UNIVERSIDADE SALVADOR – UNIFACS
ESCOLA DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE DIREITO

OCTÁVIO SANTOS DE OLIVEIRA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD): UMA ANÁLISE SOBRE A IMPORTÂNCIA NA GESTÃO DE RISCOS E PROTEÇÃO DE DADOS PESSOAIS

Feira de Santana
2023

OCTÁVIO SANTOS DE OLIVEIRA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD): UMA ANÁLISE SOBRE A IMPORTÂNCIA NA GESTÃO DE RISCOS E PROTEÇÃO DE DADOS PESSOAIS

Artigo científico apresentado à matéria de TCC II, como trabalho de conclusão de curso, do curso de graduação em Direito da Universidade Salvador – UNIFACS, sendo requisito parcial para aprovação e obtenção do título de Bacharel em Direito.

Orientador: Prof. Diego Carneiro Costa, Me.

Feira de Santana

2023

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD): UMA ANÁLISE SOBRE A IMPORTÂNCIA NA GESTÃO DE RISCOS E PROTEÇÃO DE DADOS PESSOAIS

DATA PROTECTION IMPACT ASSESSMENT (RIPD): AN ANALYSIS ABOUT THE IMPORTANCE IN RISK MANAGEMENT AND PERSONAL DATA PROTECTION

Autor: Octávio Santos de Oliveira[1]
Orientador: Prof. Diego Carneiro Costa, Me.[2]

Resumo: O presente artigo tem como finalidade apresentar uma análise qualitativa de importância sobre o Relatório de Impacto à Proteção de Dados (RIPD) para a gestão de riscos e o tratamento e a proteção de dados pessoais, fazendo a sua contextualização e histórico internacional, utilizando-se como técnica metodológica de pesquisa a análise exploratória e analítica dos dispositivos legais com enfoque na Lei Geral de Proteção de Dados (LGPD) e a análise de artigos científicos e pesquisas, fazendo correlações afim de que sejam demonstrados tanto a importância da ferramenta como os possíveis riscos à proteção de dados que podem decorrer da não elaboração e/ou da inutilização do RIPD, pontuando-se os ganhos que podem ser obtidos quando da sua utilização.

Palavras-chave: Gestão de riscos. Proteção de dados pessoais. LGPD. RIPD.

Abstract: This article aims to present a qualitative analysis of the importance of the Data Protection Impact Report (RIPD) for risk management and the processing and protection of personal data, contextualizing it and bringing its international historic, using exploratory analysis as the methodological research technique and analysis of legal provisions with focus on the General Data Protection Law (LGPD) and the analysis of scientific articles and researches, making correlations in order to demonstrate both the importance of the tool and the possible risks to data protection that may arise from not preparing and/or neglecting the RIPD, punctuating the gains that can be obtained when using the tool.

Keywords: Risk management. Personal data protection. LGPD. RIPD.

[1] Acadêmico do 10º semestre, concluinte do curso de Direito da Universidade Salvador – UNIFACS, de Feira de Santana - BA. E-mail: octavioliveira18@hotmail.com

[2] Mestre em Direito pela Universidade Federal da Bahia. Pesquisador do Grupo de Pesquisa "Autonomia e Direito Civil contemporâneo" e do "Grupo de Estudos Trabalho Vivo", na Universidade Federal da Bahia. Professor de Direito da Universidade Salvador – UNIFACS. Analista Judiciário no Tribunal Regional do Trabalho da 5ª Região. E-mail: diegcost@gmail.com

SUMÁRIO

1. INTRODUÇÃO

Hoje entende-se que tratar e gerenciar dados pessoais com foco na proteção deixou de ser apenas uma opção pouco explorada, passando a ser uma obrigação a ser seguida à risca. Atualmente, com regras importantes sobre meios adequados para se fazer o trâmite dos dados e proteger os indivíduos, os agentes 'tratadores dos dados' dispõem de um documento chamado "relatório de impacto à proteção de dados", disposto no art. 5º, XVII da Lei nº 13.709/2018, a LGPD, que nada mais é que uma importante ferramenta aliada às organizações que trabalham com o tratamento de dados pessoais e que visa, junto com os outros dispositivos da norma, proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Deste modo, dentre as várias nuances da multifacetada Lei Geral de Proteção de Dados Pessoais, destacam-se aqueles pontos em que a lei parte para a ação no quesito de instituir novos métodos que corroborem para o ideal tratamento dos dados e que possam garantir que se está adotando as melhores formas de governança para trazer segurança aos indivíduos que têm os seus dados pessoais coletados e processados. Assim, temos como uma importante ferramenta o próprio Relatório de Impacto à Proteção de Dados (RIPD), que em acordo com a LGPD, no seu art. 5º, XVII, tem como objetivo descrever os 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 quando do tratamento desses dados.

Com a promulgação da LGPD, surgiram muitas dúvidas de como seria a real aplicação e a real importância dos dispositivos da norma. Considerando isso e partindo do pressuposto geral, em que boa parcela da sociedade ainda têm um conhecimento escasso de parte da legislação de proteção de dados, entende-se ser necessária a elaboração de um estudo analítico profundo que vise demonstrar a importância da indispensável ferramenta de gestão que auxilia os atores (controladores, operadores e encarregados), dispostos na Lei, a tomar melhores decisões e gerir os possíveis riscos advindos da atividade de coleta, processamento, armazenamento e utilização dos dados pessoais.

A escolha do tema se justifica na inferência de que este ainda é um assunto

pouco tratado, haja vista que ainda não há uma obrigação explícita para que as empresas adotem a elaboração do RIPD, documento este que se mostra ser de extrema importância e pode ser uma ferramenta formidável de análise de riscos e proteção contra ataques que possam gerar um perigo às organizações que atuam com o tratamento e processamento de dados pessoais.

