FGV DIREITO SP
MESTRADO PROFISSIONAL

Análise Comparativa de Metodologias para Avaliação de Riscos nos Processos de Elaboração de Relatórios de Impacto à Proteção de Dados Pessoais

Henrique Fabretti Moraes

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

Versão final – 13.10.2022

1. Tema, contexto e delimitação de escopo

Tema:

Este trabalho de pesquisa visa responder a seguinte pergunta: "Qual é a melhor metodologia para avaliação dos riscos às liberdades e garantias fundamentais dos titulares de dados, dentro do escopo de um relatório de impacto à proteção de dados pessoais, considerando o cenário jurídico-regulatório brasileiro?",

Contexto e delimitação de escopo:

A noção de risco e formas de mitigá-lo frente o tratamento de dados pessoais é elemento presente desde as primeiras leis de privacidade e proteção de dados[1], que foram sofisticando os conceitos de regulação baseada em risco até chegarmos no modelo atualmente adotado pela Lei Geral de Proteção de Dados (LGPD) que, por sua vez, foi inspirado no texto - à época, ainda no início do processo legislativo - do Regulamento Geral sobre a Proteção de Dados da União Europeia (RGPD).

No modelo adotado por estas regulações, os agentes envolvidos em uma atividade de tratamento de dados pessoais ficam obrigados a prevenir e mitigar riscos que suas ações podem impor aos indivíduos titulares destes dados. Mais do que isso, tanto o RGPD quanto a LGPD adotaram como um dos princípios que devem permear toda atividade de tratamento de dados o do accountability[2], o que significa que os agentes de tratamento devem estar aptos a comprovar a conformidade com a legislação, o que implica, consequentemente, demonstrar que identificaram, mitigaram e prevenirem riscos advindos da operação de tratamento de dados realizada[3].

---

[1] GOMES, Maria Cecilia Oliveira. Relatório de Impacto à proteção de dados: Uma breve análise de sua definição e papel na LGPD. Revista do Advogado, São Paulo, n. 144, p. 6-15, nov. 2019.

[2] Na LGPD, o princípio do *accountability* está disposto no art. 6º, X e no RGPD, no art. 5(2).

[3] VOIGT, Paul. BUSSCHE, Axel von dem. *The EU General Data Protection Regulation (GDPR): A practical guide.* Switzerland: Springer, 2017. Pg. 31.

Para tanto, os reguladores introduziram as avaliações de risco de privacidade, primeiramente como mera recomendação na Diretiva 95/46/EC[4] e tornado obrigatório com a aprovação do RGPD, onde ganhou termo técnico próprio *Data Protection Impact Assessment* (ou relatório de impacto à proteção de dados pessoais – RIPD[5]).

Por meio deste mecanismo, o agente de tratamento[6] é obrigado a documentar que avaliou os riscos às garantias e direitos fundamentais dos indivíduos impactados pelas atividades de tratamento de dados (titulares de dados) que pretende ou pretendia realizar e implementou medidas para reduzir ou mitigar estes riscos.

Entretanto, o texto do RGPD se limita a identificar a regra para a elaboração mandatória do RIPD, bem como seu conteúdo mínimo e as autoridades europeias de proteção de dados complementaram tais disposições com exemplos de atividades de tratamento que devem ser precedidas da elaboração deste documento, *templates* e diretrizes gerais sobre o tema sempre com o intuito de orientar os agentes de tratamento a cumprirem corretamente com esta obrigação legal o que implica, logicamente, avaliarem corretamente os riscos que suas atividades impõe aos titulares de dados.

Como mencionado anteriormente, a parte fundamental do relatório de impacto é, justamente, avaliar quais riscos uma determinada atividade de tratamento de dados pode acarretar às liberdades e garantias fundamentais dos titulares de dados. Para elaborar corretamente esta avaliação, o agente de tratamento deve executar algumas etapas que dizem respeito a análise do risco em sentido estrito, tais como:

- que tipos de ameaças devem ser levadas em consideração (ou seja, devem ser consideradas como um risco);
- critérios para mensurar o nível de risco;
- identificação da probabilidade do risco se materializar e impacto que o risco pode causar, caso materializado;
- balanceamento entre as ameaças e benefícios trazidos pela atividade de tratamento;
- identificação de possíveis medidas para eliminação ou mitigação dos riscos identificados e 'quanto' estas medidas reduzem da probabilidade e do impacto; e
- avaliação se o risco residual (risco restante após a aplicação das medidas de mitigação) impede ou não a atividade de tratamento de ser realizada.

Por exemplo, uma categoria de risco tipicamente levada em consideração em um relatório de impacto é o risco do dado ser alvo de um 'ataque hacker' e ser indevidamente acessado por um terceiro não autorizado com intenções maliciosas, como a de praticar fraudes financeiras. Ao identificar que este evento pode ocorrer a uma determinada atividade de tratamento, o agente de tratamento deve indicar, por exemplo, se a probabilidade do evento ocorrer é alta, média ou baixa. Se for alta, preferencialmente adotar medidas de segurança, que reduzam a probabilidade do risco se materializar.

