelo controlador com o objetivo de redução dos riscos existentes, como pode acontecer com a decisão de não realizar tratamento de dados pessoais sensíveis em larga escala. Na LGPD, por exemplo, foram previstas algumas dessas ferramentas, como a previsão de Programas de Governança, Privacy by Design e by Default, Códigos de Boas Condutas, Certificações e até mesmo o Relatório de Impacto à Proteção de Dados Pessoais[40].

---

37 Agencia de Acceso a la Información Pública de Argentina (AAIP); Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay. Guía de Evaluación de Impacto en la Protección de Datos. Janeiro 2020.

38 GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In: Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

39 GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, Volume 34, Issue 2, 2018, pp. 279-288. Disponível em: **https://doi.org/10.1016/j.clsr.2017.12.003**

40 GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In: Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

Caso tenha interesse em se aprofundar no tema de gestão e avaliação de riscos de proteção de dados pessoais, recomendamos a leitura dos documentos e materiais abaixo:

SAIBA MAIS

- Agencia Española de Protección de Datos (AEPD). **Evalúa Riesgo RGPD**.
- Agencia Española de Protección de Datos (AEPD). **Gestión del riesgo y evaluación de impacto en tratamientos de datos personales**.
- Commission Nationale de l'Informatique et des Libertés (CNIL). **Privacy Impact Assessment (PIA)**.
- Centre for Information Policy Leadership (CIPL). **Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR**. Dezembro 2016.
- GREEN, Ben *et al*. **Open Data Privacy**. Berkman Klein Center for Internet & Society Research Publication, 2017.
- Future of Privacy Forum. **City of Seattle: Open Data Risk Assessment**. Final Report, 2018.
- Office of the Australian Information Commissioner (OAIC). **Guide to undertaking privacy impact assessments**. Setembro de 2021.
- Secretaria do Governo Digital. **Guia e Ferramenta para avaliação de riscos de segurança e privacidade**. Brasil, novembro de 2020.

Avaliação de Impacto à Proteção de Dados Pessoais

A avaliação de impacto (ou sua derivação como um relatório de impacto, previsto na LGPD) existe em diversas áreas e em diferentes contextos e é uma ferramenta já utilizada há décadas: só na área de proteção de dados estamos falando de um debate de mais de 30 anos. Porém, essa temática é recente para o campo da proteção de dados no Brasil, já que a norma sobre avaliação de impacto de proteção de dados só foi prevista na LGPD em 2018[41].

41 GOMES, Maria Cecília Oliveira. 3ª Audiência Pública da CJSUBIA. Painel 6 – Inteligência artificial e riscos: gradação

A avaliação de impacto tem ocupado um lugar de destaque como uma forma de avaliar o risco, tendo por função a prevenção de riscos aos direitos e liberdades fundamentais, bem como a promoção de maior prestação de contas e transparência. Desde logo fica clara a vinculação do instrumento com a ideia de prevenção e não de reparação.

Dito isso, é necessário que fique claro que essa avaliação precisa ser feita no momento do desenvolvimento de uma certa tecnologia ou atividade, de forma prévia, e que os riscos precisam ser avaliados e prevenidos antes de se concretizarem, sempre na lógica da prevenção e de se evitar o risco, o que está alinhado ao princípio da precaução e não apenas com o da mitigação - este último entendido quando o risco já se concretizou, por exemplo, após uma tecnologia já ter sido disponibilizada no mercado[42].

Nesse sentido, a avaliação de impacto pode seguir diversas metodologias, sendo a mais comum, inclusive no âmbito da proteção de dados, a abordagem baseada em risco (*risk-based approach*), que pode, inclusive, ser orientada a direitos, tendo como norte-central a prevenção de riscos aos direitos humanos[43]. Porém, independentemente da metodologia escolhida, é fundamental que haja um referencial e uma fundamentação adequados[44].

a. RIPD na LGPD

O art. 5º, inciso XVII da LGPD conceitua o Relatório de Impacto à Proteção de Dados Pessoais a partir de alguns elementos: (i) documento do controlador (forma que deve existir e ser apresentado); (ii) que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e direitos fundamentais; (iii)

---

de riscos; hipóteses de riscos inaceitáveis e princípio da precaução. Disponível em: **https://www12.senado.leg.br/portalcedoc/pcedoc1/2022/20220429/20220429142500_1510253.MP4**.