Desta forma, cabe aqui fazer a indicação de que no decorrer do artigo serão apresentadas as mais diversas opiniões sobre o tema em comento, fazendo a sua contextualização nacional e internacional, a correlação com outras ferramentas de gestão de riscos conhecidas no universo organizacional do ponto de vista da gestão de riscos, bem como a indicação dos benefícios que podem ser obtidos quando há a correta implantação e utilização do RIPD, considerando ser esta uma ferramenta importante que não deve ser utilizada por conta do simples cumprimento de previsão legal, sendo que há perdas em potencial quando da sua inutilização ou não implantação.

Sendo assim, e, considerando-se a relevância do tema a ser abordado, o presente artigo tem como problema de pesquisa buscar responder qual é a importância da elaboração do Relatório de Impacto à Proteção de Dados (RIPD) para a gestão de riscos, tratamento e proteção dos dados pessoais no Brasil, e, para tanto, o objetivo deste é analisar à luz da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), a disposição da ferramenta e a sua importância no contexto da gestão de riscos, do tratamento e da proteção de dados pessoais dos indivíduos.

Neste sentido, tem-se como hipótese que o RIPD tem um importante papel na proteção dos dados pessoais e da privacidade dos indivíduos, visto que o relatório, além de ser necessário do ponto de vista legal para determinadas empresas, colabora com a promoção da transparência e promoção dos direitos e garantias fundamentais, sendo que permite que as empresas que adotam a sua elaboração identifiquem e mitiguem potenciais riscos (ou riscos já existentes) a estes dados pessoais, contribuindo assim com a difusão da LGPD e suas ferramentas e beneficiando os variados segmentos da sociedade como um todo.

2. METODOLOGIA DA PESQUISA

O presente artigo tem como técnica metodológica de pesquisa a análise exploratória e analítica dos dispositivos legais com enfoque na Lei Geral de Proteção de Dados (LGPD) e a análise de artigos científicos e pesquisas, fazendo correlações do objeto de estudo com outros aspectos julgados importantes ao pleno entendimento da ferramenta ora analisada, sob a perspectiva interdisciplinar e multisetorial, por meio da pesquisa documental e bibliográfica no acervo disponível nos mais variados meios de comunicação e difusão de informações sobre a temática do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e ferramentas correlatas à luz dos costumes e da legislação brasileira e sua respectiva doutrina como principal fonte de embasamento teórico, tendo como ramificação do direito a ser utilizado o direito digital.

3. BREVE CONTEXTUALIZAÇÃO DA LGPD E PREVISÃO LEGAL DO RIPD

A Lei Geral de Proteção de Dados – LGPD, que foi promulgada em 14 de agosto de 2018 pelo ex-presidente Michel Temer é uma lei técnica, mas que, em sua essência, é uma lei protetiva que visa tutelar direitos fundamentais dos cidadãos já que, segundo Pinheiro (2021, pg. 19), ela “[...] reúne uma série de itens de controle para assegurar o cumprimento das garantias previstas cujo lastro se funda na proteção dos direitos humanos”. Sendo assim, é, portanto, uma lei aplicável tanto ao âmbito público como privado que fala sobre o “[...] tratamento de dados pessoais, inclusive nos meios digitais [...]” (BRASIL, 2018, art. 1º), destacando-se:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Em vista de uma das principais finalidades da LGPD, que é de ser uma lei que visa tutelar e garantir os direitos fundamentais dos indivíduos, como disposto no *hall* de incisos do art. 5º da CRFB/88, há de se pôr em comento que o tema "proteção de dados" como sendo um direito fundamental já vinha sendo discutido há anos no Brasil, precedendo a criação da lei, como previamente informado por Doneda:

> (...) No panorama do ordenamento brasileiro, o reconhecimento da proteção de dados como um direito autônomo e fundamental não deriva de uma dicção explícita e literal, porém da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais de igualdade substancial, liberdade e dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada. (DONEDA, 2011 pg. 103)

Deste modo, pontua-se que:

> A LGPD foi um marco na legislação brasileira, pois foi o primeiro instrumento legal inteiramente dedicado a regulamentar as atividades envolvendo os dados pessoais, visto que outras legislações tratavam de forma tangenciada a temática. Ela consolida o uso protetivo e legal dos dados pessoais, assegurando os direitos fundamentais do indivíduo: o direito à privacidade e à liberdade. A partir dela e conhecendo a maneira como os dados pessoais são tratados no Brasil, diversas ilegalidades poderão ser barradas, adequando a coleta e tratamento de dados de acordo com a necessidade. (PRESTES et al., 2021 pg. 9)

Em comento, Pinheiro (2021, pg. 19) ainda nos traz que a LGPD "é uma regulamentação que traz princípios, direitos e obrigações relacionados ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas." Sendo assim, admite-se que com a utilização e aplicação de legislações internacionais no âmbito externo ao Brasil, que versavam sobre o tema, houve a necessidade de que se criasse e instituísse uma lei nacional para abranger estes aspectos tão importantes da vida em sociedade.

