UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO DA EMPRESA E DOS NEGÓCIOS
NÍVEL MESTRADO PROFISSIONAL

NICÉLIA PEREIRA LIMA FERREIRA

DIREITO DOS NEGÓCIOS E INTERNACIONALIZAÇÃO
PROTEÇÃO DE DADOS PESSOAIS E GESTÃO DE RISCOS:
Rumo a Protocolo de Adequação a Instituição de Ensino Superior

Porto Alegre
2022

NICÉLIA PEREIRA LIMA FERREIRA

DIREITO DOS NEGÓCIOS E INTERNACIONALIZAÇÃO
PROTEÇÃO DE DADOS PESSOAIS E GESTÃO DE RISCOS:
Rumo a Protocolo de Adequação a Instituição de Ensino Superior

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito da Empresa e dos Negócios, pelo Programa de Pós-Graduação em da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientador: Prof. Dr. Cristiano Colombo

Porto Alegre
2022

F383d Ferreira, Nicélia Pereira Lima.
Direito dos negócios e internacionalização proteção de dados pessoais e gestão de riscos: rumo a protocolo de adequação a instituição de ensino superior / por Nicélia Pereira Lima Ferreira. -- Porto Alegre, 2022.

101 f. : il. (algumas color.) ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito da Empresa e dos Negócios, Porto Alegre, RS, 2022.
Orientação: Prof. Dr. Cristiano Colombo, Escola de Direito.

1.Proteção de dados. 2.Administração de risco. 3.Governança da internet. 4.Direito à privacidade. 5.Ensino superior – Efeito de inovações tecnológicas. 6.Responsabilidade (Direito). I.Colombo, Cristiano. II.Título.

CDU 34:004.056.5
378:004

Catalogação na publicação:
Bibliotecária Carla Maria Goulart de Moraes – CRB 10/1252

NICÉLIA PEREIRA LIMA FERREIRA

DIREITO DOS NEGÓCIOS E INTERNACIONALIZAÇÃO
PROTEÇÃO DE DADOS PESSOAIS E GESTÃO DE RISCOS:
Rumo a Protocolo de Adequação a Instituição de Ensino Superior

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito da Empresa e dos Negócios, pelo Programa de Pós-Graduação em da Universidade do Vale do Rio dos Sinos (UNISINOS).

Aprovado em 23 / 12 / 2022

BANCA EXAMINADORA

Prof. Dr. Cristiano Colombo (orientador) – UNISINOS

Prof. Dr. Wilson Engelmann – UNISINOS

Prof. Dr. Éderson Garin Porto – UNISINOS

Prof. Dr. Guilherme Damasio Goulart – Faculdade Inedi - CESUCA

Aos meus familiares, em especial ao meu esposo, Luiz Antonio Neves Ferreira que, com imenso amor me incentivou para que esse momento acontecesse.

AGRADECIMENTOS

Agradeço aos meus professores do Mestrado, pela dedicação e pela aprendizagem, em especial ao meu orientador, professor Cristiano Colombo, por todo o estímulo, dedicação e empatia, fez com que este trabalho se concluísse – ressalto minha admiração.

Agradeço à UniRV – Universidade de Rio Verde por acreditar no meu potencial e apoio profissional e o esforço em capacitar seus servidores realizando convênio com a Unisinos – Universidade do Vale do Rio dos Sinos, que também agradeço pela acolhida no curso de mestrado.

Enfim, agradeço a todos que de alguma forma contribuíram e participaram deste aprendizado tão importante e transformador, demonstrando uma nova visão de futuro.

“Ninguém consegue assobiar uma sinfonia, é necessária uma orquestra inteira.”

H. E. Lucoock

RESUMO

O presente trabalho tem como tema a proteção de dados pessoais e gestão de riscos, rumo ao protocolo de adequação à Instituição de Ensino Superior. Neste sentido, é importante mencionar que administrar riscos é sempre uma atividade complexa para as organizações, pois a competitividade atual, a globalização e todo o desenvolvimento tecnológico contribuem para que o gerenciamento de risco se torne cada vez mais difícil, por isso, se faz tão necessário. Alguns riscos são simplesmente escolhas equivocadas dos administradores e outros riscos podem afetar diretamente o desempenho da organização. Esta cobertura de risco somente será válida se vier a reduzir as dificuldades na seleção dos dados e as possíveis tensões financeiras. O problema da pesquisa é identificado no fato de como se implantará a análise em gestão de risco em uma organização de ensino superior buscando concretizar práticas de responsabilidade proativa pelos agentes de tratamento. No primeiro capítulo tratou-se da proteção de dados, sendo características gerais, evolução histórica, Lei Geral de Proteção de Dados Pessoais e a Gestão de Risco de forma geral. No segundo capítulo enfatizou a governança de dados para gestão de riscos em proteção de dados pessoais, com atenção especial para as boas práticas para controle de risco. Por fim, protocolo para gerenciamento de risco adequado à proteção de dados pessoais em instituição de ensino superior. Aderir a uma gestão de riscos com a sistematização e metodologia apropriadas é um elemento essencial em qualquer organização. Quanto à metodologia, a partir de pesquisas bibliográficas, artigos, documentos e relatórios acerca do tema, teve como objetivo avaliar como as instituições de Ensino Superior, vêm se protegendo dos riscos inerentes aos dados pessoais. Através de levantamento e análise de como evitar os riscos e tratar os dados pessoais dos acadêmicos, pais, servidores, enfim de toda a comunidade acadêmica, sendo de grande representação no cenário econômico brasileiro, verificou-se que estas empresas que atuam no mercado além de estarem bastante suscetíveis aos riscos de mercado, têm que demonstrar com seu exemplo o quanto é importante esta proteção, oriunda de dados pessoais.

Palavras-chave: tratamento de dados pessoais; gestão de risco; Lei Geral de Proteção de Dados (LGPD).

ABSTRACT

The present work has as its theme the protection of personal data and risk management, towards the protocol of adequacy to the Institution of Higher Education. In this sense, it is important to mention that risk management is always a complex activity for organizations, as current competitiveness, globalization and all technological development contribute to risk management becoming increasingly difficult, which is why it is done so necessary. Some risks are simply poor choices by managers, and other risks can directly affect the organization's performance. This risk coverage will only be valid if it reduces difficulties in data selection and possible financial strains. The research problem is identified in the fact of how to implement risk management analysis in a higher education organization seeking to implement proactive responsibility practices by treatment agents. The first chapter dealt with data protection, with general notions, historical evolution, the General Law for the Protection of Personal Data and Risk Management in general. In the second chapter, he emphasized data governance for risk management in personal data protection, with special attention to good practices for risk mitigation. Finally, protocol for adequate risk management for the protection of personal data in a higher education institution. Adhering to risk management with the appropriate systematization and methodology is an essential element in any organization. As for the methodology, based on bibliographical research, articles, documents and reports on the subject, it aimed to evaluate how higher education institutions have been protecting themselves from the risks inherent to personal data. Through a survey and analysis of how to avoid risks and treat the personal data of academics, parents, servants, in short, the entire academic community, being of great representation in the Brazilian economic scenario, it was verified that these companies that operate in the market, in addition to being quite susceptible to market risks, they have to demonstrate with their example how important this protection, arising from personal data, is.

Key-words: processing of personal data; risk management; General Data Protection Act (LGPD).

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
DPDC	Departamento de Defesa e Proteção do Consumidor
EC	Emenda Constitucional
GDPR	*General Data Protection Regulation*
IES	Instituição de Ensino Superior
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
NBR	Normas Brasileiras de Regulação
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OMC	Organização Mundial do Comércio
SGPI	Sistema de Gestão da Privacidade da Informação
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

No presente estudo, tratar-se-á acerca da proteção de dados pessoais e gestão de riscos, rumo ao protocolo de adequação à Instituição de Ensino Superior, a partir das legislações de proteção de dados pessoais publicadas, nos últimos anos. Com efeito, a evolução tecnológica trouxe modificações nas relações pessoais e econômicas, na medida em que novas tecnologias da informação passaram a mediar comportamentos humanos, trazendo como uma de suas consequências o aumento do lastro dos dados pessoais.

O objetivo geral, nos termos do problema de pesquisa, é avaliar as condições para a adoção de Gestão de Risco para adequação a Instituição de Ensino Superior (IES), e os objetivos específicos tratam de como as IES devem se proteger dos riscos inerentes aos dados pessoais, bem como, apresentar princípios da proteção de dados, seu papel na instituição, e os resultados que pode obter a partir da adesão a um programa de conformidade com a lei de proteção de dados, descrever as responsabilidades/deveres inerentes à Lei de proteção de Dados; retratar a estrutura/forma de como será abordada a Lei de proteção de Dados e os elementos que exigem regulamentação, implantar/implementar protocolo voltado a LGPD de forma a minimizar surgimento de riscos .

O problema de pesquisa é identificado no fato de como se implantará a análise em gestão de risco em uma organização de ensino superior buscando concretizar práticas de responsabilidade proativa pelos agentes de tratamento.

Como justificativa para a pesquisa, aponta-se o advento de instrumentos normativos como o Regulamento Geral sobre Proteção de Dados (*General Data Protection Regulation* ou GDPR), a norma europeia em vigor desde maio de 2018, ou a Lei Geral de Proteção de Dados (LGPD), a norma brasileira em vigor desde setembro de 2020, representaram marcos importantes, trazendo novas obrigações às organizações. Com a entrada em vigor da lei, as empresas terão que observar alguns procedimentos para obter dados dos clientes, bem como para arquivá-los e tratá-los, devendo alterar suas rotinas e processos. Essas normas não têm como finalidade proibir o uso dos dados pessoais, mas deixam bem claro que, para o tratamento de dados é preciso obedecer a regras, sob pena de responsabilização. O ponto central da nova lei é que nenhuma instituição pode utilizar os dados de nenhum cidadão sem o seu consentimento explícito ou com base nas hipóteses

legais autorizadoras. O texto também traz garantias para o usuário, que pode solicitar que seus dados sejam deletados, revogar um consentimento, transferir os dados para outro fornecedor de serviços, entre outras ações. E o tratamento dos dados deve ser feito levando em conta alguns quesitos, como finalidade e necessidade, que devem ser previamente acertados e informados ao cidadão.

No primeiro capítulo tratar-se-á sobre a proteção de dados, sendo caracteristicas gerais, evolução histórica, Lei Geral de Proteção de Dados Pessoais. No segundo capítulo, enfatizar-se-á a governança de dados para gestão de riscos em proteção de dados pessoais, com atenção especial para as boas práticas para o controle de risco. No último capítulo, encerrar-se-á com um protocolo para gerenciamento de risco adequado à proteção de dados pessoais em instituição de ensino superior.

A metodologia aplicada se operou através de pesquisa bibliográfica com análise em: livros, artigos, periódicos, dissertações e teses no tocante a tutela de dados pessoais no Brasil, a complexidade e necessidade de efetivo estímulo à adoção de programas de *compliance* de dados pessoais, bem como a gestão de risco na esfera da sociedade da informação, liberdade e privacidade, levando em consideração a análise de como evitar os riscos e tratar os dados pessoais dos acadêmicos, pais, servidores, enfim de toda a comunidade acadêmica, sendo de grande representação no cenário econômico brasileiro.

2 PROTEÇÃO DE DADOS

A proteção dos dados pessoais vem se tornando cada vez mais um desafio para as empresas de diversos tamanhos e nichos de negócios. Não limitada ao tamanho da empresa ou a sua natureza, a responsabilidade sobre a gestão (ou utilização) de dados e informações dos colaboradores, clientes, fornecedores e instituições de regulação (Poder Público), vem a tempos sendo analisada. Têm-se, por exemplo, as *Startups* que em sua maioria utilizam os dados pessoais de forma intensiva, ou seja, para vender os seus produtos, ou até mesmo utilizando-os como insumo para desenvolver os seus modelos de negócios. Desta forma, estas empresas devem tratar o tema da privacidade e proteção de dados pessoais em seus modelos de negócio de forma estratégica, seguindo as determinações da LGPD[1].

Diante do atual cenário, os dados são considerados ativos importantíssimos, como estratégia de negócio, pela grande versatilidade de seu uso[2]. Entretanto, justamente devido às diversas possibilidades de uso dos dados e aos riscos sociais causados pelo uso indevido desses ativos, ampliam-se também os controles e processos formais para o seu tratamento[3].