Ocorre que inexiste diretrizes claras sobre como esta etapa da avaliação deve ser conduzida, muito menos trazem definições em como mensurar, por exemplo, se a probabilidade

---

[4] Norma que precedeu o RGPD, em que pese possuía natureza jurídica diversa, por ser uma diretiva e não uma regulação.

[5] Conforme definido pelo art. 5º, XVII, da LGPD.

[6] Aqui considerada uma acepção mais abrangente do termo, como sendo a entidade que trata dados pessoais e está sujeita à regulação de proteção de dados.

de determinado risco se materializar é baixa, média ou alta, deixando tal incumbência aos agentes de tratamento o que, por sua vez, abre espaço para divergências de interpretação e da subjetividade da entidade que avalia o risco, seja ela o regulador, Poder Judiciário ou o próprio agente de tratamento.

Nesta linha, por meio da modalidade preponderante de resolução de problemas, esta pesquisa visa comparar as diferentes metodologias empregadas pelos agentes de tratamento e autoridades reguladores na análise dos riscos às liberdades e garantias fundamentais, quando da elaboração de RIPDs, para apontar aquela que melhor se adapta à realidade regulatória brasileira, reduzindo a subjetividade do processo de análise de riscos e tornando tal atividade mais eficiente[7].

2. **Quesitos, fontes de pesquisa e formas de acesso**

Quesitos referentes à contextualização fática:

- O que é regulação baseada em risco?
- Por qual motivo as regulações modernas de proteção de dados tendem a ser baseadas em risco?
- Qual a importância do princípio de *accountability* previstos nas normas de proteção de dados baseadas em risco?

Principais fontes: doutrina nacional e internacional.

Quesitos referentes ao referencial teórico-normativo:

- Quais mecanismos foram adotados pela LGPD para assegurar a eficácia da gestão de riscos realizadas pelos agentes de tratamento de dados?
- Qual o papel do RIPD na demonstração da efetividade da gestão de riscos pelos agentes de tratamento na conformidade com a LGPD?
- Quais elementos devem constar em um RIPD para efetiva demonstração de gestão de riscos pelo agente de tratamento?

Principais fontes: legislação nacional e internacional sobre proteção de dados pessoais, em especial o RGPD e a LGPD; doutrina nacional e internacional; guias orientativos e pareceres de autoridades de proteção de dados da União Europeia e da Autoridade Nacional de Proteção de Dados (ANPD).

Quesitos referentes a abordagem analítica:

[7] Eficiência aqui traduzida como: menor insegurança jurídica, maior precisão na identificação e quantificação dos riscos advindos da atividade de tratamento e menor uso de recursos (de tempo e financeiros) do agente de tratamento na condução desta atividade).

- Como os agentes de tratamento de dados pessoais definem quais são os riscos que devem ser mapeados em seus RIPDs?
- Quais são as categorias de riscos usualmente avaliadas nos RIPDs?
- Como é mensurada a probabilidade e o impacto destes riscos?
- Como as autoridades de proteção de dados analisam e criticam os RIPDs elaboradores pelos agentes de tratamento e, em última instância, quantificam os riscos identificados?

Principais fontes: doutrina nacional e internacional; guias orientativos, pareceres e decisões administrativas de autoridades de proteção de dados da União Europeia e da Autoridade Nacional de Proteção de Dados (ANPD); *frameworks* de gestão de riscos, tais como o COSO ERM 2004 e as normas ISO/IEC 31000 e 29134; e RIPDs que tenham sido elaborados e disponibilizados publicamente por entidades de reconhecida credibilidade.

Recomendações finais:

- Qual a melhor metodologia para identificar as categorias de riscos que devem constar em um RIPD e quantificar a probabilidade e o impacto destes riscos?

Produto:

- *Framework* para identificação e quantificação de riscos avaliados por meio de um RIPD.

3. **Relevância prática, caráter inovador e potencial de impacto**

Como mencionado na contextualização da pesquisa, relatórios de impacto à proteção de dados pessoais são instrumentos indispensáveis para a demonstração da avaliação de riscos realizada frente a uma determinada atividade de tratamento e, consequentemente, da própria conformidade com a LGPD. Assim, qualquer agente de tratamento, seja ele público ou privado, dificilmente escapará à necessidade de elaboração deste documento. Tamanha é a importância do tema, que a Autoridade Nacional de Proteção de Dados inseriu a regulação sobre os RIPDs em sua agenda regulatória como um dos primeiros temas a ser abordado[8], bem como nas ainda escassas análises de casos práticos, a autoridade solicitou ou analisou os relatórios de impacto elaborados pelos agentes de tratamento envolvidos no procedimento administrativo[9].

Assim, dificilmente uma atividade de tratamento de dados pessoais que apresente um nível maior de sofisticação e complexidade poderá existir (em conformidade com a LGPD) sem que um RIPD a tenha precedido, o que demonstra a relevância prática do tema objeto da pesquisa.