Em tempo, faz-se necessário entender o que significa dados pessoais e, também, dados pessoais sensíveis, que serão dois importantes objetos de discussão ao longo do artigo. Em acordo com o disposto no art. 5º, I e II, respectivamente, da LGPD, é:

> I - Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

> II - Dado pessoal sensível: 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; (BRASIL, 2018)

Assim sendo, urge salientar que apesar de ser uma lei brasileira que instituiu diversos avanços no tocante à proteção dos dados pessoais, a necessidade de criá-la não está diretamente ligada às necessidades brasileiras que fazem referência a esta questão. Gomes (2019) comenta que “antes da sanção da LGPD já existiam no Brasil mais de 40 normas setoriais de proteção de dados, como o Código de Defesa do Consumidor, Código Civil, Marco Civil da Internet, entre outros [...]”, porém, os principais propulsores da criação dessas legislações mundo afora são acontecimentos internacionais, e, no caso da LGPD do Brasil, mais especificamente a adoção de leis que tratam sobre o assunto na União Europeia, haja visto que:

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior do fluxo de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização. (PINHEIRO, 2021, pg. 23)

Neste sentido, e tendo como maior percussor da adoção da LGPD no Brasil a União Europeia, entende-se que o catalisador para que muitas nações começassem a adotar posturas mais rígidas no sentido de proteção de dados foi, em acordo com Pinheiro (2021, pg. 24), “[...] a promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados [...]”, sendo que:

> Este, por sua vez, ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDRP. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar. (PINHEIRO, 2021, pg. 24)

Em contexto, a criação do GDPR decorreu de um anseio popular por parte dos indivíduos da União Europeia como um todo, dado que:

> O regulamento foi criado como resposta a uma crescente exigência popular, com normas rígidas em relação aos dados que as pessoas disponibilizam para plataformas online. Isso porque são passadas informações como identidade, endereço, opiniões e características biológicas às organizações.
> Diante de tantos conteúdos disponíveis, é essencial responsabilizar as empresas quanto à segurança dessas informações. Assim, elas não vão ser divulgadas de forma indevida ou cair nas mãos de indivíduos mal-intencionados. É nesse contexto que a GDPR aparece como uma saída para proteger a população europeia. A norma vem como uma resposta aos anseios e às necessidades dos cidadãos, de maneira a garantir que a proteção de dados e a segurança sejam direitos das pessoas.
> Para tanto, a legislação estabelece regras rígidas às organizações de diversos tipos e portes. Como consequência, a coleta, o processamento e o armazenamento dos dados são regulamentados, o que contribui para resguardar a privacidade dos cidadãos. (GAEA, 2020)

Neste sentido, entende-se que a LGPD é uma lei baseada numa legislação internacional que também dispõe sobre o tema da proteção de dados, e, sabendo-se que é comum que o legislador, nas suas atribuições em função da formulação da lei nacional, tenha adequado meios e ferramentas dispostos na GDPR para que se espelhe e replique na legislação nacional, temos que o Relatório de Impacto à Proteção de Dados (RIPD) do Brasil, é, de certa forma, uma adaptação do Data Protection Impact Assessment (DPIA) disposto na GDPR europeia, sendo que ambos têm similaridade nos seus procedimentos de elaboração, são dotados de caráter fundamentalmente preventivo e visam dar mais transparência aos processos de coleta e tratamento de dados.

Assim sendo, a indicação do que é o relatório de impacto à proteção de dados está disposto no art. 5º, XVII da LGPD (2018), que diz que é a:

> (...) documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018)

Neste sentido, faz-se necessária a identificação do sujeito responsável pelo RIPD, qual seja: o controlador, que tem a sua definição no inciso VI, do artigo 5º da LGPD e é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;”. Em resumo, entende-se que é este o responsável tanto pela elaboração do RIPD como por tomar decisões sobre como se dará os métodos de gestão e prevenção de riscos relacionados às atividades com os dados pessoais, podendo esta tarefa ser atribuída tanto a uma pessoa física como para uma pessoa jurídica, ressaltando-se

que os entes de direito público também são abrangidos pelas necessidades impostas pela lei.

Mas em se tratando da correlação entre o DPIA presente na legislação de proteção de dados europeia e o RIPD da LGPD, os legisladores europeus foram ainda mais além no tocante às particularidades da ferramenta, incluindo de forma sistemática na legislação quais itens deverão ser obrigatoriamente adotados, no mínimo, quando da elaboração do DPIA, fato pelo qual os interessados em adotar o RIPD no Brasil deverão considerar utilizar como base o modelo europeu, que em acordo com o disposto no art. 35, item 7 do capítulo 4 da GDPR determina a informação de, pelo menos:

> A avaliação deve conter pelo menos:
>
> uma descrição sistemática das operações de tratamento previstas e das finalidades do tratamento, incluindo, se for caso disso, o interesse legítimo prosseguido pelo responsável pelo tratamento;
>
> uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação às finalidades;
>
> uma avaliação dos riscos para os direitos e liberdades das pessoas (...); e
> as medidas previstas para enfrentar os riscos, incluindo salvaguardas, medidas de segurança e mecanismos para garantir a proteção dos dados pessoais e para demonstrar o cumprimento do presente regulamento tendo em conta os direitos e interesses legítimos dos titulares dos dados e outras pessoas interessadas. (GDPR-INFO, 2018 - tradução livre)

Seguindo um padrão, e em acordo com o que preconiza o art. 38 da LGPD, que informa que poderá ser determinada a elaboração de um RIPD àqueles que tratem dados, mais recentemente o portal Gov.Br, na página destinada à Autoridade Nacional de Proteção de Dados (ANPD), por meio da sua agenda regulatória do biênio 2023/2024, estabeleceu por meio do seu sítio eletrônico, no campo de perguntas e respostas sobre o RIPD, no item 6, que os requisitos mínimos que devem estar contidos no RIPD são:

> Conforme o art. 38 da LGPD, o RIPD deverá conter, pelo menos:
>
> a) a descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma;
> b) a metodologia usada para o tratamento e para a garantia da segurança das informações; e
> c) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados. (GOV.BR - ANPD, 2023)

Considerando o disposto, Pinheiro (2021, pg. 82) pontua que o RIPD (também considerado na sua obra como DPIA) “é um documento muito importante como prova de conformidade para os agentes de tratamento de dados, lembrando que, (...)” segundo Braz Jr. (2019 apud. Pinheiro, 2021 pg. 82) “(...) o propósito de um DPIA não é eliminar todos os riscos, mas sim minimizar a existência destes, bem como verificar se os riscos remanescentes são justificáveis.”