Em 2020 entrou em vigência a lei nº 13.709/2018, intitulada Lei Geral de Proteção de Dados (LGPD), a qual fez com que os cidadãos, Poder Público e empresas se adaptassem a uma nova política de tratamento e compartilhamento de dados no Brasil.

2.1 Caracterização da proteção de dados pessoais

Entende-se por Dados pessoais, qualquer informação relativa a uma pessoa singular identificada ou identificável, é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um

---

[1] FONSECA, Marcos De Lucca; MIGLIO Marcelo. **LGPD para startups**. Disponível em: https://mmiglio.com.br/advocacia-sp/artigo-lgpd-startup.html. Acesso em: 08 set. 2022.

[2] BARBIERI, C. **Governança de dados**: práticas, conceitos e novos caminhos. [*S.l.*]: Alta Books, 2020.

[3] FERNANDES, Aguinaldo Aragón; ABREU, Vladimir Ferraz de. **Implantando a governança de TI**: da estratégia à gestão de processos e serviços. [*S.l.*]: Brasport, 2014.

número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social[4].

Devido rápida evolução ocorrida nos meios digitais, principalmente no final do século XX, as relações sociais se apresentam com uma nova vertente, por meio da qual eliminou obstáculos e o mundo todo pode se conectar rápida e simultaneamente. Assim, tendo em vista a realidade proporcionada pelo *Big Data*[5] e por todo o cenário de informações trocadas online, as interações sociais passam a estar cada vez mais à mercê da tecnologia, possibilitando, assim, o surgimento dos dados pessoais e sua relevância no mundo jurídico.

Os dados pessoais compreendem certas especificações para serem caracterizados. Inicialmente, tem-se que o termo dado o qual manifesta uma informação antes mesmo de ela ser interpretada ou de passar por um processo de elaboração (DONEDA)[6]. Compreendem-se por dado pessoal todas as informações de cunho individual, que são pertinentes de alguém ou que se relacionam a essa pessoa, ligados diretamente ou indiretamente. Os dados pessoais são tratados como aquilo que nos tornam individuais, diferentes, e que só podem estar ligados a uma determinada pessoa, pode-se citar aqui a título de exemplo: CPF; RG; dentre outros que nos tornam seres individualizados, compreendem as espécies de dados:

a) Dado Anonimizado - Relacionado a determinada pessoa que possa se tornar identificável, mas que a priori não pode ser identificada. O dado anonimizado se desvincula da identificação da pessoa, mas pode ser considerado um dado pessoal caso essa anonimização possa chegar a ser revertida. Os dados anonimizados não nos possibilitam a identificação de seu titular. Segundo Bioni[7]:

> A antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado termo, anônimo seria aquele que não tem nome nem rosto. Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização. Esse processo pode se valer de diferentes técnicas que

[4] CEARÁ. Tribunal de Justiça. **Dado pessoal, dado pessoal sensível e dado anominizado.** Disponível em: https://www.tjce.jus.br/lgpd/lgpd-dados-pessoais/. Acesso em 13 nov. 2022.

[5] O termo Big Data refere-se a dados que extrapolam a capacidade de processamento de sistemas de banco de dados convencionais – representa um enorme complexo de dados, em constantemovimento, sejam eles estruturados ou não. (DUMBILL, Edd. Getting up to speed whit big data. *In:* BIG data now. 2012).

[6] DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. **Revista Espaço Jurídico**, Joaçaba, v. 12, n. 103, 2011.

[7] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

> buscam eliminar tais elementos identificadores de uma base de dados, variando entre: a) supressão; b) generalização; c) randomização e; d) pseudoanonimização.

b) Dados Sensíveis: Diretamente ligados a origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato, organização de caráter religioso, filosófico, bem como, aqueles que dizem respeito a saúde ou a vida social, ou dados genéticos ou biométricos. Tais dados necessitam de maiores cuidados e só devem ser utilizados com o consentimento do titular, podendo ser utilizados nos seguintes casos: pelo responsável ao tratamento de dados; por profissionais da área da saúde; e para órgãos de pesquisa desde que assegurem a segurança destes. De acordo com Bioni[8]:

> Os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação. Quando se pensa em dados que exprimem a orientação sexual, religiosa, política, racial, estado de saúde ou filiação sindical, surge a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade.

c) Dados da Criança e do Adolescente: Devem ser protegidos de maneira que seus dados não sejam utilizados sem a autorização dos pais ou responsáveis legais. Tais dados só poderão ser utilizados sem consentimento se necessário a proteção do menor, ou para que sejam localizados os pais ou responsáveis, para efeito desses dados e conforme previsão do Estatuto da Criança e do Adolescente considera-se criança a pessoa com até 12 anos e adolescente de 12 anos até os 18 anos de idade[9].

De acordo os critérios da maioria dos instrumentos internacionais relevantes, é considerado uma criança quem tiver idade inferior a 18 anos, a menos que tenha adquirido a maioridade legal antes dessa idade[10]. Como ser humano, a criança tem direito ao respeito pela sua privacidade. O artigo 16º da Convenção das Nações Unidas sobre os Direitos da Criança determina que nenhuma criança pode ser sujeita a intromissões arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou correspondência, nem a ofensas ilegais à sua honra e reputação.

---

[8] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[9] NUCCI, Guilherme de S. **Estatuto da criança e do adolescente:** comentado. 5. ed. 2020. Disponível em: https://online.**minhabiblioteca**.com.br. Acesso em: 2021.

[10] Nomeadamente o artigo 1.° da Convenção das Nações Unidas sobre os Direitos da Criança de 20.11.1989.

Portanto estabelece no Estatuto, constituir criança o ser humano até 11 anos completos; adolescente, o ser humano com 12 anos completos. Associando-se ao disposto pelo Código Civil, torna-se adulto, para fins civis, o ser humano que atinge 18 anos de idade; no mesmo prisma, o Código Penal fixa em 18 anos a idade da responsabilidade para fins criminais. Diante disso, aplica-se o conteúdo da Lei 8.069/90, como regra, à pessoa com até 17 anos.

A regulamentação traz princípios de tratamento para serem seguidos à risca, portanto, devem ser cuidadosamente observados, não podendo desviar-se de quaisquer destes. O titular dos dados deve ser cientificado de todos os atos, se estes estão em cumprimento ao estabelecido e se estão sendo utilizados para o devido tratamento ao qual se atinja a finalidade informada ao titular.

2.1.1 Evolução histórica da proteção de dados no Brasil e no mundo

A sociedade, ao longo dos anos, passou por vários modelos de organização social, de forma que, em cada período, houve um elemento principal para o seu desenvolvimento[11]. Nesse contexto, após a Segunda Guerra Mundial, percebeu como as informações pessoais dos cidadãos são importantes, programando ações com o intuito de um crescimento constante.

Mediante o avanço tecnológico e pela globalização, passou-se a ter uma dependência maior de bases de dados pessoais, em relação aos negócios da economia digital[12]. Logo, a informação, na sociedade atual, é o elemento central para o desenvolvimento da economia, passando-se a solicitar normas para a proteção de dados pessoais[13].

Como base na sociedade informacional segundo Manuel Castells[14], a internet foi criada nos anos 1960, surgindo, na década seguinte, a preocupação com a manipulação de dados pessoais na Guerra Fria, despontando por isso um ramo legislativo para a proteção de dados. O avanço das telecomunicações e dos

---

[11] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.
[12] PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.
[13] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.
[14] CASTELLS, Manuel. **A sociedade em rede**. 9. ed. rev. ampl. São Paulo: Paz e Terra, 2008.

computadores, com o progressivo aumento de armazenamento, proporcionou a verdadeira revolução de tecnologia da informação.

A ameaça do uso indiscriminado dos dados pessoais trouxe preocupações além do direito à privacidade. Outros questionamentos surgiram nos governos mundiais como, por exemplo, a manipulação de pensamentos e ideias políticas e até mesmo o controle de rebeliões ou a instauração delas. A internet nas mãos de quem sabe utilizar possui um poder gigantesco como por exemplo para controlar eleições ou causar rebeliões como por exemplo o que ocorreu na Primavera Árabe[15] .

Na Europa, as primeiras leis surgiram na década de 70 como um esboço do que se tornaram hoje. Viktor Mayer-Schönberger (1998) divide as leis de proteção de dados na Europa em gerações, sendo elas 4 (quatro) no total. Segundo o autor, as primeiras gerações de leis de proteção de dados não focam na proteção direta da privacidade individual, mas se concentram na função do processamento desses dados na sociedade. De acordo com a sua análise, os computadores em si, representavam um perigo para a proteção da informação e essas leis deveriam servir para conter esses perigos. Além disso, Para Doneda[16],

> Essa primeira geração era composta por leis que refletiam o estado da tecnologia e a visão do jurista à época, pretendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão de dados pessoais.

Todo esse processo de modificação das leis passou a incluir o titular da informação no processo de análise e coleta de dados de forma a fazê-lo parte da garantia do seu direito de forma a expandir as liberdades e garantias.

Para assegurar um controle sobre os dados começaram a surgir as primeiras leis de proteção de dados. Cabe ressaltar que, a princípio, não houve uma regulamentação mundial em relação ao uso da internet. Essa impossibilidade se dá, entre outros fatos, devido às diferenças culturais de um mundo ainda bastante heterogêneo[17] .

---

[15] A primavera árabe foi o conjunto de revoltas que ocorreram em países principalmente do oriente médio que lutaram para derrubar diversos líderes políticos autoritários. As revoluções tiveram como palco de organização as redes sociais que foram utilizadas para divulgar as ideias de revolta e combinar as ações populares.

[16] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

[17] PONTICELLI, Murilo Meneghel**. O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da Lei Geral de Proteção de Dados**. Trabalho de Conclusão de Curso (Graduação em Direito) – Curso de Direito, Universidade do Sul de Santa Catarina, Tubarão, 2018. Disponível em:

Para assegurar um controle sobre os dados começaram a surgir as primeiras leis de proteção de dados. Cabe ressaltar que, a princípio, não houve uma regulamentação mundial em relação ao uso da internet. Essa impossibilidade se dá, entre outros fatos, devido às diferenças culturais de um mundo ainda bastante heterogêneo[18].

Essas primeiras leis da primeira geração se deram na Alemanha e na Suécia. As pioneiras, segundo Pedro Peres Cavalcante[19] foram: ‘‘Land de Hesse na Alemanha a primeira lei de proteção de dados (*Hessisches Datenschutzgesetz*), em 1970, e à Suécia, a primeira lei nacional de proteção de dados em 1973 chamada de *data protection act*. Esses primeiros não possuíam muitos dos princípios da proteção de dados que existem hoje (Öman, 2010) porém, foram marcos no início da normatização. Além dessas, na primeira geração ainda há o Estatuto de Proteção de Dados do Estado alemão de *Rheinland-Pfalz* (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Todas elas fazem parte da primeira geração devido a linguagem que possuíam e a estrutura. Essas leis estavam embasadas em um contexto em que grandes centros de processamento de dados buscavam concentrar a coleta e gestão de dados pessoais. ‘‘Elas tinham um foco em conceder autorização para a criação destes bancos e do controle posterior a ser exercido por órgãos públicos’’[20]. É importante ainda lembrar que essas leis tinham como destinatários os entes públicos e não de fato a privacidade do indivíduo detentor desses dados.

Segundo Mendes,[21] em 1970 começam a surgir algumas decisões jurídicas e legislações que afirmam que os dados pessoais são uma projeção da personalidade do indivíduo e por isso deveriam receber tutela jurídica. Com isso, será analisada, nos próximos tópicos, a evolução dessas leis e como elas avançaram e influenciaram outras leis no mundo, inclusive o ordenamento jurídico brasileiro.

---

https://repositorio.animaeducacao.com.br/bitstream/ANIMA/6124/1/TCC%20Murilo%20Assinado.pdf. Acesso em: 2021.

[19] CAVALCANTE, Pedro Peres. **Privacidade e proteção de dados pessoais**: uma análise comparativa dos quadros regulatórios brasileiro e europeu. 2018. 62 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Pernambuco, Recife, 2018. Disponível em: https://repositorio.ufpe.br/handle/123456789/34357. Acesso em: 24 nov. 2022.

[20] DONEDA, Danilo; CUNHA, Mario Viola de Azevedo. Risco e informação pessoal: o princípio da finalidade e a proteção de dados no ordenamento brasileiro. **Revista Brasileira de Risco e Seguro**, v. 5, n. 10, 85-102, 2009. Disponível em: http://hdl.handle.net/1814/13485. Acesso em: 3 out. 2022.

