FGV DIREITO SP
MESTRADO PROFISSIONAL

Abordagem de riscos considerando premissas relacionadas ao Privacy by Design, Security by Design e Human Centered AI

Lizandra Muchelli P. S. de Almeida

Projeto de pesquisa apresentado ao
Mestrado Profissional da FGV Direito SP.

Versão de 13.11.2023

1. Tema, contexto e delimitação de escopo

1.1. Contextualização e recorte temático:

Este trabalho de pesquisa tem por objetivo a elaboração de documentos-modelo consistentes em **frameworks e matrizes de riscos** para o desenvolvimento de novas tecnologias, considerando premissas e conceitos relacionados ao *Privacy By Design, Security By Design* e *Privacy Enhancing Technologies* (PETs), e considerando ainda, uma abordagem de desenvolvimento da Inteligência Artificial centrada no ser humano (*Human Centered AI*). Além dos aspectos técnicos relacionados aos citados conceitos, os documentos-modelo a serem elaborados como fruto desta pesquisa levarão em consideração o **custo-benefício econômico e a competitividade** para as empresas de tecnologia.

1.2. Questão central de pesquisa

A definição e a avaliação de riscos no contexto do desenvolvimento tecnológico sempre foi um ponto crítico para a elaboração de frameworks e matrizes de riscos capazes de avaliar de maneira eficaz os pontos críticos de um projeto, identificando as respectivas medidas mitigadoras e refletindo adequadamente a realidade do projeto.

O objetivo de frameworks e matrizes de riscos é trazer uma ponderação, uma análise de custo-benefício para o desenvolvimento de um novo produto/serviço, e deverá levar em consideração não apenas fatores técnicos, mas em especial fatores que podem impactar a vida humana, trazendo riscos muitas vezes difíceis de se mensurar e mitigar.

Trazer todos os elementos relevantes para esses documentos é um desafio, na medida em que isso envolve questões multidisciplinares e uma análise muitas vezes filosófica relacionada ao impacto que novos produtos/serviços de tecnologia podem gerar na economia e na sociedade, de forma global.

Entender como esses riscos devem ser identificados, analisados, mensurados, classificados e, por fim, mitigados pode impactar diretamente na forma como se dará a evolução da sociedade. Isso porque, a depender dos impactos produzidos em função dos riscos assumidos no desenvolvimento de produtos tecnológicos, pode-se chegar a uma mudança na forma como a sociedade se comunica, locomove ou mesmo como as pessoas enxergam o certo e o errado em termos éticos.

A tecnologia está presente em todas as searas da vida humana e não há caminho de volta. Mas ainda há como direcionar corretamente essa onipresença da tecnologia, fazendo com que funcione a favor do bem-estar humano. Por isso é fundamental que, mesmo com o crescimento ilimitado de produtos/serviços tecnológicos, inundando nossas rotinas e mentes, o desenvolvimento dessas novas tecnologias seja feito com foco no ser humano, este considerado de forma holística, em todas as suas facetas: física, mental e social.

1.3. Modelo de pesquisa predominante

O modelo de pesquisa predominante será o de resolução de problema, uma vez que esta pesquisa se volta para a elaboração de modelos que poderão ser utilizados por empresas para uma análise mais robusta de riscos, considerando o desenvolvimento de novos produtos tecnológicos, atendendo a um só tempo a requisitos legais, econômicos, culturais e sociais.