42 GOMES, Maria Cecília Oliveira. 3ª Audiência Pública da CJSUBIA. Painel 6 – Inteligência artificial e riscos: gradação de riscos; hipóteses de riscos inaceitáveis e princípio da precaução. 29 de abril de 2022.

43 GOMES, Maria Cecília Oliveira. 3ª Audiência Pública da CJSUBIA. Painel 6 – Inteligência artificial e riscos: gradação de riscos; hipóteses de riscos inaceitáveis e princípio da precaução. Disponível em: **https://www12.senado.leg.br/portalcedoc/pcedoc1/2022/20220429/20220429142500_1510253.MP4**.

44 GOMES, Maria Cecília Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In: Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

além de conter também as medidas, salvaguardas e mecanismos de mitigação de risco.

A partir dessa leitura, observa-se que tal documentação não tem como objetivo primário a conformidade de uma organização com as normas de proteção de dados pessoais, mas sim, por meio de uma matriz de risco de uma avaliação de risco, prevenir e mitigar riscos aos direitos dos titulares, o que inclui não apenas os direitos de proteção de dados pessoais por si só, mas também os direitos e liberdades fundamentais previstos na Constituição Federal de 1988 e demais legislações infraconstitucionais[45].

Ainda, é essencial que o relatório de impacto não seja difundido como um documento frio e estático, feito apenas para mera conformidade da organização com a legislação de proteção de dados pessoais. Pelo contrário, deve ser entendido como um documento vivo dinâmico, que deve ser atualizado e revisitado de tempos em tempos, principalmente após alguma mudança significativa nas operações envolvendo dados pessoais, de forma a auxiliar na governança de dados e na prevenção e mitigação de riscos vinculados ao tratamento de dados pessoais[46].

Como já salientado, a natureza desse instrumento parte de uma ideia de prevenção, apesar de o texto da LGPD focalizar também na mitigação, isto é, na redução de danos causados por riscos e redução dos riscos já presentes que ainda não foram geradores de danos. Consequentemente, o relatório de impacto na LGPD atua como uma ferramenta de governança de dados, não apenas utilizado durante os processos de adequação regulatória, mas para garantia dos direitos e liberdades fundamentais dos titulares[47], principalmente nos casos de tratamento de dados pessoais de alto risco, conforme o texto do art. 55-J, inciso XIII da lei.

Apesar de a LGPD ter conceituado o relatório de impacto e trazido um artigo específico sobre ele, (art. 5º, XVII e art. 38, respectivamente), será fundamental que a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) traga maiores orientações, de forma didática e acessível, sobre quais operações podem acarretar riscos aos titulares e, ainda, como mensurar esses riscos, por meio do desenvolvimento de uma matriz de risco baseada em uma metodologia de avaliação a ser utilizada durante a avaliação de impacto

45 GOMES, Maria Cecília Oliveira. Relatório de Impacto a Proteção de Dados. Uma breve análise da sua definição e papel na LGPD. Publicado na Revista do Advogado nº 144, 2019. p. 9-11.

46 Ibid. p. 14.

47 Ibid. p. 12.

e, finalmente, concretizada e indicada no relatório, considerando a realidade brasileira e suas particularidades[48].

Ademais, caso a ANPD traga uma lista de atividades que entenda como de alto risco, deve haver a indicação clara de se tratar de um rol meramente exemplificativo, pois a existência de um rol taxativo seria um objetivo ilusório já que, conforme Maria Cecília Gomes Oliveira, "é possível que operações de tratamento de dados pessoais que possam gerar alto risco não estejam acobertadas por uma orientação porque elas não foram mapeadas e analisadas em estudos de caso, ou simplesmente, porque elas ainda não existem"[49].