[21] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

Na visão de Stefano Rodota[22], o direito buscando o controle jurídico da revolução informacional, passou à onda de leis de proteção de dados, chamadas leis de primeira geração. E assevera que a finalidade das leis desta geração era de responder às preocupações sobre violação da intimidade individual que partiriam dos avanços tecnológicos.

A primeira geração de leis se insere no contexto do Estado Moderno, onde o Estado se utilizava de grandes bancos de dados, pois o controle da população se dava por meio de obtenções massivas de informações sobre os indivíduos. Dessa forma, segundo Doneda[23]:

> O núcleo dessas leis girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle a posteriori por órgãos públicos. Essas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) dessas normas.

Nessa perspectiva, o Estado foi então centralizado como o destinatário desses regulamentos, que se direcionavam diretamente à própria tecnologia. Um exemplo das leis de primeira geração é o Privacy Act, norte-americano de 1974. A primeira geração se estende até o implemento da Bundesdatenschutzgesetz, a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977. Várias leis acerca de proteção de dados foram implementadas na Alemanha nessa época e conforme explica Gasiola[24].

> [...] são reações a projetos estatais para implementar bancos de dados centralizados sobre a população, em meio à euforia tecnológica que marcou o pós-guerra. O choque entre a recente lembrança (ou presença) dos governos autoritários e a iminência de tais projetos levou ao reconhecimento expresso da proteção de dados perante as pretensões públicas de aumentar seu poder informacional. O objetivo dessas leis era, acima de tudo, estabelecer limites e garantir a transparência na criação de bancos de dados.

---

[22] RODOTA, Stefano. **Uno statuto giuridico globale dela pesona elettronia**. Discurso proferido na 23ª Conferência Internacional sobre a Privacidade e a proteção de Dados Pessoais em Paris. 24 set. 2001. Disponível em http://intelex .it/675/rodotat.htm. Acesso em 20 jun.2022.

[23] DONEDA, Danilo. Princípios da proteção de dados pessoais. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coord.). Direito Internet III. São Paulo: Quartier Latin, 2015. v. 1: Marco Civil da Internet (Lei n.12.965/2014).

[24] GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha.** 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em 14 jun. 2022.

Essa geração de leis baseada somente em autorizações tornou obsoleta, pois, frente ao avanço da tecnologia, o tratamento de dados passa a ser feito além do domínio governamental, sendo feito também por entes privados. Portanto, esse cenário ensejou a segunda geração de leis, em que, segundo Bioni[25] , o usuário, mediante o seu consentimento tem o poder de participar do processo de tratamento de dados, em fases como a coleta, uso e compartilhamento de seus dados pessoais.

Neste contexto histórico, surge, segundo Laura Schertel Mendes[26], a primeira geração de normas de proteção de dados pessoais: as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-pfalz (1974) e lei Federal de proteção de Dados da Alemanha (1977).

A segunda geração aborda questões sobre o consentimento do cidadão e o exercício de sua liberdade de escolha, no contexto de Estado Social. A principal diferença em comparação às leis de primeira geração é a melhor compreensão pelos legisladores do fenômeno computacional. Na perspectiva de Danilo Doneda[27], percebeu-se que o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para sua efetiva participação na vida social.

A terceira geração de leis se preocupa mais com a tutela do direito à privacidade, indo além da liberdade de ceder ou não os dados, mas sim em garantir a efetividade deste direito. Nessa perspectiva, afirma Bioni[28] que se amplia a participação do indivíduo agora para todas as fases. Os regulamentos crescem até atingir o conceito central de autodeterminação informativa. Nas palavras de Doneda[29] :

> A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes proporcionando o efetivo exercício da autodeterminação informativa.

---

[25] BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

[26] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

[27] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[28] BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

[29] DONEDA, Danilo. Princípios da proteção de dados pessoais. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coord.). **Direito Internet III**. São Paulo: *Quartier Latin*, 2015. v. 1: Marco Civil da Internet (Lei n.12.965/2014).

Porém, essa geração só abarcou uma parcela de indivíduos e isso fez com que a terceira geração se tornasse insuficiente, caminhando assim para a quarta geração, que prevalece até hoje. Sendo que, com a terceira geração, as pessoas poderiam participar diretamente da decisão sobre quais dados seriam compartilhados ou não. Como exemplos de leis da terceira geração é possível citar a emenda à lei federal de proteção de dados pessoais alemã de 1990, a emenda da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda.

Na visão de Doneda[30], a terceira geração é resultado da proliferação dos bancos de dados interligados, possuindo como marco a decisão do Tribunal Constitucional Alemão o qual declarou inconstitucionalidade em parte da Lei do Censo, surgindo então alterações na Lei Federal de Proteção de dados alemã de 1990 e na Noruega, emenda na lei da Áustria de 1989 e previsão constitucional de proteção de dados pessoais na Holanda.

Mencionado por Bioni[31], esta geração alcançou o êxtase da própria terminologia do direito à autodeterminação informativa, possibilitando que o indivíduo possuísse um controle mais extensivo sobre suas informações pessoais.

Na quarta geração, as normas setoriais sobre proteção de dados são complementadas por normas setoriais suplementares, incluindo nela também a Diretiva Europeia sobre a proteção de dados de 1995 (95/46/EC), a norma precursora do Regulamento Geral de Proteção de Dados que entrou em vigor em 2018, mais conhecido como *General Data Protection Regulation* (GDPR)[32].

A discussão sobre o que hoje se conceituaria como privacidade originou-se a partir do momento em que as tecnologias se tornaram invasivas, dando margem à divulgação de informações da esfera privada do indivíduo. Segundo Mendes[33], um dos marcos para essa discussão foi o artigo *the right of privacy* (o direito à privacidade), escrito por *Warren* e *Brandeis*.

---

[30] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[31] BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

[32] UNIÃO EUROPEIA. **Article 29 working party**. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em:https://ec.europa.eu/justice/article 29/documentation/opinionrecommendation/files/2014/wp217_en.pdf. Acesso em: 2022.

[33] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

Para Cancelier,[34] concepção de privacidade, até aqui, era a assumida pelo jurista Thomas McIntyre que cunhou em 1888 a expressão *right to be let alone* (o direito a estar só).

Destaca-se também que o *right to be let alone*, chamado de “o direito de ser deixado sozinho” ou “direito de estar só”, é utilizado por Warren e Brandeis como um argumento para defender o direito de privacidade. É caracterizado como pioneiro do direito à privacidade nos EUA e, mais tarde como o direito à personalidade de cada um referindo-se à doutrina de Warren e Brandeis[35] como o direito a determinar em que medida os pensamentos, os sentimentos e as emoções serão comunicados a outrem.

Percebe-se que o direito à privacidade na época tinha cunho fortemente individualista e era visto como um direito negativo. Tendo em vista, dizer que o direito à privacidade estaria sendo garantido desde que o Estado se abstivesse de adentrar na esfera individual de cada um. Essa perspectiva era condizente com a primeira geração de direitos fundamentais em que se inseria, vinculada diretamente com o direito à liberdade.

Essa conceituação começa a assumir novos delineados no fim do século XX, aproximadamente em 1960, com o avanço das tecnologias e frente a uma “capacidade técnica cada vez maior de recolher, processar e utilizar a informação”. Junto a isso, cresce a democratização do interesse pela tutela de sua privacidade e de seu exercício[36].

Com o tratamento informatizado de dados surgiu e ganhou enfoque, houve a necessidade de que o conceito de direito à privacidade se modificasse a fim de abranger a proteção de dados pessoais. Segundo Mendes[37], aproximadamente em 1970, são vistas decisões jurídicas e legislações que afirmam que os dados

---

[34] CANCELIER, Mikhail Vieira de Lorenzi; CRISTO, Camila Kohn de; MAFRA, Gabriela. Evasão de informações privadas: proteção à privacidade nos casos de pornografia de vingança. *In*: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 4., 2017, Santa Maria. **Anais,** p. 1. Disponível em: https://egov.ufsc.br/portal/conteudo/evas%C3%A3o-de-informa %C3%A7%C3%B5es-privadas-prote%C3%A7%C3%A3o-%C3%A0- privacidade-nos-casos-de-pornografia-de-vingan%C3%A7. Acesso em: 2 jun. 2022.

[35] WARREN, Samuel; BRENDEIS, Louis. The right to privacy. **Harvard Law Review,** v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 13 nov. 2022.

[36] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[37] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

pessoais são uma projeção da personalidade do indivíduo e por isso são hábeis a receber tutela jurídica.

Dessa forma, a evolução do direito à proteção de dados pela perspectiva da União Europeia pode ser dividida em quatro períodos. No primeiro período surgiram as primeiras leis nacionais sobre a temática, ainda nas décadas de 70 e 80. Já no segundo, iniciado a partir da década de 80, ocorre a internacionalização do direito à proteção de dados. No terceiro, vislumbra-se um movimento de internalização no ordenamento jurídico dos países-membros das normas internacionais. E, por fim, o quarto período corresponde à harmonização europeia das normas de proteção de dados pessoais entre 1995 e 2016, com a implementação da Diretiva 95/46/CE e do GDPR[38].

Adiante, as regulamentações sobre proteção de dados passam por diversas fases até chegar ao momento atual em que o direito à proteção de dados adquire o enfoque como um direito fundamental e passa a ter legislações específicas e completas como a LGPD e a GDPR. As doutrinas defendem a visão de Viktor Mayer-Scönberger, que propõe que a regulamentação da proteção de dados pessoais percorreu quatro gerações distintas, que, de acordo com Doneda[39], são "leis que partem de um cerne mais técnico e restrito para, por fim, ampliar as disposições e as técnicas referentes às tecnologias modernas".

Na atualidade, no entanto, onde a hiperconexão e, consequentemente, o monitoramento online é constante, os painéis de coleta de dados pessoais dos consumidores alcançam maior sofisticação e assertividade. Isso tudo porque, por meio da reunião e leitura de dados pessoais, coletados de forma incessante por dispositivos do cotidiano (como celulares), segundo Bioni[40] tornou-se possível inferirem-se:

> (i) riscos de um tomador de crédito sofrer calote, o que auxilia a realizar a calibragem dos juros e concessão de crédito; (iii) parâmetros de saúde dos segurados, facilitando a formatação dos preços para planos de saúde; (iv) o nível de atenção e prudência na direção de automóveis, que pode auxiliar

[38] UNIÃO EUROPEIA. **Article 29 working party**. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em:https://ec.europa.eu/justice/article 29/documentation/opinionrecommendation/files/2014/wp217_en.pdf. Acesso em: 2022.

[39] DONEDA, Danilo. Princípios da proteção de dados pessoais. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coord.). **Direito Internet III**. São Paulo: Quartier Latin, 2015. v. 1: Marco Civil da Internet (Lei n.12.965/2014).

[40] BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

> na oferta e negativa de inclusão de determinado sujeito nos seguros de automóvel; (v) tendências de mercado, possibilitando a diversificação e segmentação dos serviços e produtos; e (vi) direcionamento publicitário preciso, a partir da personalização da comunicação e propaganda.

A despeito destes propósitos, por vezes justificáveis para além da ótica econômica, é certo que o uso de dados pessoais não pode estar submetido tão somente a uma lógica de mercado, sob a pena de esvaziar o conteúdo de um dos atributos da personalidade.

Por estas razões, impulsionadas por escândalos mundiais como o *Cambridge Analytica* e o episódio *Edward Snowden*, é que foram surgindo leis para a proteção de dados pessoais, que, no entanto, ainda conferem demasiado protagonismo à figura do consentimento do titular como expressão central para legitimar a coleta e uso por atores privados[41]. O consentimento este que nestas relações onde a cessão de dados pessoais tem destaque, representa uma ficção: seja sob o aspecto das limitações cognitivas do titular para avaliação.

De acordo com Colombo, Engelmann e Faleiros Júnior[42], quando se referir aos elementos específicos de identidade entende-se que os dados são pessoais e necessitam de cuidados especiais, conforme o Regulamento de proteção de Dados a União Europeia nos termos do artigo 4º, I, devendo promover a privacidade dos dados e por outro lado cumprir o princípio da transparência, sendo assim, a temática foi objeto do artigo 29, no Parecer 2/2016, destacando as medidas para resolver o conflito:

> Ao decidir se os dados pessoais devem estar acessíveis a nível mundial, através de motores de busca externos, é conveniente tem em conta o objetivo de garantir a ampla disponibilização das informações. Se houver interesse público a nível mundial na disponibilização desses dados, sobretudo tendo em conta a categoria dos seus titulares, tal divulgação poderá ser justificada, desde que os potenciais impactos nos direitos e liberdades dos titulares tenham sido tidos em conta. No entanto, se não existir interesse público a nível mundial ou essa ampla divulgação for considerada inadequada, poderá ser preferível disponibilizar os dados

---

[41] BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

[42] COLOMBO, Cristiano; BERNI, Duílio Landell de Moura. ***Privacy* no Direito Italiano: Tríade de Decisões Judiciais Rumo a insights sobre limites conceituais, deslocamento Geográfico e transparência do corpo eletrônico**. *In*: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura. **Tutela jurídica do corpo eletrônico**: novos desafios ao direito digital. [*S.l.*]: Foco, 2022. p. 53-72.