2. Quesitos, fontes de pesquisa e formas de acesso

2.1. Quesitos referentes à contextualização fática

- Quais metodologias são utilizadas para as análises de riscos relacionados à privacidade, proteção de dados e segurança da informação por empresas de tecnologia? Em quais premissas de análise de riscos as empresas têm se baseado para atingir o resultado esperado pela matriz de riscos?
- Como esses riscos são identificados, analisados, mensurados, classificados e mitigados? Qual o grau de efetividade atingido com as análises de riscos, considerando o apetite de risco das empresas e os impactos dos riscos residuais?
- Como a análise de riscos baseada em premissas que considerem a privacidade, a proteção de dados e a segurança da informação de maneira central e desde a concepção do projeto/produto pode impactar no desenvolvimento de novas tecnologias?
- Considerando as abordagens até hoje desenvolvidas para fins de criação de legislações sobre privacidade e proteção de dados (i. Risco, ii. Risco e Benefícios; iii. Direitos; iv. Direitos e Riscos), como elas poderiam se comunicar trazendo uma nova abordagem em um contexto mais amplo, que considerasse os três elementos (riscos, benefícios e direitos) para fins de análise e ponderação relacionados à privacidade e à proteção de dados?
- Quais impactos sociais, culturais, legais e econômicos podem advir de uma

nova abordagem relacionada às premissas de privacidade e segurança na análise de riscos?

Principais fontes de pesquisa: doutrina e publicações de artigos nacionais e internacionais.

2.2. Quesitos de referencial teórico-normativo

- Considerando que a LGPD é uma lei baseada em riscos, haveria espaço para avaliar qual abordagem/metodologia seria a mais adequada ao cenário brasileiro (Risco; Risco e Benefício; Direitos; Direitos e Riscos)?
- Como as recomendações de mitigação de riscos previstas na LGPD podem auxiliar na elaboração de matrizes de riscos e frameworks mais robustos e efetivos em termos de segurança da informação, privacidade e proteção de dados?
- Quais frameworks e matrizes de riscos, nacionais e internacionais, podem ser considerados como referenciais para uma adequada análise de riscos, sob a perspectiva da legislação brasileira de proteção de dados?
- Existem decisões administrativas, judiciais ou jurisprudência – nacional e internacional - para embasar a necessidade de se pensar em uma nova abordagem de riscos envolvendo a privacidade, a proteção de dados e a segurança da informação?

Principais fontes de pesquisa: legislação nacional e internacional de privacidade, proteção de dados pessoais, em especial a LGPD e o GDPR; doutrina e publicações de artigos nacionais e internacionais; guias orientativos da Autoridade Nacional de Proteção de Dados (ANPD) e de Autoridades Internacionais, *como Information Commissioner´s Office* (ICO) e AEPD (*Agencia Española de Protección de Datos*); artigos de entidades internacionalmente reconhecidas, como a *International Association of Privacy Professionals* (IAPP); frameworks de organismos internacionais, como CNIL, NIST e ISO; decisões e pareceres de autoridades de proteção de dados da União Europeia e da Autoridade Nacional de Proteção de Dados (ANPD); e jurisprudência nacional e internacional relacionadas ao tema.

2.3. Quesitos referentes a abordagem analítica

- Quais são os principais desafios que as empresas de tecnologia enfrentam no mapeamento e classificação de riscos? A abordagem desses riscos é voltada somente para riscos corporativos ou considera o titular como centro dessa análise de riscos?
- Como as empresas de tecnologia podem se valer de frameworks e matrizes de riscos mais efetivos, considerando análises que considerem os direitos

relacionados à privacidade dos titulares, o custo-benefício para o negócio e o aumento de competitividade?

- Como alinhar as necessidades de inovação e desenvolvimento de novas tecnologias aos requisitos de privacidade, proteção de dados e segurança da informação previstos nas legislações – nacionais e internacionais - cada vez mais rígidas?

Principais fontes de pesquisa: legislação nacional e internacional de privacidade, proteção de dados pessoais, em especial a LGPD e o GDPR; doutrina e publicações de artigos nacionais e internacionais; guias orientativos da Autoridade Nacional de Proteção de Dados (ANPD) e de Autoridades Internacionais, como *Information Commissioner´s Office* (ICO) e AEPD (*Agencia Española de Protección de Datos*); artigos de entidades internacionalmente reconhecidas, como a *International Association of Privacy Professionals* (IAPP); decisões e pareceres de autoridades de proteção de dados da União Europeia e da Autoridade Nacional de Proteção de Dados (ANPD); e jurisprudência nacional e internacional relacionadas ao tema.