[8] Vide Portaria nº 11, de 27 de janeiro de 2021, da Autoridade Nacional de Proteção de Dados.

[9] Em suma, a ANPD publicou, até o momento, notas técnicas referentes à análise da política de privacidade do WhatsApp, ao produto *Data Valid* comercializado pela Serpro e ao compartilhamento de dados sobre o ENEM pelo INEP, onde indica ter solicitado e/ou analisado o relatório de impacto das atividades de tratamento sob análise.

Quanto ao caráter inovador, em que pese existam pesquisas e obras dedicadas a explicarem as noções de risco, práticas para gestão de riscos em privacidade e proteção de dados em sentido amplo, *templates* e manuais para elaboração deste documento, não identificamos nenhum trabalho que se proponha a comparar as diferentes metodologias de avaliação de riscos e identificar aquela que seja mais eficiente, menos subjetiva e melhor se adapte ao contexto regulatório europeu e, muito menos brasileiro.

Por fim, quanto ao potencial de impacto do trabalho pretendido, dada a relevância do tema e a dificuldade que se percebe do mercado de tornar objetiva as avaliações de risco em privacidade e proteção de dados, o resultado desta pesquisa poderá servir de norte a todos os profissionais que atuam na área de privacidade e proteção de dados, à entidades setoriais no desenvolvimento de seus códigos de conduta e aos entes reguladores em seus processos de regulação e fiscalização, uma vez ser de interesse de todos enxugar a subjetividade do processo, aumentando a segurança jurídica destas avaliações.

4. **Familiaridade com objeto da pesquisa**

Atuo com a prática de privacidade e proteção de dados desde 2016, quando assumi a função de responsável pelo programa de *compliance* em privacidade e proteção de dados de uma empresa multinacional americana, onde parte de minha atividade era avaliar os riscos de atividades de tratamento de dados.

Desde então, conduzi e supervisionei a elaboração de dezenas de relatórios de impacto à proteção de dados pessoais e desenvolvi alguns *frameworks* para auditorias e avalições de riscos de privacidade em organizações sujeitas à aplicação da Lei Geral de Proteção de Dados e sou sócio responsável pela área de privacidade e proteção de dados de um dos mais reconhecidos escritório de direito digital do país, onde tenho a oportunidade de atender diversos clientes que exigem a análise de risco de situações práticas.

Adicionalmente, possuo algumas certificações de reconhecimento global na área, dentre elas a *Certified Information Privacy Manager* (CIPM) e a *Certified Data Privacy Solutions Engineer* (CDPSE), que exigem conhecimento na avaliação de riscos de privacidade.

5. **Bibliografia preliminar**

BINNS, REUBEN. “Data Protection Impact Assessments: a meta-regulatory approach.” In International Data Privacy Law, v. 7, n. 1, 2017.

GELLERT, RAPHAËL. “Understanding the notion of risk in the General Data Protection Regulation.” In: Computer Law & Security Review: The International Journal of Technology Law and Practice (2017).

GELLERT, RAPHAËL. *Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk*. Tese (Doutorado). Faculteit Recht en Criminologie, Vrije Universiteit Brussel, 2017.

QUELLE, CLAUDIA. *The Data Protection Impact Assessment, or: How the General Data Protection Regulation May Still Come to Foster Ethically Responsible Data Processing* (November 25, 2015).

QUELLE, CLAUDIA. "Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach." In European Journal of Risk Regulation. Vol. 9:3, 2018.

BISZTRAY, TAMAS. GRUSCHKA, NILS. "Privacy Impact Assessment: Comparing methodologies with a focus on practicality." Em: 2019 Nordic Conference on Secure IT Systems (NORDSEC). 2021.

BISZTRAY, TAMAS. GRUSCHKA, NILS. "Privacy Impact Assessment: Comparing methodologies with a focus on practicality." Em: 2019 Nordic Conference on Secure IT Systems (NORDSEC). 2021.

6. **Cronograma de execução**

Atividade	*jun/22*	*jul/22*	*ago/22*	*set/22*	*out/22*	*nov/22*	*dez/22*	*jan/23*	*fev/23*	*mar/23*	*abr/23*	*mai/23*	*jun/23*	*jul/23*	*Horas*
Revisão bibliogrática	12	12	12	12	12	12	6								78
Identificação das principais regulações no mundo que tratam sobre avalições de risco em privacidade	4	4	4												12
Identificação dos principais frameworks e normas empregadas pelos agentes de tratamento para avaliação de riscos de privacidade				4	4	4									12
Coleta e análise de decisões emitidas por autoridades reguladoras sobre a análise de risco de privacidade conduzida por agentes de tratamento							5	8	8	8					29
Coleta e análise de relatórios de impacto à proteção de dados elaborados por agentes de tratamento							5	8	8	8					29
Elaboração do trabalho	5	5	5	5	5	5	5	5	5	5	20	20	20		110
Revisão do trabalho														30	30