> através de motores de busca internos ou de outros mecanismos de acesso seletivo (por exemplo, com um nome de utilizador ou <captcha>)[43]

A evolução destes regramentos protetivos tenta evoluir na mesma medida das potências de tratamento de dados dos computadores atuais.

A Califórnia é um dos estados americanos com maior nível de proteção à privacidade, citando este direito no primeiro artigo de sua Constituição. O estado aprovou em 2018 a California Consumer Privacy Act (CCPA), com entrada em vigor em 2020, que trata de dados pessoais de consumidores de forma a dar-lhes maior controle sobre suas informações pessoais. A legislação utilizada por este estado, já influenciou diversos estados vizinhos, sendo eles rascunhos para as futuras leis estaduais de proteção de dados[44].

Com o intuito de superar tais desvantagens do enfoque individual conferido pelas outras gerações, surge a quarta geração, vivenciada até os dias atuais, com leis que priorizam os titulares dos dados frente a terceiros que possam manipular suas informações pessoais. Conforme de Doneda[45]:

> Nestas leis procura-se enfocar o problema integral da informação, pois elas presumem que não se pode basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção.

Sendo assim, o consentimento continua sendo o traço marcante dos regulamentos, mas começa a sofrer limites e condições de forma a se adequar à autonomia do titular nesse contexto. Passa a ser, então, tomado como um consentimento livre, informado, inequívoco, explícito e/ou específico. Posto isso, pela grande importância dada ao consentimento nesses regulamentos, os próximos

---

[43] PROTEÇÃO de dados: parecer n.11. Disponível em: https//www.uc.pt/proteção-de-dad0s/proteção_dados-pessoais/pareceres-do_EPD/PO011. Acesso em: 2022. (COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura. **Tutela jurídica do corpo eletrônico**: novos desafios ao direito digital. [*S.l.*]: Foco, 2022).

[44] STOLTZ, Brenda. A new california privacy law could affect every u.s. business – will you be ready? **Forbes**, 2019. Disponível em: https://www.forbes.com/sites/allbusiness/2019/09/07/california-consumer-privacy-act-could-affect-your-business/?sh=6aa04d5c36ac. Acesso em: 22 jun. 2022.

[45] DONEDA, Danilo. Princípios da proteção de dados pessoais. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coord.). **Direito Internet III**. São Paulo: Quartier Latin, 2015. v. 1: Marco Civil da Internet (Lei n.12.965/2014).

tópicos percorrerão a evolução do termo na União Europeia para, enfim, adentrar o assunto na legislação brasileira[46].

A Convenção 108 é regulamentada pelo Conselho Europeu que estabelece a relação entre dados pessoais e o livre fluxo informacional transfronteiriço[47]. Essa Convenção é grande influenciadora da Diretiva Europeia de Dados Pessoais (95/96 EC). Através dessa diretiva é estruturado o modelo europeu, que, conforme indica Doneda[48], trata-se de uma disciplina ampla e detalhada que é transposta para a legislação interna de cada estado-membro. Serve, então, como uma uniformização legislativa.

De acordo com Bioni[49], a inovação trazida por essa regulamentação é hábil a enquadrá-la, inclusive, agora na quarta geração de leis de proteção de dados, pois vê-se que foco da Diretiva gira em torno do titular dos dados e dos data *controllers*.

Em relação às diretivas, cada país possui um determinado prazo para que faça a adaptação, o que ganha o nome de “transposição” e que pode incorrer à resposta pela mora do país diante da Corte Europeia de Justiça (Doneda)[50].

Nota-se que, há um cenário de desigualdade perante o direito de proteção da privacidade e intimidade das pessoas com o aumento no processamento de dados, compartilhamento de informações e no progresso da inteligência artificial[51].

Até a aprovação da Lei Geral de Proteção de Dados Pessoais, o Brasil encontrava-se apenas com normas setoriais sobre a proteção de dados pessoais por meio da Constituição Federal, do Código de Defesa do Consumidor, da Lei do Cadastro Positivo, a Lei de Acesso à Informação, Lei Carolina Dieckmann, o Marco Civil da Internet, entre outras legislações.

---

[46] BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

[47] KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do Brasil (lei nº 13.709/18)**. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf? sequence=1&isAllowed=y. Acesso em: 12 jun. 2022.

[48] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[49] BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

[50] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[51] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

A Constituição Federal assegura que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação[52].

Estabelece ainda a possibilidade da impetração de *habeas data* a fim de assegurar o conhecimento de informações relacionadas à pessoa do impetrante, constantes em bancos de dados ou registros de entidades governamentais ou de caráter público. Tal como, para retificar seus dados, quando não se queira fazer por meio de processo judicial ou administrativo, no âmbito sigiloso[53].

Segundo Danilo Doneda[54], teve se também a disposição constitucional do art. 5º, LXXII e a Lei n. 9.507/1997 conhecida como Lei do *Habeas Data*, que regulam o direito de acesso a informações, também apresentam um dos instrumentos para a proteção de dados pessoais antes da LGPD, reafirma ainda que:

> O Código de Defesa do Consumidor, Lei 8.078 de 1990, em seu artigo 43, disciplinou acerca de bancos de dados de informações de consumidores. Observa-se que, a legislação consumerista optou por conceder direitos como: acesso, retificação, cancelamento, bem como princípios relacionados com a transparência e limitação temporal para que o consumidor exerça o controle de suas informações, ou seja, a autodeterminação informacional[55].

A matéria de proteção de dados no Brasil antes da Lei Geral apoiava-se em grande parte me outros ramos do direito como o Código de Defesa do Consumidor, determina no art. 43[56]:

> O consumidor, sem prejuízo do disposto no art.86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as respectivas fontes.

Com isto, para Bruno Bioni[57], o Código de Defesa do Consumidor buscou conferir a autodeterminação informacional conforme já mencionado anteriormente, o

---

[52] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 jun. 2022.

[53] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 jun. 2022.

[54] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

[55] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[56] BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em: 20 jun. 2022.

que perpassa desde regras para garantir a exatidão dos dados até temporais para seu armazenamento.

A questão também foi abordada pelo Código Civil pelo art. 186 “Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito” e art. 927 “Aquele que, por ato ilícito (arts.186 e 187), causar dano a outrem, fica obrigado a repará-lo.

A Lei do Cadastro Positivo, Lei 12.414 de 2011, diz respeito à formação de bancos de dados de adimplentes para a finalidade de concessão de crédito. Dentre os direitos previstos, o titular dos dados pessoais possui o dever de gerenciá-los, tendo, portanto, novamente o referencial da autodeterminação informacional[58].

De acordo com Danilo Bioni[59], a Lei do Cadastro Positivo, trouxe a peça legislativa orientação de que o titular dos dados pessoais deve ter o poder de gerenciá-los e, ainda, que o gestor da base de dados não deve coletar informações excessivas, sensíveis e sem finalidade vinculada.

De acordo com Krieger[60] e Mendes[61], a Lei do Cadastro Positivo, estabelece regulamentação sobre os dados derivados de operações financeiras e adimplementos dos consumidores, que facilitam a concessão de crédito é uma lei que consolida a evolução do conceito de autodeterminação informativa no ordenamento, na medida em que coloca o consentimento como necessário para o compartilhamento de dados ser lícito.

Fundamental observar também que a Lei do Cadastro Positivo exige o consentimento do titular para que de fato ocorra o tratamento de dados, o que por sua vez não era visualizado no CDC, tendo em vista que havia apenas a exigência de uma mera notificação ao consumidor.

---

[57] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[58] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[59] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[60] KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do Brasil (lei nº 13.709/18)**. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf? sequence=1&isAllowed=y. Acesso em: 12 jun. 2022.

[61] MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

A Lei de Acesso à Informação, Lei 12.527 de 2011, determina procedimentos a serem observados pelos órgãos públicos, com o objetivo de garantir o acesso a informações a todos, de acordo com o direito fundamental previsto no inciso XXXIII do artigo 5º da Constituição Federal[62].

A Lei Carolina Dieckmann, Lei 12.737 de 2012, tipificou como crime a invasão de dispositivo informático alheio, o que gerou o aumento da proteção da privacidade dos usuários[63].

O Marco Civil da Internet, Lei 12.965 de 2014, cujo impulso se deu pela denúncia realizada por *Snowden*, no escândalo de espionagem do governo americano, estabelece direitos e garantias do cidadão para o uso da internet no Brasil. Segundo a análise dos dispositivos desta legislação, percebe também como característica a autodeterminação informacional para a proteção de dados pessoais[64].

Para Bioni[65], o Marco Civil da Internet se constitui como uma reação à tentativa de regular o uso da internet por meio de leis penais, já que uma técnica prescritiva e restritiva para regular o uso da internet poderia resultar em um retardo da inovação tecnológica no país. Por isso, essa legislação se afasta dessa técnica e busca regular o uso da internet, conferindo direitos e garantias do cidadão nas relações travadas no meio virtual, de uma forma principiológica.

Portanto, o Marco da Internet, regula a tratativa de dados pessoais, como exemplo o art. 3º, III que inseriu a proteção de dados pessoais em seus princípios, o art. 7ºm VII, informa os direitos dos usuários em não terem seus dados pessoais fornecido sem consentimento livre ou em possuir informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais. Assim também mencionado nos art. 11 e art. 16:

> Art.11. Em qualquer operação de colete, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente

---

[62] OLIVEIRA; Marco Aurélio Belizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

[63] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[64] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[65] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

> respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações e dos registros.
>
> Art.16. Na provisão de aplicação de internet, onerosa ou gratuita, é vedada a guarda: I – dos registros de acessos a outras aplicações de internet sem que o titular dos dados tenha consentimento previamente, respeitado o disposto no art. 7º; ou II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular[66].

O desenvolvimento da tecnologia e da internet possibilitou que diversos tipos de informações e dados passassem a circular pelas redes de comunicação, ocasionando um crescimento exponencial da informação e, paralelamente uma preocupação com a privacidade, pois os dados pessoais[67] passaram a obter um valor econômico e a servir como ferramenta para as organizações públicas e privadas angariar vantagens pecuniárias, políticas, dentre outras.

Nesta lei, já há menção expressa ao consentimento e sua adjetivação, tendo em vista que, principalmente após o escândalo, buscou-se conferir proteção especial ao titular dos dados, dando a ele participação no processo de tratamento de dados. Todavia, conforme explica Malheiros (2017)[68], ainda não havia uma legislação que tratasse diretamente da proteção de dados.

2.1.2 Lei geral de proteção de dados – LGPD

A sociedade da Informação está em evidência na atualidade e com isto, a proteção de dados pessoais se apresenta como um delicado desafio a ser enfrentado pelo direito contemporâneo. Essa nova forma de organização social foi sedimentada em razão da evolução tecnológica recente, que criou mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais imaginável. Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais. Há uma nova

---

[66] BRASIL. **Lei 10.406, de 10 de janeiro de 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso: 20 jun. 2020.

[67] Serão considerados dados pessoais os descritos nos incisos I e II do artigo 5º da LGPD, in verbis: "Art. 5º Para os fins desta Lei, considera-se: 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; [...]"

[68] MALHEIROS, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet**: uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade de Brasília, 2017. Data da publicação: 8 jan. 2018. Disponível em: bdm.unb.br/handle/10483/18883. Acesso em: 13 jun. 2022.

compreensão (mais abreviada) da relação entre tempo-espaço, o que outrora acarretava maior cadência às interações sociais[69]. De um lado tem-se uma excessiva velocidade dos avanços tecnológicos relacionados a esses ativos econômicos, e por outro, encontra o demorado processo legislativo intrínseco à produção das normas jurídicas. A proteção de dados já possui base normativa Constituição Federal (CF/88)[70], a qual preconiza a inviolabilidade da intimida e vida privada, autodeterminação informacional e livre desenvolvimento da personalidade.