Subentende-se ser primordial que se realize esta correlação de obrigatoriedade e pontos principais das ferramentas para que se tenha em mente que apesar de a LGPD apresentar menos incisividade quando da proposição da elaboração do RIPD, para que este seja realmente adotado, deve-se levar em consideração as boas práticas mais consolidadas que têm sido adotadas mundo afora afim de que se mantenha certo padrão (que por sinal é o esperado) de qualidade nos processos que envolvem dados que, por vezes, podem inclusive ser tratados fora do Brasil.

Neste diapasão e considerando que as atividades que envolvem dados pessoais são, por si só, uma atividade dotada de certo risco, informa Freitas (2022, pg. 230) que: “ao se ter por premissa que é impossível reduzir riscos à zero, independentemente da área de aplicação, há que se mitigar os riscos jurídicos e tecnológicos decorrentes do meio ambiente digital para se alcançar a proteção de dados pessoais e garantir direitos e liberdades dos titulares de dados”. Entende-se, portanto, que é de extrema importância a formulação do RIPD, tanto para ficar em dia com as possíveis obrigações junto à Autoridade Nacional de Proteção de Dados (ANPD), como para ter uma ferramenta de gestão importante e aliada à função de tratamento de dados.

4. O RIPD COMO (IMPORTANTE) FERRAMENTA DE GESTÃO, DE RISCOS E PROTEÇÃO DE DADOS PESSOAIS

A *priori*, o RIPD pode ser entendido como mais uma ferramenta burocrática recepcionada de uma legislação estrangeira e aplicada a determinadas empresas de forma a lhes incumbir mais um “ônus” sem que esta agregue nenhum valor real aos propósitos das companhias, visando apenas um senso de conformidade que faz alusão a uma realidade utópica de proteção de dados. Destarte isso, a real

importância e a aplicação prática e de valor da ferramenta podem ser deixadas de lado quando não entendida como uma ferramenta de gestão de riscos que pode elevar os ganhos e minimizar a possibilidade de intercorrências que podem ter a capacidade de gerar prejuízos às empresas e principalmente aos titulares dos dados. Como pontua Gomes:

> O relatório de impacto à proteção de dados não deve ser enxergado na LGPD como uma ferramenta burocrática, mas sim como uma documentação que reflete um processo de aprendizado por agentes de tratamento, que é o de realizar a governança de dados dentro de casa. (GOMES, 2019)

E informa, ainda, que:

> (...) A ideia do relatório de impacto é refletir uma avaliação de impacto, cuja base regulatória é a identificação de riscos, que pode ser realizada para propósitos diferentes, como: avaliar o impacto de incidentes de segurança; avaliar o impacto de novas tecnologias; avaliar o impacto de novos produtos que podem gerar riscos aos direitos dos titulares de dados etc. (GOMES, 2019)

Neste sentido é importante que se ressalte que a gestão de riscos deve ser adotada nas empresas independentemente de qualquer obrigatoriedade prevista em lei e não só pelo fato de ser algo que ajude no desenvolvimento das atividades da melhor maneira, mas também porque transmite aos consumidores a ideia de que os seus produtos e serviços são de qualidade e seguros. Segundo a Fia Business School:

> A gestão de risco é o conjunto de atividades coordenadas que têm o objetivo de gerenciar e controlar uma organização em relação a potenciais ameaças, seja qual for a sua manifestação. Isso implica no planejamento e uso dos recursos humanos e materiais para minimizar os riscos ou, então, tratá-los. É uma estratégia que envolve um trabalho preventivo de se antecipar a possíveis situações e considerar a prática como parte dos processos da empresa. (FIA Business School, 2018)

Sendo assim, é plausível pôr em comento que muito se fala no âmbito corporativo sobre como transmitir a ideia de qualidade e preocupação que se tem no desenvolvimento, manejo e aplicação das novas tecnologias e processos, tanto que por anos as corporações têm buscado mecanismos que auxiliem na gerência de riscos e mitigação de perdas, sendo que o RIPD passou a figurar como uma dessas

ferramentas ao lado de outras tão conhecidas e aplicadas quanto, sendo uma das mais populares o 5W2H, que segundo o Sebrae/SC:

> (...) é um checklist das atividades preventivas e corretivas que precisam ser desenvolvidas dentro de uma empresa, organizado de forma prática, simples, eficiente e clara. Para isso, envolve líderes e colaboradores para identificação de necessidades e propostas de soluções aos objetivos que se deseja alcançar. (SEBRAE/SC, 2022)

Sendo que:

> A sigla vem do inglês e tem a origem nas letras iniciais das perguntas que devem ser feitas ao traçar o plano:
>
> *5W*
>
> • What – o que será feito?
> • Why – por que será feito?
> • Where – onde será feito?
> • When – quando será feito?
> • Who – por quem será feito?
>
> *2H*
>
> • How – como será feito?
> • How much – quanto vai custar?
>
> Ou seja, a função dessa ferramenta é definir o que será feito, por que, onde, por quem, quando, como e quanto isso custará. Dessa forma, o método auxilia na organização e no planejamento de quaisquer processos internos da empresa. (SEBRAE/SC, 2022)

A figura 1 apresenta um modelo de 5W2H disponibilizado pelo Sebrae/SC:

5W					2H		STATUS
WHAT (O QUE)	WHY (POR QUE)	WHERE (ONDE)	WHO (QUEM)	WHEN (QUANDO)	HOW (COMO)	HOW MUCH (QUANTO CUSTA)	
O QUE SERÁ FEITO? QUAL É O SEU OBJETIVO? COMO DESCREVER O MELHOR QUE PODE OBTER NESTA SITUAÇÃO?	POR QUE SERÁ FEITO? QUAL É A RAZÃO QUE MOTIVA ESSA AÇÃO? O QUE VAI CONSEGUIR DE RETORNO? FAZ PARTE DE SUA MISSÃO? VALE A PENA?	ONDE SERÁ FEITO?	POR QUEM SERÁ FEITO? QUEM ESTÁ ENVOLVIDO OU É RESPONSÁVEL EM CADA AÇÃO? QUEM DEVE SER AVISADO?	QUANDO SERÁ FEITO? QUAIS SÃO AS PRIMEIRAS AÇÕES NECESSÁRIAS? ESSAS AÇÕES SÃO PROATIVAS OU DEPENDEM DE OUTRAS FORA DO SEU CONTROLE?	COMO SERÁ FEITO? COMO INICIAR, MENSURAR E ATIVAR AS AÇÕES NECESSÁRIAS? QUAIS SÃO AS SOLUÇÕES DE CONTINGÊNGIA, NO CASO DE ENCONTRAR OBSTÁCULOS? O QUE SINALIZARÁ QUE É O MOMENTO DE AGIR ASSIM?	QUANTO CUSTARÁ FAZER? QUANTO CUSTARÁ EM TEMPO, ESFORÇO, DINHEIRO, CONHECIMENTO, PREPARAÇÃO PSICOLÓGICA E NEGOCIAÇÃO OU MOTIVAÇÃO PESSOAL E DE GRUPO?	

Figura 1: Exemplo de estrutura do 5w2h
Fonte: SEBRAE/SC (2022)

Partindo do pressuposto de que há um tipo de conexão adjacente ao relatório de impacto à proteção de dados com relação a outras ferramentas de gestão de riscos e uma similaridade com o 5W2H apresentado na figura 1, por conta da sua finalidade e abrangência, apesar de ainda não haver uma estipulação concreta de um modelo para que se desenvolva o RIPD, tem-se que o mesmo, em acordo com os requisitos mínimos estabelecidos pela ANPD, deve se apresentar com base nas etapas de elaboração mínimas presentes na figura 2:

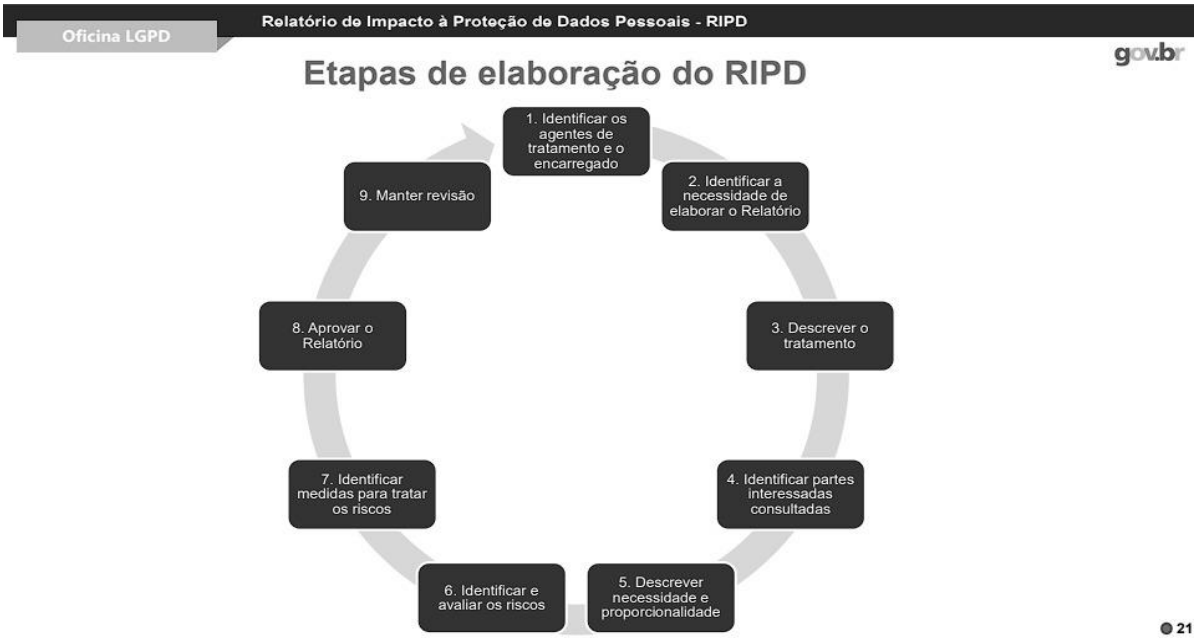

Figura 2: Etapas de elaboração do RIPD
Fonte: Governo Digital (2020, pg. 21)

Em suma, ambas as ferramentas se assemelham por apresentarem uma estrutura e organização lógica, sendo que fazem uma análise detalhada para pormenorizar os processos fazendo com que seja possível a identificação de elementos-chave que ajudarão no processo de gestão tendo com principal foco, em ambos os casos, a orientação à ação, visto que uma das finalidades de ambas as ferramentas é fazer com que haja uma avaliação crítica dos pontos apresentados para que se tome as medidas cabíveis.