Caso tenha interesse em se aprofundar no tema de avaliação de impacto de proteção de dados pessoais, recomendamos a leitura dos documentos e materiais abaixo:

SAIBA MAIS

- EDPB. **Guidelines on Data Protection Impact Assessment (DPIA)**. 2017.
- EDPS. **Survey on Data Protection Impact Assessments under Article 39 of the Regulation** (case 2020-0066).
- Agencia de Acceso a la Información Pública de Argentina (AAIP); Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay. **Guía de Evaluación de Impacto en la Protección de Datos**. Janeiro 2020.
- DATA PRIVACY BRASIL. **Reunião Técnica sobre Relatório de Impacto de Proteção de Dados Pessoais – Maria Cecília O. Gomes**. Youtube, 1 jul. 2021.
- IAB Europe. **Guidance: GDPR Data Protection Impact Assessments (DPIA) for Digital Advertising under GDPR**. Novembro 2020.
- GOMES, Maria Cecília Oliveira. **Relatório de Impacto a Proteção de Dados. Uma breve análise da sua definição e papel na LGPD**. Publicado na Revista do Advogado nº 144, 2019.

48 Ibid. p. 13.

49 GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. *In: Temas atuais de proteção de dados*. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

- GOMES, Maria Cecília Oliveira. **Para além de uma obrigação legal: o que a metodologia de benefícios e riscos nos ensina sobre o papel dos relatórios de impacto à proteção de dados**. *In: Direito Digital: Debates Contemporâneos*, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. Revista dos Tribunais, 2019, pp 141-153.
- Agencia Española de Protección de Datos (AEPD). **Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado**. Março de 2022.
- Information Commissioner 's Office (ICO-UK). **Sample DPIA template**. 2018.
- GOMES, Maria Cecília Oliveira. **LGPD: Desafios da regulamentação do relatório de impacto**. JOTA, publicado em 11 fevereiro de 2021.
- GOMES, Maria Cecília Oliveira. **3ª Audiência Pública da CJSUBIA. Painel 6 – Inteligência artificial e riscos: gradação de riscos; hipóteses de riscos inaceitáveis e princípio da precaução**. 29 de abril de 2022.
- KLOZA, Dariusz *et al*. **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), pp. 1-4.
- KLOZA, Dariusz *et al*. **Data protection impact assessment in the European Union: developing a template for a report from the assessment process**. d.pia.lab Policy Brief, 2020(1), 1-52.
- Secretaria do Governo Digital. **Guia e Template de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. Brasil.

b. Quais atividades de proteção de dados pessoais podem ser consideradas como de alto risco?

Apesar de a LGPD não ter exemplificado atividades de tratamento de dados pessoais de alto risco e ainda não termos uma regulamentação da ANPD específica para esta questão, já existem algumas orientações sobre risco que podem ser retirados dos mais recentes documentos publicados pela Autoridade brasileira, além de outras Autoridades do direito comparado, como é o caso do European Data Protection Board – EDPB (antigo Article 29 Data Protection Working Party – WP29). Vejamos:

AUTORIDADE DE PROTEÇÃO DE DADOS	WP29 (atual EDPB)
NOME DO DOCUMENTO	**Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679**
ATIVIDADE DE ALTO RISCO	Alguns critérios orientadores: • Realização de avaliação ou pontuação, incluindo criação de perfil e previsão, especialmente de "aspectos relativos ao desempenho do titular dos dados no trabalho, situação econômica, saúde, preferências ou interesses pessoais, confiabilidade ou comportamento, localização ou movimentos"; • Decisões automatizadas com significativos efeitos legais; • Monitoramento sistemático de titulares de dados; • Tratamento de dados com dados pessoais sensíveis; • Tratamento em larga escala; • Combinação de bancos de dados; • Utilização de dados de titulares de dados vulneráveis; • Utilização ou aplicação de novas tecnologias ou soluções organizacionais, como a combinação de digitais e reconhecimento facial para o controle físico de acessos; • Quando o tratamento de dados por si só impede que os titulares exerçam seus direitos, utilizem serviços ou contratos