A ânsia brasileira por legislação protetiva de dados pessoais se fazia presente antes mesmo do vigor do Regulamento Geral de Proteção de Dados da União Européia. Inserir-se entre as nações que protegem os dados de seus titulares tornou-se essencial ao jogo político internacional. Para o País se pautar fortemente no regulamento europeu significava adequar às quatro gerações sobre a proteção de dados pessoais[71].

Contudo, mesmo com uma maior aproximação de proteção de dados, o Marco Civil da Internet, ainda era consideravelmente limitado por ser aplicável apenas ao ambiente digital. Trata-se de uma lei que buscou regular a internet. Criou-se então a LGPD, lei de nº 13.709, de 14 de agosto de 2018, é uma Lei Federal que se dedica à vulnerabilidade do titular de dados pessoais, cuja finalidade é a proteção das pessoas naturais contra o tratamento ilegal destes dados realizado por qualquer pessoa, independentemente de ser pessoa física ou jurídica, de direito público ou privado, conforme previsto em seu art. 1°[72]:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

---

[69] BIONI, Bruno Ricardo**. Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019

[70] BRASIL. **Constituição da República Federativa do Brasil de 1988**: emendas constitucionais de revisão. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 set. 2022.

[71] CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. Brasília: Conselho da Justiça Federal, Centro de Estudos Jurídicos, 2021.

[72] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 15 jun. 2022.

Logo, é possível notar que, pelo verbo proteger, contido no referido artigo, o legislador viu o titular dos dados em posição de desigualdade frente ao agente de tratamento, ficando nítida a sua vulnerabilidade[73]. A Lei Geral de Proteção de Dados aplica-se em todos os ambientes e não somente ao digital, alcançando em parte o Poder Público e as transferências internacionais[74].

Sendo assim, a LGPD brasileira surge não com uma proposta de reestruturação de um sistema já posto e sim com a criação de um novo arcabouço jurídico, com novos direitos e proteção à estrutura jurídica. Com isso, regulando todos os setores que porventura se utilizem de dados pessoais.

Conforme entendimento de Danilo Doneda[75], a discussão de uma Lei Geral de Proteção de Dados Pessoais no Brasil tramitou por aproximadamente oito anos. No início, eram órgãos do governo sobre a matéria de Proteção de dados pessoais, como o Departamento de Defesa e Proteção do Consumidor – DPCD, publicando o livro intitulado “A proteção de dados pessoais nas relações de consumo: para além da informação creditícia” [76].

O Ministério da Justiça[77] criou site incentivando debate para obter contribuições destinadas a proteção de dados no período de 30 de novembro de 2010 a 30 de abril de 2011, cujo anteprojeto da lei continha 48 artigos. Obteve cerca de 2.500 contribuições.

A primeira tramitação sobre proteção de dados pessoais não se deu pelo anteprojeto do Ministério da justiça, mas sim pelo Projeto de Lei n. 4060/2012, proposto pelo Deputado Milton Monti (PR-SP). O então projeto em nada assimilava as discussões propostas pelo Ministro da Justiça, possuindo 25 artigos e tratando apenas de direitos do titular e dos requisitos para tratamento de dados pessoais.

---

[73] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[74] CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. Brasília: Conselho da Justiça Federal, Centro de Estudos Jurídicos, 2021.

[75] DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. **Revista Espaço Jurídico**, Joaçaba, v. 12, n. 103, 2011.

[76] BRASIL. Ministério da Justiça. Departamento de Defesa e Proteção do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília: SDE/DPDC, 2010. Disponiel em: htttps;/www.justica.gov/seus-direitos/consumidor/Anexo/manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 20 jun. 2022.

[77] BRASIL. Ministério da Justiça. **Debate público**: proteção de dados pessoais. Disponível em: http://pensado.mj.gov.br/dadospessoais2011/debata-a-norma/ Acesso em: 23 jun. 2022.

Entre as justificativas para tramitação estavam a proteção dos direitos individuais, bem como as recentes transformações tecnológicas[78].

Em 2013 é proposto no Senado Federal o Projeto de Lei n. 330/2013 pelo Senador Antonio Carlos Valadares (PSB/SE) com 19 artigos, focando no direito dos titulares, tratamento de dados de bancos de dados, citando em sua justificativa o romance 1984 de George Orwell, bem como as denúncias de Edward Snowden[79].

Em 2014, houve o primeiro grande caso brasileiro de utilização de perfiz comportamentais em detrimento do consumidor-usuário, sendo aplicada pelo DPDC multa de R$3,5 milhões à TNL PCS S/A (Oi). Foi constatado no processo administrativo que a parceria da Oi com uma empresa britânica Phorm consistia no desenvolvimento de software que mapeava o trafego de dados do consumidor na internet de modo a compor seu perfil de navegação[80].

Este caso veio a reforçar a necessidade de um caráter de punição daqueles que atuassem em desobediência às normas de proteção de dados pessoais.

Em 2015, iniciou-se a segunda fase com uma discussão mais técnica e aprofundada, que se manteve até a promulgação da lei em 2018. Ainda em 2015, o Ministério da Justiça disponibilizou o texto do anteprojeto da LGPD com 52 artigos para novo debate público[81].

Com tramitação lenta até 2015, os esforços estavam centrados na elaboração do Marco Civil da Internet, Lei n. 12.965/2014, já mencionada anteriormente, que segundo Bruno Bioni[82], teve sua tramitação acelerada pelos escândalos de espionagem:

> O art. 7º detinha, apenas, cinco incisos, passando a ter no cenário ‘pós-snowden’, oito incisos, sendo que todos eles foram direcionados para a proteção dos dados pessoais. Com o acréscimo de tais dispositivos, houve

---

[78] CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. Brasília: Conselho da Justiça Federal, Centro de Estudos Jurídicos, 2021.

[79] CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. Brasília: Conselho da Justiça Federal, Centro de Estudos Jurídicos, 2021.

[80] BRASIL. Ministério da Justiça. **Multa Oi por monitorar navegação de consumidores na internet**. Disponível em: https://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em 27 jun. 2022.

[81] BRASIL. Ministério da Justiça. **Proteção de dados pessoais**. Disponível em: https:// http://pensando.mj.gov.br/dadospessoais/. Acesso em 27 jun. 2022.

[82] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

> uma alteração de ordem qualitativa no arranjo normativo do MCI, tendo sido o usuário eleito como o grande protagonista para desempenhar a proteção de seus dados pessoais.

Foram realizadas pela comissão especial onze audiências públicas e um seminário internacional, ocorreram constantes debates a fim de avaliar as diferentes perspectivas da lei e contrapor tanto a visão consumerista como a visão empresarial, movimentando de forma ampla diversos atores sociais.

O Brasil apresentou pedido formal de acessão à Organização para a Cooperação e Desenvolvimento Econômico, seguida à execução de programa de trabalho que resultou do Acordo de Cooperação assinado entre Brasil e a OCDE em 2015[83].

A OCDE desenvolveu análise sobre o Governo Digital brasileiro pulicada em 2018, realizando recomendações para atingir um governo digital como estabelecer comunicações “intrafederativas” para expandir de forma consistente o governo digital entre estados e municípios[84]. Em 2019, o Brasil renunciou tratamento especial concedido a países em desenvolvimento pela Organização Mundial do Comércio (OMC), com o objetivo de se tornar parte da OCDE[85]. Até o momento, não houve a aceitação do País como membro, no entanto pode participar de Comitês da Organização e de inúmeras instâncias de trabalho.

Diante do caso de vazamento de dados da *Cambridge Analytica* em 2018, foi um ano propício para a provação da LGPD, havendo inclusive, requerimento pela Comissão Especial para a análise dos impactos da coleta ilegítima de dados relativa aos projetos que tramitavam na Câmara[86]. Por fim, percebe-se que a ampla discussão legislativa desenvolveu um documento fruto de amplo debate entre os mais diversos mediadores da sociedade.

---

[83] BRASIL. Ministério de Ciência e Tecnologia, Inovações e Comunicações. **Estratégia brasileira para a transformação digital**: e-digital. Brasília, 2018. Disponível em: https://www.mctic.gov.br/mctic/export/site. Acesso em 27 jun. 2022.

[84] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Digital government review of Brazil. **OCDE Digital Government Studies**, p.1-146, 2018. Disponível em: http//www.ocde.org/governance/digital-government-review-of-brazil-97899264307636-em.html Acesso em: 27 jun. 2022.

[85] CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. Brasília: Conselho da Justiça Federal, Centro de Estudos Jurídicos, 2021.

[86] CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. Brasília: Conselho da Justiça Federal, Centro de Estudos Jurídicos, 2021.

A LGPD, em seu art. 2°[87], define de forma clara e direta, em 7(sete) incisos, quais são seus fundamentos, sendo eles: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VII - a livre iniciativa, a livre concorrência e a defesa do consumidor; VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Verifica-se que além do respeito à privacidade, à liberdade de expressão, de informação, de comunicação e de opinião, da inviolabilidade da intimidade, da honra e da imagem, como fundamentos da LGPD, vem a demonstrar a preocupação também com direitos fundamentais e essenciais ao desenvolvimento da personalidade do indivíduo. Atualmente não se trata exclusivamente de isolamento ou solidão, mas de conferir o poder ao indivíduo de propiciar o controle pleno da sua privacidade, de suas manifestações, controlando, assim, quem será admitido na esfera de sua vida íntima, e de não ser repreendido por expressar suas posições ideológicas. Nesse sentido, a lei de dados brasileira previu ferramentas para que a pessoa natural tenha maior controle das informações relacionadas à sua vida privada[88].

Ainda, segundo Márcio[89], a pessoa natural, titular do dado pessoal que venha a sofrer tratamento por controlador/operador, tem o pleno direito de saber o que é feito com seus dados e da fidedignidade dos mesmos. Desta forma, por este fundamento, soma-se a possibilidade de manifestação de vontade do titular, que não poderá ser impedida por terceiros, com a obrigação do controlador em prestar informações sobre seus dados.

O legislador menciona na Lei de proteção de dados brasileira que as atividades envolvendo tratamento de dados pessoais deverão observar a boa-fé e 10 (dez) princípios que se correlacionam, distribuídos nos seus incisos, os quais sejam: i) Finalidade; ii) Adequação; iii) Necessidade; iv) Livre Acesso; v) Qualidade

---

[87] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 15 jun. 2022.

[88] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[89] COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

dos Dados; vi) Transparência; vii) Segurança; viii) Prevenção; ix) Não Discriminação; e, x) Responsabilização e Prestação de Contas[90]. Quanto aos princípios jurídicos, primeiro deve-se compreender que, ao se falar desta fonte do direito, está a se falar do suporte teórico e dos valores sobre os quais o legislador pátrio se baseou no momento de criação da norma.

Para que a dimensão da LGPD possa ser corretamente compreendida de forma objetiva e importante a definição de alguns conceitos. De acordo com KLEE e NETO[91], temos o seguinte, sobre os conceitos legais abordados na lei:

> A LGPD define alguns conceitos que nortearão a sua interpretação e aplicação. É um ponto bastante positivo da Lei. Entre os conceitos trazidos no texto legal, destaque deve ser dado às definições de dado pessoal, de dado pessoal sensível, dado anonimizado, banco de dados, tratamento e consentimento. Mas a LGPD não se restringe a apenas esses conceitos, trazendo outros.

Portanto, a LGPD possui alguns conceitos que nortearão a sua interpretação e aplicação, sendo pontos positivo da lei e trazidos no texto legal com a finalidade de melhor explicação.

2.2 Autoridade nacional de proteção de dados (ANPD) e sanções aplicáveis

Da mesma forma que se deu na União Europeia e nos demais países que já internalizaram uma cultura a respeito da Proteção de Dados, o Brasil também reconheceu a impossibilidade de que a autodeterminação informativa fosse completa simplesmente de acordo com as disposições da lei geral e com as ações conscientes do próprio titular dos dados.

Nesse cenário, a Autoridade Nacional de Proteção de Dados (ANPD), foi criada em 2018 e sancionada em 2019, inicialmente, no tocante a sua criação, sofreu um veto presidencial em razão de vício de iniciativa, posteriormente foi

---

[90] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 15 jun. 2022.:

[91] KLEE, Antônia Espindola Longoni, NETO, Alexandre Pereira Nogueira. **Proteção de dados pessoais**: privacidade versus avanço tecnológico. Caderno Adenauer 3 Schutz von persönlichen Daten (2019). PDF disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em 08 nov. 2022

alterada pela Medida Provisória no 869/18 e pela Lei no 13.853/19. Portanto, a criação dessa nova autoridade é de suma importância, pois a mesma busca medidas viáveis de implementação da nova regulamentação de proteção de dados[92].