Destarte isso, os pontos díspares entre as ferramentas de gestão, seja na correlação do RIPD com o 5W2H ou com qualquer outro instrumento do tipo, está justamente no seu objetivo específico, na sua área de aplicação, no seu escopo de análise e na sua previsão legal, tendo em vista que o RIPD é uma ferramenta com propósitos específicos, disposta em lei e que pode ser solicitada pela ANPD como

sendo um documento obrigatório ao controlador de dados, não excluindo, por exemplo, a possibilidade de que haja a adoção de outras ferramentas de gestão que contribuam para o papel e finalidade atribuídos ao relatório de impacto.

Embora ainda pouco difundido e com modelo padrão um tanto incerto, o RIPD propriamente dito pode ou não ser disponibilizado de forma pública para que os interessados tenham acesso aos dados, oportunidade na qual os titulares destes podem ter acesso ao documento e as empresas interessadas na sua elaboração podem ter um norte para a confecção, como informa o item 6 das perguntas e respostas do sítio eletrônico, do portal Gov.br, da ANPD:

> Embora a divulgação do RIPD não seja, em regra, obrigatória, permitir o acesso ao público em geral pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas, previstos, respectivamente, pelo art. 6º, incisos IV, VI e X, da LGPD.
> Para isso, o controlador pode disponibilizar o RIPD em meios de fácil acesso pelo titular, especialmente em seus sítios eletrônicos, com informações sobre suas atividades de tratamento de dados pessoais, de forma clara, adequada e ostensiva. Contudo, nesse caso a versão pública do RIPD pode ser distinta da versão interna, no intuito de resguardar segredos comercial e industrial e outras informações protegidas por lei.
> Especificamente em relação a entidades e órgãos públicos, o RIPD deverá ser publicado: (i) por determinação da ANPD, nos termos do art. 32 da LGPD; ou (ii) pelo próprio controlador, quando não identificada hipótese de sigilo aplicável ao caso, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011. (GOV.BR - ANPD, 2023)

Neste sentido, para que se tenha a noção da porção de importância que o RIPD detém no cenário da proteção dos dados pessoais, cabe colacionar parte específica do próprio relatório do Banco Central do Brasil (BCB), criado e disposto pela própria instituição (disponível por meio da política de acesso à informação), que norteia as atividades que envolvem o tratamento de dados e que fizeram com que se criasse, gerisse e atualizasse métodos para a proteção desses dados, como é apresentado no Anexo I do documento:

> Anexo I – Gerenciamento dos Riscos à Proteção de Dados Pessoais
>
> (...)
>
> Metodologia de Gerenciamento dos Riscos à Proteção de Dados Pessoais
>
> (...)

> A metodologia desse processo de avaliação de risco, ferramenta fundamental para a gestão de riscos, traz como vantagens: facilitar o entendimento do negócio e suas vulnerabilidades; apontar atividades críticas com controles frágeis ou inexistentes; gerar maior qualidade nas informações de risco e trazer flexibilidade ao processo de avaliação. (BCB, 2022)

Pode-se depreender, portanto, que para além da função regulamentar do RIPD, que pode eventualmente tornar-se obrigatório, há também a função de fazer com que as empresas pensem e adotem mecanismos e metodologias (como no caso do BCB) para que se aplique a melhor forma de governança de dados para coibir possíveis infortúnios passíveis de acontecer quando na função de 'tratador' dos dados pessoais. A finalidade é que se otimize e melhore os processos internos, até mesmo os que, de certa forma, independem do disposto no relatório, para fazer com que as companhias comecem a adotar boas práticas e uma política empresarial mais sólida, baseada na confiança e na transparência.

5. BENEFÍCIOS QUE PODEM SER OBTIDOS QUANDO DA IMPLEMENTAÇÃO DO RIPD E OS MALEFÍCIOS QUANDO NÃO UTILIZADO

A princípio, é necessário que se entenda que a implementação do RIPD não é só uma forma de ter um documento que comprove que se está tomando alguma medida (e/ou salvaguarda) frente às possíveis adversidades encontradas quando em função do tratamento dos dados pessoais, mas sim uma forma de, também, estar em conformidade com o que demanda a LGPD, já que a sua aplicação pressupõe a análise e observância do disposto na lei, como tem pontuado Pinheiro:

> Atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de *compliance* digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura. (PINHEIRO, 2021 pg. 77)

Neste sentido, a adoção do RIPD, por si só, já configura um benefício para a empresa, visto que, afirma Pinheiro (2021, pg. 84), "todas as ferramentas são úteis e necessárias ao longo do tratamento de dados, pois permitem que as instituições

adotem mais controles e transparência em seus procedimentos.” Sendo assim, dentre os tantos outros benefícios decorrentes da implantação das medidas dispostas na LGPD, como o RIPD:

> Vale destacar algumas vantagens da implementação da LGPD, como o apreço por parte dos clientes, e o fortalecimento das relações comerciais em virtude da responsabilidade solidária, ao passo que a empresa poderá fechar mais contratos (VASCONCELOS, 2020)

Neste ponto, cabe a ressalva de que os ganhos obtidos com a implantação do RIPD não são exclusivos das empresas que o adota, mas sim, também, para a parte mais importante na relação de coleta e tratamento de dados, que são os titulares. Em tempo, a sociedade como um todo também ganha com essa relação visto que existirá empresas preocupadas e transparentes quando o assunto é o tratamento de dados pessoais, sendo assim, cabe fazer uma relação elencando os ganhos para estes três setores.

Para as empresas, há de se falar no cumprimento da legislação, já que a adequação das políticas da organização para recepcionar a LGPD e, consequentemente, O RIPD, faz com que esta esteja em dia com as disposições legais que tratam sobre a coleta, a armazenagem e o tratamento de dados pessoais, o que faz com que se evite possíveis sanções e penalidades decorrentes da má gestão e governança de dados.