2.4. Recomendações finais

- O projeto tem por objetivo demonstrar que o desenvolvimento de novas tecnologias tendo como premissas o *Privacy by Design*, *o Security by Design* e o *Human Centered AI* não apenas é mais ético e justo para a sociedade como também possui um maior custo-benefício econômico para as empresas e organizações, sendo um diferencial competitivo de alta relevância no mercado atual.

- Este projeto irá analisar as metodologias até hoje desenvolvidas, considerando as abordagens baseadas em i. Risco, ii. Risco e Benefícios; iii. Direitos; iv. Direitos e Riscos, entendendo se estas são suficientes ou se há espaço para uma nova abordagem considerando uma intersecção entre os três elementos (riscos, benefícios e direitos).

- Os entregáveis finais serão documentos-modelo consistentes em frameworks e matrizes de risco a serem utilizadas como padrão para a análise de novos produtos em empresas que desenvolvam tecnologias, especialmente as que utilizem inteligência artificial.

3. Relevância prática, caráter inovador e potencial de impacto

Atualmente o mercado de tecnologia é essencialmente direcionado ao tratamento de um número ilimitado de dados. Todavia, as medidas de proteção e segurança desses dados não acompanharam esse crescimento exponencial de dados tratados. Assim, embora haja esforços globais no sentido de se garantir uma legislação protetiva em relação ao tratamento de dados pessoais, bem como esforços para o desenvolvimento de medidas técnicas adequadas à

segurança da informação, na prática ainda estamos muito aquém de uma garantia efetiva da privacidade.

Em relação ao caráter inovador, embora existam artigos, doutrina e trabalhos publicados voltados para este tema, não foi identificado um trabalho que se proponha a fazer uma abordagem prática destinada à criação de documentos-modelo efetivos de matrizes de riscos e frameworks focados, concomitantemente, nas premissas de *Privacy by Design*, S*ecurity by Design* e *Human Centered AI*, e considerando como plano de fundo a análise de custo-benefício econômico e de competitividade para as empresas de tecnologia.

Quanto ao potencial impacto do trabalho, os entregáveis poderão servir como modelos a serem adotados pelas empresas de tecnologia no desenvolvimento de novos produtos/serviços, garantindo maior segurança aos titulares de dados/consumidores e promovendo um posicionamento mais competitivo das empresas no mercado, impactando a um só tempo a economia e a sociedade.

4. Familiaridade com objeto da pesquisa

Atuo na área de Privacidade e Proteção de Dados desde 2020, quando assumi o papel de PMO do Projeto de Adequação à LGPD em uma empresa multinacional. Por ocasião desta atuação, tive a oportunidade de avaliar diversos projetos de tecnologia sob o ponto de vista do *Privacy by Design*, avaliando os riscos dos projetos e atuando de forma preventiva na redução desses riscos relacionados à privacidade e proteção de dados.

Em 2021 assumi a posição de DPO (*Data Protection Officer*) no Sebrae SP, onde tive a oportunidade de conduzir o projeto de adequação à LGPD da entidade desde o início, contemplando iniciativas para engajamento da alta direção, elaboração de Políticas e procedimentos internos, treinamento e conscientização de colaboradores, revisão de contratos, dentre outros.

Ainda no Sebrae, umas das atuações mais importantes durante a minha gestão foi a liderança do *squad* de Transformação Digital, que possibilitou a automação de diversos processos manuais, com desenho de fluxos e análise de ferramentas desde a concepção dos projetos, considerando premissas relacionadas ao *Privacy by Design* e *Security by Design*. Essa atuação prática possibilitou um enorme aprendizado em termos de projetos envolvendo tecnologia e aguçou ainda mais a minha visão sobre a importância da análise de riscos pautada nas premissas objeto deste trabalho.

Por fim, possuo certificações internacionais na área de privacidade de dados, como CIPM – IAPP- *Certified Information Privacy Manager* (CIPM), CDPO – IAPP – *Certified Data Protection Officer* e EXIN - DPO.

5. Bibliografia preliminar

SHNEIDERMAN, BEN. *HUMAN-CENTERED AI.* English edition. Maryland: Oxford University Press, USA, 2022.