O Governo Federal veio a editar o Decreto nº 10.474 de 26 de agosto de 2020 o qual aprovou a Estrutura Regimental e o Quadro de cargos em comissão e funções de confiança da Autoridade Nacional de Proteção de Dados, logo após o Senado Federal aprovar a conversão em lei da Medida Provisória nº 959 de 2020 a qual deu vigência imediata a Lei Geral de Proteção de Dados[93].

De acordo com as novas regras fixadas pela MP 1.124/2022[94] a ANPD foi, então, transformada em autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio. O fato de a ANPD ter sido transformada em uma autarquia modifica bastante suas prerrogativas de atuação. A ANPD possui uma estruturação que é composta pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Ouvidoria, Corregedoria, Conselho Diretor, Órgão de assessoramento jurídico e Unidades Administrativas necessárias à aplicação da Lei, sendo esses diretores membros do Conselho, escolhidos e nomeados pelo Presidente da República[95].

A autoridade Nacional de proteção de dados é um dos pilares da proteção de dados, pois é com sua existência e sua independência que possibilita a execução das funções inerentes ao bom andamento da proteção de dados, cujas funções seriam: fiscalizar o cumprimento das regras sobre o tema, especificar padrões técnicos e administrativos para garantir a segurança das atividades de coleta e tratamento de dados, elaborar regulamentos, analisar os Códigos de Boas Práticas (as normas deontológicas), verificar o nível de proteção de outros países para receber dados pessoais dos cidadãos de seu país, receber e apreciar as reclamações dos indivíduos, aplicar sanções administrativas quando necessário,

---

[92] PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 – LGPD. 2. ed. São Paulo: Saraiva Educação, 2020. E-book. Disponível: https://books.google.com.br/books?hl=ptBR&lr=&id=oXPWDwAAQBAJ&oi=fnd&pg=PT13&dq=Autoridade+nacional+de+prote%C3%A7ao+de+dados&ots=k8_mBpMKYJ&sig=b6-fTVclEUdJOpK4jzMU0F5v3Zg#v=onepage&q=Autoridade%20nacional%20de%20prote%C3%A7ao%20de%20dados&f=false. Acesso em: 07 out. 2022.

[93] OLIVEIRA, Felipe. **Senado decide que LGPD entra em vigor agora, mas prazo depende da sanção.** Disponível em: https://bit.ly/33rXZDE. Acesso em: 14 set. 2020

[94] https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/153611 Acesso em 12 nov. 2023

[95] CAPEZ, Fernando. **Lei geral de proteção de dados**: as competências da ANPD e o Procon, 2020. Disponível em: https://economia.ig.com.br/colunas/defesa-doconsumidor/2020-06-12/lei-geral-de-protecao-de-dados-as-competencias-da-anpd-eo-procon.html. Acesso em: 07 nov, 2022.

entre outras que forem necessárias para que o órgão possa cumprir diligentemente com a sua missão precípua, que é a garantia de um sistema eficiente de proteção dos dados pessoais[96].

Os motivos que fundamentaram a criação da ANPD são vários, a saber: a necessidade de fortificar a economia nacional, de criar um órgão com competência reconhecida sobre a matéria, de proteger os direitos constitucionalmente garantidos, tais como privacidade, honra entre outros. Com função primordial de fiscalização e controle do cumprimento da lei pelos agentes que realizam tratamento de dados, utilizam a denominação Autoridade de Controle. Na Seção II da LGPD (Órgão Competente e Conselho Nacional de Proteção de Dados e da Privacidade), falava-se em "órgão competente" e sobre a criação do Conselho Nacional de Proteção de Dados e da Privacidade (arts. 53 a 55)[97]. Mais precisamente no art. 55-J da LGPD, a partir da redação da Lei n. 13.853/2019, traz rol das competências da ANPD, quais sejam:

> I – Zelar pela proteção dos dados pessoais, nos termos da legislação;
> II – Zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
> III – elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> IV – Fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
> V – Apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
> VI – Promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;
> VII – promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;
> VIII – estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;
> IX – Promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;
> X – Dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

---

[96] LIMA, Cíntia Rosa Pereira D. **Autoridade nacional de proteção de dados e a efetividade da lei geral de proteção de dados**. Coimbra: Almedina, 2020. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 12 set. 2022.

[97] LIMA, Cíntia Rosa Pereira D. **Autoridade nacional de proteção de dados e a efetividade da lei geral de proteção de dados**. Coimbra: Almedina, 2020. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 12 set. 2022.

> XI – solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei
> XII – elaborar relatórios de gestão anuais acerca de suas atividades;
> XIII – editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; entre outros.

Portanto, como visto no artigo acima citado (lei 13.853/2019), as competências da ANPD têm um rol extensivo que merece atenção especial para prover o bom andamento da proteção dos dados pessoais.

Quanto às sanções previstas na LGPD, o capítulo VIII é voltado ao processo de fiscalização do cumprimento das regras de tratamento e proteção de dados pessoais, conforme dispostas pelo texto legal. A competência fiscalizatória e sancionatória incumbe majoritariamente à Autoridade Nacional de Proteção de Dados, porém sem excluir o eventual cabimento de demais ações administrativas, civis ou penais aplicáveis a cada caso[98].

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas Lei LGPD, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: Para evitar sanções administrativas vale ressaltar que estão previstas no artigo 52 da LGPD:

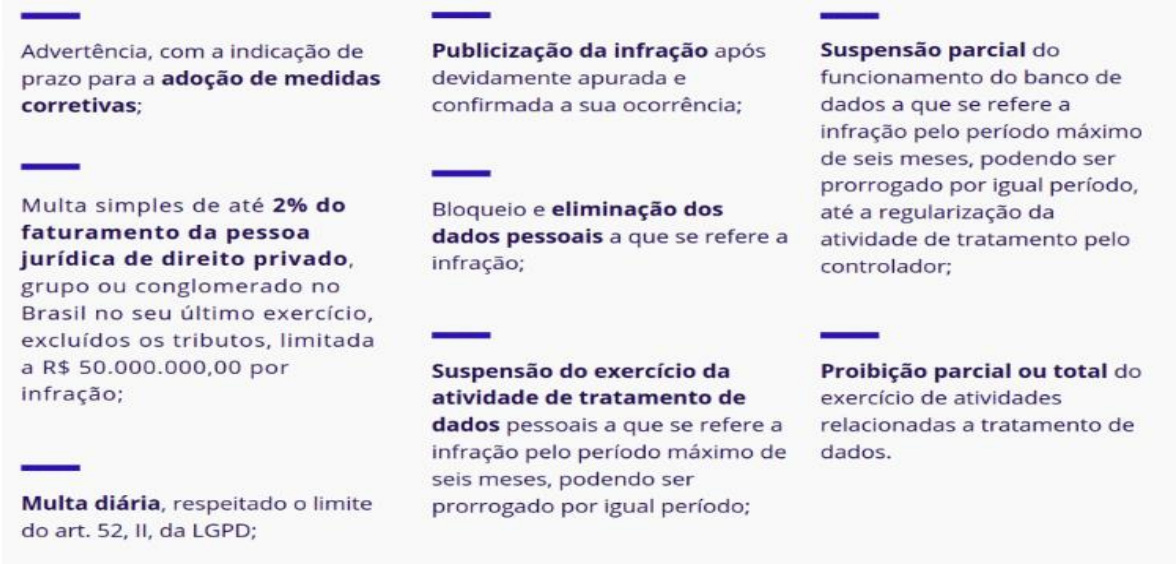
> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I – Advertência, com indicação de prazo para adoção de medidas corretivas;
> II – Multa simples, de 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;
> VII – (VETADO);
> VIII – (VETADO);
> IX – (VETADO).
> 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;

[98] FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. **Comentários à lei geral de proteção de dados**: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 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;
> XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados[99].

Por força da Lei 14.010/20, entrou em vigor de 1º de agosto de 2021, as sanções acompanhadas de punições que podem chegar até 2% do faturamento, com um limite de até 50 milhões de reais.

Figura 1 - Sanções Administrativas previstas na LGPD



Fonte: LPGD...[100]

Há sanções que pretendem estimular o cumprimento de uma determinada regra, como é o caso da multa diária ou do bloqueio dos dados pessoais, mas, por outro lado, há sanções que aparentemente visam castigar o infrator da lei. Sobre isso, devemos entender um pouco mais sobre a natureza das sanções que se pretende evitar.

De acordo com Ricardo Oliveira[101], a lista de sanções é exaustiva, ou seja, a ANPD (Autoridade Nacional de Proteção de Dados) não poderia aplicar sanções

---

[99] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

[100] LGPD: multas e sanções previstas na lei. Disponível em: https://blconsultoriadigital.com.br/lgpd-multas-e-sancoes/. Acesso em: 19 nov. 2022.

[101] OLIVEIRA, Ricardo. **LGPD**: Como evitar as sanções administrativas. São Paulo: Saraiva, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 19 nov. 2022.

diferentes ou não previstas na LGPD, ainda que entenda que sua aplicação favoreceria o cumprimento da lei no futuro, como é o caso de aplicar uma multa bilionária sobre as empresas com alta capacidade financeira, só por considerar que o teto de 50 milhões de reais ser considerado baixo para elas. Nesse caso a autoridade dispõe de outros tipos de sanção e sua escolha deve se fazer com inteligência, para que não se cometa injustiça.

Também, segundo o autor supra citado, LGPD estabeleceu os critérios para dosimetria da sanção: (i) a gravidade e a natureza das infrações e dos direitos pessoais afetados; (ii) a boa-fé do infrator; (iii) a vantagem auferida ou pretendida pelo infrator; (iv) a condição econômica do infrator; (v) a reincidência; (vi) o grau do dano; (vii) a cooperação do infrator; (viii) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; (ix) a adoção de política de boas práticas e governança; (x) a pronta adoção de medidas corretivas; e, (xi) a proporcionalidade entre a gravidade da falta e a intensidade da sanção[102].

Sendo assim, deve-se esperar que a ANPD, na aplicação das sanções administrativas, não deixe de lado a proporcionalidade e razoabilidade da punição, pois, ao mesmo tempo que se quer punir o infrator, não se pretende levá-lo à falência ou à interrupção de suas atividades econômicas, exceto se as mesmas violarem a LGPD de forma intolerável à sociedade em geral.

As empresas precisam elaborar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que representa um documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e os direitos fundamentais dos titulares desses dados[103]. Segundo o inciso XVII do art. 5º da LGPD, o RIPD é a documentação que deve ser mantida pelo controlador dos dados pessoais.

---

[102] OLIVEIRA, Ricardo. **LGPD**: Como evitar as sanções administrativas. São Paulo: Saraiva, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 19 nov. 2022.

[103] CRAVO, Victor *et al.* **Guia de boas práticas**: lei geral de proteção de dados (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-dedados/GuiaLGPD.pdf. Acesso em: 22 ago. 2022.

2.3 Normas Brasileiras (NBR), Organização Internacional para Padronização (ISO) relacionadas com Gestão de Risco

A NBR/ISO 27701[104] tem o como objetivo estabelecer, instituir, manter e melhorar continuamente o Sistema de Gestão da Privacidade da Informação (SGPI). Este último trata das questões referentes a riscos e controles de Dados Pessoais. Além disso, a norma define requisitos e guias para auxiliar o tratamento de dados pessoais pelos controladores responsáveis e transparência no processamento de tais dados. O SGPI é integrado ao Sistema de Gestão da Segurança da Informação (SGSI), definido na NBR/ISO 27001 e, portanto, as normas 27701 e 27001 são correlacionadas. Também de acordo com a norma 27701 e da 27001, a avaliação de riscos deve ser um processo que define critérios de aceitação e de desempenho da avaliação de riscos da segurança da informação de forma contínua, produzindo resultados comparáveis, válidos e consistentes. Para o tratamento do risco é necessário instituir e aprovar: um plano de tratamento do risco (a ser apreciado pelos responsáveis pelo risco); tratamento dos riscos; e aceitação de riscos residuais. Em caráter exemplificativo, ambas as normas relacionam os riscos às dimensões da qualidade de dados, tais como a perda de confidencialidade, integridade e disponibilidade da informação. Podemos então fazer um comparativo entre os riscos e a qualidade de dados. Neste contexto de projetos de dados, um risco seria um evento incerto que impacta direta ou indiretamente na qualidade dos dados, e sua identificação pode estar associada aos controles e medições da qualidade de dados.