AUTORIDADE DE PROTEÇÃO DE DADOS	ANPD
NOME DO DOCUMENTO	**Resolução CD/ANPD nº 2 de 2022 - Regulamento de Aplicação da LGPD para agentes de tratamento de pequeno porte**
ATIVIDADE DE ALTO RISCO	É considerado de alto risco o tratamento de dados pessoais que atenda de forma cumulativa a pelo menos 1 critério geral e um específico, conforme lista abaixo: • Critérios gerais: a) 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; • 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.

AUTORIDADE DE PROTEÇÃO DE DADOS	ANPD
NOME DO DOCUMENTO	**Regulamento de Dosimetria e Aplicação de Sanções Administrativas**
ATIVIDADE DE ALTO RISCO	Possíveis critérios para tratamento de dados de alto risco, considerando o que a ANPD considera como infração grave da LGPD: • Envolver tratamento de dados pessoais em larga escala ou afetar significativamente interesses e direitos fundamentais dos titulares em conjunto com, pelo menos, uma das hipóteses abaixo: a. Tratamento com auferição ou pretensa auferição de vantagem econômica fruto deste tratamento; b. Tratamento que implique risco à vida ou à integridade física do titular; c. Envolver tratamento de dados sensíveis ou dados de crianças e adolescentes e de idosos; d. Tratamento de dados pessoais realizado sem amparo a uma das bases legais da LGPD; e. Tratamento de dados que se utiliza da fraqueza ou ignorância do titular de dados, considerando sua saúde, conhecimento ou condição social; f. Tratamento que tenha efeitos discriminatórios ilícitos ou abusivos.

AUTORIDADE DE PROTEÇÃO DE DADOS	Comissão Europeia
NOME DO DOCUMENTO	**Proposta de Regulamento de Inteligência Artificial da União Europeia**
ATIVIDADE DE ALTO RISCO	Exemplos de atividades realizadas por sistemas de inteligência artificial que são consideradas de alto risco: • sistemas de IA autônomos com implicações em matéria de direitos fundamentais, tais como: a. Identificação biométrica e categorização de pessoas naturais; b. Gestão e funcionamento de infraestruturas críticas, como os sistemas de IA desenvolvidos para utilização em sistemas de segurança na gestão e controle de trânsito, abastecimento de água, gás, aquecimento e eletricidade; c. Utilização em educação e formação profissional; d. Utilização na área de emprego, gestão de trabalhadores e acesso ao emprego por conta própria; e. Acesso a serviços privados e a serviços e prestações públicas essenciais, bem como o usufruto dos mesmos;

	f. Utilização para manutenção da ordem pública, como os utilizados por autoridades policiais para avaliar riscos individuais de pessoas para determinação do risco do cometimento de infrações; g. Utilização para gestão da migração, asilo e controle de fronteiras; h. Utilização para administração da justiça e processos democráticos, como auxílio a uma autoridade judiciária na investigação e interpretação de fatos e aplicação da lei.

Dito isso, ainda esperaremos futuras orientações da ANPD específicas sobre a figura do relatório de impacto à proteção de dados pessoais, assim como a definição ou exemplificação sobre as atividades de tratamento de alto risco. De certo, a Autoridade não deve estabelecer um conceito fechado sobre o que é risco mas sim demonstrar como o risco pode ser avaliado por meio de metodologias para avaliação de risco e elaboração de relatórios de impacto à proteção de dados pessoais. Consequentemente, como mencionado, será fundamental que sejam estabelecidos os critérios mínimos de análise de uma atividade de alto risco, o que pode, inclusive, beber dos exemplos elencados acima, desde que sejam consideradas as particularidades do contexto de proteção de dados brasileira.