ICO (INFORMATION COMMISSIONER'S OFFICE). Privacy-enhancing technologies (PETs): Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance, 2022. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/09/ico-publishes-guidance-on-privacy-enhancing-technologies/. Acessado em 15.07.2023.

MALINA, Lukas; SRIVASTAVA, Gautam; DZURENDA, Petr; HAJNY, Jan Hajny; RICCI, Sara. A Privacy-Enhancing Framework for Internet of Things Services, 2019.

Cha, S.C., Hsu, T.Y., Xiang, Y., Yeh, K.H.: Privacy enhancing technologies in the internet of things: Perspectives and challenges. IEEE Internet of Things Journal, 2018.

Trask A. in Lunar Ventures (Lundy-Bryan L.) 2021 Privacy Enhancing Technologies: Part 2—the coming age of collaborative computing. Disponível em: https://www.kisacoresearch.com/sites/default/files/documents/pet_white_paper_part_2_-_the_coming_age_of_collaborative_computing10992.pdf, 2022. Acessado em 15.07.2023.

EUROPEAN DATA PROTECTION SUPERVISOR. Accountability on the ground Part I: Records, Registers and when to do Data Protection Impact Assessments, 2019. Disponível em: https://edps.europa.eu/sites/edp/files/publication/19-07-17_accountability_on_the_ground_part_i_en.pdf. Acessado em 13.11.2023

FUTURE OF PRIVACY FORUM. City of Seattle Open Data Risk Assessment. Disponível em https://fpf.org/wp-content/uploads/2017/08/FPF-Seattle-Open-Data-Report_Proposed-Draft-August-2017.pdf

EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation (case 2020-0066). Disponível em https://edps.europa.eu/sites/edp/files/publication/20-07-06_edps_dpias_survey_en.pdf . Acessado em 08.11.2023.

BERKMAN KLEIN CENTER. Principled Artificial Intelligence. Mapping consensus in ethical and rights-based approaches to principles for AI. Disponível em https://cyber.harvard.edu/publication/2020/principled-ai. Acessado em 08.11.2023

GOMES, Maria Cecilia Oliveira. Entre o método e a complexidade: compreendendo a noção de risco na LGPD, 2020. Disponível em https://www.academia.edu/44022945/Entre_o_m%C3%A9todo_e_a_complexidade_compreendendo_a_no%C3%A7%C3%A3o_de_risco_na_LGPD. Acessado em 16.10.2023.

CNIL. Privacy Impact Assessment (PIA). Disponível em https://www.cnil.fr/en/privacy-impact-assessment-pia. Acessado em 25.10.2023.

ICO. Data protection impact assessments. Disponível em https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/. Acessado em 25.10.2023.

LAPIN. AVALIAÇÃO DE IMPACTO ALGORÍTMICO PARA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS. Disponível em https://lapin.org.br/2023/04/13/avaliacao-de-impacto-algoritmico-para-protecao-dos-direitos-fundamentais/. Acessado em 08.11.2023.

GOMES, Maria Cecilia Oliveira. Políticas públicas e o relatório de impacto à proteção de dados: análise do caso do aplicativo NHS COVID-19, 2022. Disponível em https://www.academia.edu/83908668/Poli ticas pu blicas e o relato rio de impacto a prot ec a o de dados ana lise do caso do aplicativo NHS COVID 19. Acessado em 08.11.2023.

6. Cronograma de Execução

	2023						2024												2025		
Atividade	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	...	Horas
Entrega do Projeto de Pesquisa																					120
Atribuição do Orientador																					N/A
Revisão e Leitura Bibliográfica																					200
Estruturação do Sumário																					20
Redação																					250
Validação do Orientador																					40
Revisão da Redação																					120
Versão Preliminar																					N/A
Revisão da Versão Preliminar																					60
Versão Intermediária																					N/A
Revisão da Versão Intermediária																					60
Versão Provisória (V.P)																					N/A
Banca de Qualificação (B.Q)																				Até 45d após V.P	N/A
Versão Definitiva (V.D)																				Até 90d após B.Q	60
Banca Final																				Até 60d após V.D	N/A