As normas 27701 e 27002[105] dedicam um tópico para discorrer sobre vulnerabilidades que devem ser consideradas quando os dados são acessados através de dispositivos móveis ou via estações de trabalho remoto. Isto ocorre porque, em ambos os casos, envolve-se de forma mais visceral o tráfego dos dados pela rede mundial de computadores. Portanto, neste cenário, é recomendável que sejam observados cuidados especiais, que as normas definem como “ambientes desprotegidos”. Outro aspecto importante a se considerar é a conscientização de

---

[104] ISO CENTRAL SECRETARY. Security techniques — extension to iso/iec 27001 and iso/iec 27002 for privacy information management — requirements and guidelines. Standard ISO/IEC TR 27701:2019, International Organization for Standardization, Geneva, CH, 2019.

[105] KANWAL, T., SHAUKAT, S. A. A., ANJUM, A., CHOO, K.-K. R., KHAN, A., AHMAD, N., AHMAD, M., KHAN, S. U., ET AL. Privacy-preserving model and generalization correlation attacks for 1: M data with multiple sensitive attributes. Information Sciences 488 (2019).

todos os colaboradores da organização quanto ao tratamento de Dados Pessoais. De fato, principalmente se levado em conta o pouco tempo em que essas questões têm ganhado foco nos debates sobre segurança, a aculturação dos princípios de proteção e privacidade tem que ser alavancada por ações de conscientização, educação e treinamento em segurança da informação e privacidade.

A ISO/IEC 27002[106] é um código de práticas para a gestão de segurança da informação. Esta norma pode ser vista como um prelúdio para o desenvolvimento de diretrizes e princípios gerais sobre metas geralmente aceitas para a gestão da segurança da informação. A gestão da segurança da informação necessita de um planejamento adequado ao negócio da organização. Os objetivos de controle e os controles têm como finalidade ser implementados para atender aos requisitos identificados por meio da análise/avaliação de riscos. A norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades interorganizacionais. Deve ser elaborado um plano estratégico de segurança que atenda a toda a organização. O plano deve identificar o cenário da organização aonde a segurança da informação deverá atuar.

É importante destacar a definição de controle e os seus componentes, conforme descrito na ISO/IEC 27002[107]: a definição de controle compreende a forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

A norma internacional ISO/IEC 27005 é parte da série de normas da ISO/IEC 27000, a qual é uma série bem estabelecida de normas de gestão de segurança da informação e é aceita em todo o mundo. O âmbito de aplicação destas normas pode ser na organização como um todo, ou em partes, como os processos de um departamento, uma aplicação de TI ou uma infraestrutura de TI[108] (BECKERS et al, 2011). Esta norma internacional fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo

---

[106] ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005

[107] ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005

[108] BECKERS, K.; SCHMIDT, H.; KÜSTER, J. C. & FAßBENDER. S. Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. Sixth International Conference on Availability, Reliability and Security, 2011.

particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI).

Também é importante evidenciar a definição de risco de segurança da informação e seus componentes, segundo a ISO/IEC 27005[109]:

> Riscos de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização. É medido em função da combinação da probabilidade de um evento e de sua consequência.

A norma ISO/IEC 27005[110] convém que a gestão de riscos de segurança da informação possa contribuir para:

> • Identificação de riscos; •Análise/avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência; • Comunicação e entendimento da probabilidade e das consequências destes riscos; • Estabelecimento da ordem prioritária para tratamento do risco; • Priorização das ações para reduzir a ocorrência dos riscos; • Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos; • Eficácia do monitoramento do tratamento do risco; • Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos; • Coleta de informações de forma a melhorar a abordagem da gestão de riscos; • Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visam à identificação, avaliação e priorização de riscos, seguido pela aplicação coordenada e econômica dos recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, reduzindo o risco a um nível aceitável.

O uso de padrões para o desenvolvimento de uma gestão de riscos baseada na norma ISO/IEC 27005 pode contribuir para uma melhoria na definição de processos para gestão de segurança da informação, a fim de dar maiores garantias para o cumprimento dos requisitos definidos pelas normas. Propor a utilização de padrões de segurança pelas organizações pode ser uma garantia para o atingimento

---

[109] ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005

[110] ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2008.

dos objetivos a qual a norma se propõe. Cabe a cada organização escolher os padrões que mais se adequam aos seus objetivos de negócios.

A ISO 29100 fornece uma estrutura de alto nível para a proteção de dados pessoais dentro de sistemas de informação, dispondo de aspectos técnicos, organizacionais e procedurais dentro desta estrutura, ajudando empresas a definir seus requisitos de privacidade a partir de um entendimento comum sobre proteção de dados privados dos titulares[111].

Os principais objetivos da norma 29100 são de estabelecer uma terminologia comum sobre privacidade, definir os atores e seus papéis no processamento de dados pessoais, descrever as considerações para proteção da privacidade, e fornecer as referências para os princípios de privacidade para tecnologia da informação. Com foco em unificar os conceitos e estabelecer o entendimento comum de suas definições, fornecendo inclusive um anexo com as relações entre os conceitos da 27001 e 29100. Dentre estes conceitos, e claro como especialista em gestão de riscos, o conceito de *privacy risk* faz todo o sentido (inclusive alinhado com a ISO 31000)[112]. Sendo assim, a norma ISO 29100, é fundamental para entendimento e adoção de linguagem comum para uma estrutura de privacidade para qualquer empresa. Entende-se, portanto, que esta norma seja de leitura fundamental para as empresas que desejam implantar uma estrutura de privacidade para atendimento ao requisito regulatório.

[111] https://www.linkedin.com/pulse/iso-29100-e-lgpd-luiz-eduardo-poggi/?originalSubdomain=pt Acesso em 17 jan, 2023.
[112] https://www.linkedin.com/pulse/iso-29100-e-lgpd-luiz-eduardo-poggi/?originalSubdomain=pt Acesso em 17 jan, 2023.

3 GOVERNANÇA DE DADOS PARA GESTÃO DE RISCOS EM PROTEÇÃO DE DADOS PESSOAIS

O termo governança tem sido extremamente utilizado nos últimos anos. Inicialmente o termo foi utilizado para a Governança Corporativa logo após as ações de controle para que as corporações não sofram as ações de administrações fraudulentas e/ou irresponsáveis. O fato de tal situação ter acontecido com algumas grandes organizações que aparentemente não corriam riscos fez com que legislações e regulamentos surgissem e fossem aprovados para minimizar esses riscos[113].

O risco pode ser considerado uma via de mão dupla, pois o retorno de determinado empreendimento está associado ao grau de risco envolvido. Em finanças, a relação risco/retorno indica que, quanto maior o nível de risco aceito, maior o retorno esperado do investimento, e, nesse sentido, empreender significa buscar um retorno econômico-financeiro adequado ao nível da atividade[114].

Conforme resume Gitman[115], risco, no contexto econômico, é a chance de perda financeira. Porém, tem se difundido um debate em torno da definição deste conceito que leva a ampliar as perspectivas de risco para uma interpretação mais dilatada nos ambientes corporativos.

A implementação da governança é exigida, pelo Art. 50, por processos, regras e normas que comtemplem o regimento de funcionamento, procedimentos, a segurança da informação, o treinamento e ações educativas, os mecanismos de monitoramento e controle e resposta aos riscos, entre outros, bem como, a demonstração dos procedimentos adotados pela organização à ANPD[116]. Sendo:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas

[113] FONTES, Edison. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2008.
[114] SILVA, Daniel C.; COVAC, José R. **Compliance como boa prática de gestão no ensino superior privado**. 2015. 9788502624382. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502624382/. Acesso em: 20 jun. 2022.
[115] GITMAN, Lawrence J. **Princípios de administração financeira**. São Paulo: Pearson Prentice Hall, 2010.
[116] BRASIL. Ministério de Ciência e Tecnologia, Inovações e Comunicações. **Estratégia brasileira para a transformação digital**: e-digital. Brasília, 2018. Disponível em: https://www.mctic.gov.br/mctic/export/site. Acesso em 27 jun. 2022.

> de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais[117].

A consideração dos riscos e benefícios do tratamento de dados relativos a cada setor específico define no parágrafo 1º do art. 50 que o estabelecimento das regras de boas práticas deve levar em consideração a relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular[118]. Ou seja, confirma-se o cabimento de que tais regras de boas práticas sejam ponderadas conforme a realidade de cada setor específico - e também conforme o tipo e a natureza dos riscos envolvidos com o tratamento de dados pessoais.

Os princípios da segurança e prevenção constantes no parágrafo 2º do art. 50, da LGPD prevê a possibilidade implementação de programa de governança em privacidade e a demonstração de sua efetividade. Ambos os princípios envolvem normas abertas, que remetem à utilização de medidas técnicas e administrativas não especificadas e que, evidentemente, variam de acordo com a evolução social, com a prática do setor e com o avanço da tecnologia disponível[119].

Portanto, olhando por este prisma é muito relevante que as associações e entidades sindicais possam definir e especificar essas medidas em normas específicas de boas práticas. Além de elas serem discutidas e definidas pelo próprio setor econômico, levarão em conta as realidades e circunstâncias específicas desse setor.

A proteção de dados não tem por objetivo inviabilizar a coleta de dados para conhecimento do público alvo e aprimoramento das atividades empresariais. Todo empresário tem legítimo interesse de conhecer quem são seus consumidores, empregados e candidatos a emprego[120]. Entretanto, a LGPD esclarece que os dados

---

[117] ARTIGO 50 da Lei nº 13.709 de 14 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/topicos/200398676/artigo-50-da-lei-n-13709-de-14-de-agosto-de-2018 Acesso em: 15 jul. 2022.

[118] CARDOSO, André Gushow. **O art 50 da LGPD e a competência da ANPD para reconhecer e divulgar regras de boas práticas e governança**. Disponível em: https://www.migalhas.com.br/depeso/351510/o-art-50-da-lgpd-e-a-anpd-para-reconhecer-e-divulgar-regras Acesso em 15 jul 2022.

[119] ARTIGO 50 da Lei nº 13.709 de 14 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/topicos/200398676/artigo-50-da-lei-n-13709-de-14-de-agosto-de-2018 Acesso em: 15 jul. 2022.

[120] FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. [*S.l.*]: Thomson Reuters Brasil, 2019.

coletados para essa finalidade legítima pertencem às pessoas físicas às quais os dados se referem e precisam ser tratados e coletados em respeito a essa relação de pertencimento.

Nas palavras de Ana Frazão, Gustavo Tepedino e Milena Donato[121], as entidades de classe tem importante papel a ser assumido, mediante o art. 50 e formularem regras de boas práticas, na medida em que, conhecedoras das especificidades da atividade, podem contribuir para o estabelecimento de critérios adequados à cada hipótese, para além de traduzir os preceitos legais em ações concretas a serem tomadas pelos agentes econômicos. Podendo esses, a seu turno, beneficiarem da segurança decorrente da (adequada) estruturação de normas de governança fixadas pela entidade, capaz de sugerir uniformização dos padrões aplicáveis àquele mercado. A efetiva atribuição de valor a esses parâmetros por terceiros (incluindo-se a ANPD e o Poder Judiciário) é essencial para que se construa a segurança com eles pretendida.

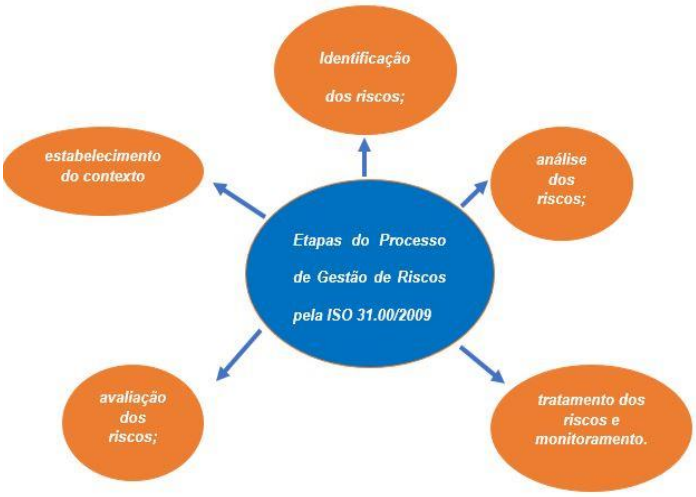
Um processo de gerenciamento de riscos tem a finalidade de construir uma estrutura capaz de mitigar potenciais problemas. Dessa forma as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas, reduzindo surpresas e custos ou prejuízos associados, na qual demandam soluções rápidas para que suas consequências não prejudiquem o bom andamento da empresa. Com o advento da LGPD, o gerenciamento de riscos tornou-se fundamental para demonstrar *compliance* com a lei.