A elaboração do RIPD contribui para a melhoria constante dos processos internos das organizações visto que este requer que sejam feitos estudos detalhados tanto dos processos internos da organização quanto da LGPD em si, portanto, a aplicação do relatório contribui para uma melhoria constante e contínua, pois além de agregar informações extremamente úteis ao dia a dia da empresa, também faz com que se verifique os processos já existente e corrija vulnerabilidades que coloquem em risco os dados utilizados.

Ainda, possibilita e promove a inovação tecnológica de forma responsável, já que a adoção do RIPD faz com que as organizações se preocupem em conduzir projetos, atuais e futuros, com o pensamento focado na proteção dos dados pessoais, o que contribui e está alinhado aos interesses dos titulares dos dados e da sociedade, o que demonstra o seu compromisso social com a segurança e a inovação, além de que faz com que a empresa tenha respaldo perante os clientes e

parceiros, já que a adoção do RIPD e de quaisquer outras medidas que mostrem estar em acordo com o previsto em lei e baseado em boas práticas molda a imagem corporativa de forma positiva, o que permite criar bons e duradouros laços comerciais.

Ademais, fortalece e impulsiona a sociedade digital, sendo que com a adoção de ferramentas como o RIPD, a empresa contribuirá para a fomentação de outros projetos correlatos, próprios e de terceiros - de forma indireta – que ajudarão na estruturação de uma sociedade digital com maior observância dos preceitos legais e com foco em garantir os direitos fundamentais individuais e da coletividade.

Já para os titulares dos dados há de se falar, principalmente, da proteção da privacidade e da garantia dos direitos fundamentais, já que certamente os titulares dos dados são os mais beneficiados com a adoção do RIPD por meio dos agentes tratadores de dados, pois com a ferramenta elaborada nos limites do que está exposto na LGDP, deduz-se que a sua privacidade e os seus direitos e garantias fundamentais estão sendo respeitados e bem guardados na medida do possível. Neste sentido, ainda são beneficiados, de certa forma, com a transparência e a confiança, já que a adoção do RIPD pressupõe a observação de todo o exposto na LGPD, portanto, os titulares dos dados são beneficiados pois terão as informações completas dos seus dados disponibilizados, onde estão armazenados, para o que estão sendo usados, com quem estão sendo compartilhados e podem optar pela exclusão ou não dos mesmos, garantindo confiabilidade.

Para a sociedade há um fortalecimento social e um sentimento de confiança já que com a adoção e implantação do RIPD por parte de qualquer empresa que trabalhe com dados pessoais, seja ela pública ou privada, terá o seu impacto social de forma extremamente positiva, fazendo com que a sociedade como um todo tenha confiança tanto nas plataformas como na legislação em si, contribuindo com a manutenção de uma fluidez social e ganhos inestimáveis, tendo em vista o principal: a garantia dos direitos fundamentais.

Na contramão dos que são considerados os ganhos por conta da elaboração e implantação do RIPD, tem-se que os malefícios quando da sua inutilização ou não implantação por parte das empresas que realizam o tratamento de dados pessoais são exatamente os opostos dos benefícios. Há de se falar que os riscos à privacidade aumentam de forma exponencial, já que os titulares não saberão como as organizações estão lidando com os seus dados pessoais, as empresas podem

sofrer com sanções e penalidades, legalmente descritas na seção 1, das sanções administrativas, disposta na LGPD, além de perder credibilidade e competitividade (principalmente se ocorrer algum evento adverso), pode pôr em *check* a proteção aos princípios basilares que regem a vida em sociedade e os direitos fundamentais.

Deste modo, Sá (2023) elenca que dentre as principais consequências da não observância dos dispostos na LGPD, pode-se pontuar como mais importantes: a possibilidade de que haja multa no importe de até 2% sob o faturamento da empresa, com limite de até 50 milhões de reais, a ser aplicada pela ANPD e a possibilidade de haver ainda mais danos financeiros, tendo em vista que a LGPD prevê a indenização por danos morais e/ou materiais aos titulares dos dados por parte dos agentes tratadores se comprovada a inobservância e descumprimento da LGPD quando houver obrigação explícita, como elenca a lei:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> (..)
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018)

Neste sentido, entende-se que há uma gama de benefícios e vantagens competitivas quando da implantação do RIPD que seriam deixadas de lado caso não houvesse a sua implementação, o que colabora com a ideia de que o relatório é algo essencial a ser adotado pelas organizações como um todo, independentemente da

obrigatoriedade, tendo em vista que para além de todos os benefícios quando da sua adoção, as organizações ainda estarão cobertas e respaldadas, aumentando o nível de confiança dos seus clientes e parceiros.

6. CONSIDERAÇÕES FINAIS

A adoção e implantação do Relatório de Impacto à Proteção de Dados (RIPD) presente na Lei Geral de Proteção de Dados (LGPD) é de suma importância em se tratando de boas práticas organizacionais e com vistas à preocupação que normalmente decorre das tarefas derivadas da coleta, armazenamento e tratamento de dados pessoais, sensíveis ou não. Neste artigo foi explorado, de forma pormenorizada, qual o papel do RIPD e, também, qual o seu grau de importância bem como quais são os benefícios esperados pelos variados segmentos da sociedade como um todo quando da sua aplicação prática.

Para além de uma simples adequação aos requisitos legais, o RIPD não deve ser enxergado como uma forma de burocratização encontrada pelo estado para incumbir as organizações de mais um ônus, sendo que este se mostra ser uma ferramenta formidável de gestão de riscos, que inclusive possui semelhanças e pode ser utilizada de forma concomitante com outras ferramentas do tipo, de elaboração facultativa, sem previsão legal, para que se complementem e deem mais firmeza às ações que porventura os “figurantes” da LGPD venham a performar.

A implantação do RIPD, como preconiza a sua estrutura mais simples, tem o poder de demonstrar o compromisso das organizações não só com a proteção dos dados pessoais dos titulares, mas também com os direitos fundamentais individuais e da coletividade, fazendo com que haja, também, uma aprimoração dos processos e uma minimização exponencial dos riscos que podem acometer os mesmos.

Pode-se concluir, por fim, que a adoção do relatório de impacto à proteção de dados é de extrema importância para a gestão de riscos e proteção dos dados pessoais, que é o tema central da análise feita neste artigo. Portanto, é imprescindível que todas as ramificações da sociedade entendam não só a importância da sua aplicação, mas também a necessidade que os dias atuais têm de ferramentas com o “poder” benéfico que o RIPD tem, sendo esta uma ferramenta confiável e que estabelece a busca por medidas protetivas importantíssimas,

principalmente dado o cenário atual em que estamos inseridos, com um bombardeio tecnológico sem fim que cada dia mais traz mais e mais conteúdo e nos cobra mais e mais dados e informações pessoais em troca. Neste cenário, nada mais justo do que estarmos cientes de que estamos protegidos.

REFERÊNCIAS BIBLIOGRÁFICAS

BANCO CENTRAL DO BRASIL. **Relatório de Impacto à Proteção de Dados Pessoais**. BCB, 2022. Disponível em: https://www.bcb.gov.br/content/acessoinformacao/lgpd_docs/relatorio_de_impacto_a_protecao_de_dados_pessoais.pdf. Acesso em: 2 jun. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constitui-cao/Constituicao.htm. Acesso em: 23 mar. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 27 mar. 2023.

DELPHIX. **O que é governança de dados e por que é importante?**. Disponível em: https://www.delphix.com/br/glossario/o-que-e-governanca-de-dados. Delphix, [c2023]. Acesso em: 27 mar. 2023.

DONEDA, Danilo. A PROTEÇÃO DOS DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011

FIA. **O que é gestão de risco?** Fia, 2018. Disponível em: https://fia.com.br/blog/o-que-e-gestao-de-risco/. Acesso em: 23 mai. 2023.

FREITAS, Cinthia O. A., **Risco e proteção de dados pessoais.** RRDDIS – Revista Rede de Direito Digital, Intelectual & Sociedade, Curitiba, v. 2, n. 4, p. 225-247, 2022. Disponível em: https://revista.ioda.org.br/index.php/rrddis/article/view/74/49. Acesso em: 26 abr. 2023.

GAEA. **Entendendo a Conformidade com o GDPR.** Gaea, 2020. Disponível em: https://gaea.com.br/entendendo-a-conformidade-com-o-gdpr/. Acesso em: 4 mai. 2023.

GDPR-INFO. **Art. 35 GDPR Data Protection Impact Assessment**. Gdpr-info, 2023. Disponível em: https://gdpr-info.eu/art-35-gdpr/. Acesso em: 17 mai. 2023.

GETPRIVACY. **O que é e como elaborar o Relatório de Impacto à Proteção de Dados Pessoais.** Getprivacy, [c2022]. Disponível em: https://getprivacy.com.br/relatorio-de-impacto-lgpd/. Acesso em: 27 mar. 2023.

GOMES, Maria C. O. **Relatório de impactos à proteção de dados:** uma breve análise da sua definição e papel na LGPD. Academia, 2019. Disponível em: https://www.academia.edu/41160034/Relat%C3%B3rio_de_Impacto_a_Prote%C3%A7%C3%A3o_de_Dados_Pessoais_uma_breve_an%C3%A1lise_da_sua_defini%C3%A7%C3%A3o_e_papel_na_LGPD. Acesso em: 27 mar. 2023.

GOOGLE. **O que é governança de dados?** Google, [s.d.] Disponível em: https://cloud.google.com/learn/what-is-data-governance?hl=pt-br. Acesso em: 27 mar. 2023.

GOV.BR - ANPD. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**. GOV.BR, 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 23 fev. 2023.

GOVERNO DIGITAL. **Apresentação do Relatório de Impacto à Proteção de Dados (RIPD)**. Governo Digital, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_ripd.pdf. Acesso em: 20 mai. 2023.

GRASSO, Ian M. 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**, SP – Edição Especial – Direito Digital |Ano 3| n. 1| p. 142-174| 2021

PINHEIRO, Patrícia P. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 3ª ed. São Paulo: Saraiva, 2021. 176p.

PRESTES, Marcus V. P. et al. **Lei geral de proteção de dados nº 13.709/2018: apontamentos sobre sua contextualização como marco legal no Brasil.** Research, Society and Development. 01/10/2021. v. 10, n. 12, e 568101220906

SÁ, Bruna de. **Quais são as consequências de não cumprir a LGPD?** Jusbrasil. 2023. Disponível em: https://www.jusbrasil.com.br/artigos/quais-sao-as-consequencias-de-nao-cumprir-a-lgpd/1833570683. Acesso em: 4 jun. 2023.

SEBRAE/SC. **5W2H: O que é, para que serve e por que usar na sua empresa?** Sebrae/SC, 2022. Disponível em: https://www.sebrae-sc.com.br/blog/5w2h-o-que-e-para-que-serve-e-por-que-usar-na-sua-empresa#:~:text=O%20que%20%C3%A9%20a%20ferramenta,os%20envolvidos%20em%20um%20projeto. Acesso em: 23 mai. 2023.

VASCONCELOS, Kleber. **Os benefícios da implementação da LGPD**. Serpro, 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/beneficios-riscos-lgpd-empresas. Acesso em: 3 jun. 2023.