Uma proposta de um processo de gerenciamento de riscos que pode ser aplicado à LGPD é composto por cinco atividades: Identificar os riscos, analisar riscos, efetuar tratamento dos riscos e monitorar e comunicar a evolução dos riscos.

---

[121] FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. [*S.l.*]: Thomson Reuters Brasil, 2019.

Figura 2 - Etapas do Gerenciamento de Riscos



Fonte: Tavares[122]

O gerenciamento de riscos é uma estratégia que age, de forma preventiva, quando se antecipa a uma série de situações negativas. Essa prevenção faz com que os eventos sejam anulados ou minimizados, para que as organizações estejam preparadas para lidar com as possíveis adversidades da melhor forma possível.

De acordo com Ana Frazão, Gustavo Tepidino e Milena Donato[123], é possível apontar três fatores que contribuem para robustecer o papel dos mecanismos de *compliance* no âmbito da proteção de dados pessoais:

> Em primeiro lugar, o amplo escopo de incidência da LGPD (decorrência, como visto, do conceito de dado pessoal, de tratamento e de banco de dados) torna necessária a adaptação não apenas de atividades centralizadas na coleta e/ou tratamento de dados, mas também de qualquer operação que perpasse, ainda que indiretamente, a utilização de informações relacionadas ou relacionáveis a pessoas naturais.

Nesse contexto, observa-se que o *compliance* de dados não se limita apenas ao relacionamento com consumidores, mas acaba por repercutir em várias esferas da atividade empresarial, a demandar adaptação também de setores que, inicialmente, não estariam diretamente relacionados com a LGPD. O compliance de dados assume caráter transversal, a tornar necessário rever os padrões de conduta estabelecidos para cumprimento de outras normas. Remeta-se, mais uma vez, à

---

[122] TAVARES, Daiane Gabriela Lucas. **Quais são as etapas de um processo de gestão de riscos?** Disponível em: https://www.mmpcursos.com.br/blog/quais-etapas-processo-gestao-riscos. Acesso em: 14 jul 2022.

[123] FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. [*S.l.*]: Thomson Reuters Brasil, 2019.

relação de trabalho: as regras de conformidade adotadas nesse setor deverão ser atualizadas para contemplar também os preceitos da LGDP, evitando-se, por exemplo, a coleta de dados desnecessários ou cujo emprego possa ser considerado discriminatório.

> O segundo fator está associado ao primeiro: uma vez que são diversas as entidades que deverão cumprir os preceitos da LGPD, há, dentro de cada comando da lei, níveis de exigência distintos e adaptações necessárias à luz das hipóteses de tratamento de dados envolvidas, até mesmo com vistas a evitar que a proteção termine por inviabilizar a exploração econômica de certas atividades.

Verifica-se, portando que a proteção de dados não tem por objetivo inviabilizar a coleta de dados para conhecimento do público alvo e aprimoramento das atividades empresariais. O empresário tem legítimo interesse de conhecer quem são seus consumidores, empregados e candidatos a emprego. Entretanto, a LGPD esclarece que os dados coletados para essa finalidade legítima pertencem às pessoas físicas às quais os dados se referem e precisam ser tratados e coletados em respeito a essa relação de pertencimento.

Por fim de com os autores Ana Frazão, Gustavo Tepedino e Milena Donato[124]:

> Um terceiro fator consiste na necessidade de conferir concretude a alguns preceitos empregados pela LGPD e, assim, permitir que sejam adotados comportamentos em conformidade com a lei. Como consequência do (necessário) recurso a cláusulas gerais pelo legislador, muitos dos comandos legais comportam significativa margem interpretativa. É o caso, por exemplo, do conceito de "legítimo interesse do controlador" (empregado no artigo 7º, inciso IX como hipótese autorizativa para o tratamento de dados): muito embora o artigo 10 tenha procurado delimitar seu conteúdo e o art. 37, a seu turno, recrudesça o controle sob as operações realizadas com base em tal exceção ao consentimento, verifica-se margem de discricionariedade cuja avaliação, no comum dos casos, será feita a posteriori pelos órgãos competentes. Abre-se, assim, mais um espaço de complementação a ser realizada pelos programas de *compliance.* Em observância dos deveres de transparência exigidos pela LGPD – no que concerne ao legítimo interesse, bastante reforçado – as regras de governança podem dispor sobre as hipóteses específicas em que o tratamento será considerado pela entidade como fundamentado no seu legítimo interesse.

Todos esses elementos fundamentam a extrema relevância de se estabelecerem normas de governança no âmbito do tratamento de dados pessoais

---

[124] FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. [*S.l.*]: Thomson Reuters Brasil, 2019.

que sejam bem estruturadas e atendam aos comandos legais. Apenas a partir da concreta identificação das necessidades específicas de adaptação de cada agente será possível garantir a conformidade com a nova legislação.

Em decorrência dos rígidos padrões estabelecidos na LGPD, os custos para o estabelecimento dos programas de integridade, dependendo da atividade exercida pela empresa e os riscos aos quais está submetido, serão altos. Desta forma, para que de fato as boas práticas e governança sejam adotadas, deverão ter incentivos e estímulos para a sua adoção[125]. Dentre tais estímulos, estão: o bom relacionamento com os titulares de dados, no qual contribui para a construção de um ambiente de confiança, algo fundamental para a boa reputação da empresa; a implementação de um programa de *compliance* serve como mecanismo para afastar ou diminuir a sua responsabilidade (art. 43º)[126] e dar maior segurança em possíveis futuras ações; além de ser critério atenuante no estabelecimento das sanções administrativas pela ANPD.

3.1 Boas práticas para Controle de risco

As boas práticas de governança de dados são ferramentas base que visam gerenciar, utilizar e proteger os dados, elas auxiliar as organizações a cumprir regulamentos de conformidade com a lei. As boas práticas referem-se ao conjunto das melhores técnicas para se realizar uma tarefa, já a governança no contexto de dados e tecnologia da informação é um conjunto de diretrizes, habilidades, competências e responsabilidades assumidas pela alta direção da empresa e pelos agentes de tratamento para guiar as ações organizacionais, de modo a controlar processos, otimizar a aplicação de recursos, dar suporte para a tomada de decisões e garantir a segurança das informações[127]

Os processos internos das boas práticas e de governanças buscam formular regras que estabeleçam as condições de organização, o regime de funcionamento,

---

[125] FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. ***Compliance***: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

[126] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

[127] FLOWTI. **Governança de TI**: saiba tudo sobre este conceito. 2021. Disponível em: https://flowti.com.br/blog/governanca-de-ti-saiba-tudo-sobre-este-conceito > Acesso em: 19 nov. 2022.

os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais, incluindo também padrões técnicos e obrigações específicas para os diversos envolvidos no tratamento.

O relatório deve conter a descrição dos processos de tratamento de dados pessoais e que podem gerar riscos às liberdades civis e aos direitos fundamentais, além de medidas de segurança e formas de mitigar os riscos (artigo 5 º, XVII). No entanto, ainda que o tratamento de dados não seja feito com base no legítimo interesse ou não envolva o uso de dados sensíveis, o controlador pode utilizar a elaboração de relatórios de impacto à proteção de dados como uma ferramenta de apoio para avaliar o risco da realização de determinados tratamentos.

Tanto os registros como o relatório são importantes para avaliar e gerir os riscos envolvidos do tratamento, e também para demostrar a efetividade das medidas técnicas adotadas em busca da conformidade com a LGPD. Trata-se de uma abordagem que busca primeiramente prevenir os danos, em vez de remediá-los. As organizações devem estar preparadas para mitigar os danos, evitando os prejuízos que podem derivar desses incidentes.

No que diz respeito ao risco de *compliance,* este é o risco de sanções legais ou regulamentares, perdas financeiras ou mesmo perdas reputacionais decorrentes da falta de cumprimento de disposições legais, regulamentares, códigos de conduta. Sobre essa expressão, risco de *compliance*, Vanessa Alessi Manzi[128], discorre:

> A expressão risco de *compliance*, por sua vez, é definida como o risco legal, das sanções regulatórias, de perda financeira ou perda de reputação, que uma organização pode sofrer como resultado de falhas no cumprimento de leis, regulamentações, código de condutas e das boas práticas.

Dessa forma, o trabalho de gestão de risco integrado consiste na identificação de todos os fatores que podem provocar danos à imagem, reputação e atuação da empresa em seu segmento e na sociedade como um todo. Ou seja, consiste em identificar e calcular os riscos envolvidos no negócio.

---

[128] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi. **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas: 2010, p. 2.

Corroborando neste mesmo contexto Éderson Garin Porto[129], nos diz que o objetivo do *compliance* é assegurar que a corporação esteja aderente às normas vigentes, fazendo com que os riscos sejam afastados ou mitigados. Acredita-se que a empresa estando comprometida com a cultura do *compliance* estará menos exposta aos riscos e terá um ambiente corporativo impróprio para o surgimento de condutas irregulares ou ilícitas.

As sociedades que empregam programas de *compliance* buscam estabelecer melhor segurança na condução dos negócios, na proteção dos interesses dos clientes e na preservação da reputação institucional. Tais atitudes procuram reduzir ou eliminar o risco de possíveis impactos causados pelas inconformidades nos processos[130]. De acordo com Porto[131]:

> O escopo de atuação do *compliance* envolve tanto uma estratégia preventiva, no sentido de evitar o surgimento de risco e ilícitos, assim como engloba uma atuação repressiva ou reativa, assegurando que a organização tenha ferramentas para identificar as irregularidades e tomar as medidas cabíveis para sua preservação. Esta atuação preventiva e repressiva busca evitar ocorrências de riscos legais (aqueles que estão regulados pela legislação), assim como os riscos reputacionais (aqueles que embora não regulados podem igualmente representar em danos a corporação.

Assim, face à evolução tecnológica, a importância do *compliance* dos sistemas de informação nunca parou de crescer e, com o advento da internet e a sistematização de processos administrativos e contábeis, indivíduos e corporações esperam que estes sistemas sejam capazes de prever seu risco e apresentar estratégias para a sua redução[132], o impulso de informações organizacionais seguras deu início à necessidade de desenvolver melhores métricas para compreender o estado e o comportamento da segurança informacional na organização[133].

A partir do momento em que foram encontrados os riscos, deve-se seguir: a elaboração de um Código de Condutas (na LGPD nomeado como Boas Práticas e

---

[129] PORTO, Éderson Garin. **Compliance e governança corporativa**: uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020.

[130] CANDELORO, Ana Paula P.; RIZZO, Maria Balbina Martins de; PINHO, Vinícius. **Compliance 360º**: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

[131] PORTO, Éderson Garin. **Compliance e governança corporativa**: uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020.

[132] JOUINI, Moura; RABAI, Latifa Bem Arf. Comparative study of information security risk assessment models for cloud computing systems. **Procedia Computer Science**, n.83, p. 1084–1089, 2016.

[133] CASTRO, Alexandra Ramírez; BAYONA, Zulima Ortiz. Gestão de riesgos tecnológicos baseada na ISO 31000 e ISO 27005 e suporta a continuidade dos negócios. **Ingeniería**, v. 16, n. 2, p. 56-66, 2011.

Governança); a ativa participação da alta administração no estabelecimento e adoção dessas práticas; a avaliação contínua de riscos e monitoramento para verificar se de fato a política adotada pela empresa está sendo efetiva; além de haver uma constante reavaliação dos processos de tratamento e uso dos dados que estão mantidos na organização. Os princípios das Boas Práticas e Governança estão previstos no art. 50º, o qual estabelece os preceitos mínimos a serem seguidos pelos agentes de tratamento de dados na instituição de um programa de *compliance*.

> Art. 50º Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais[134].

Em análise, percebe-se a importância deste artigo na Lei, conferindo aos agentes de tratamento, principalmente ao controlador, responsável para implementar o programa de governança em privacidade, e demonstrar o devido comprometimento da empresa com a adequação as normas de proteção de dados. Assim como foi mencionado, é de vital importância que o programa de *compliance* atenda às necessidades próprias da organização, sendo papel do controlador estabelecer um Código de Conduta que se adeque as especificidades da organização e do tipo de dados que são coletados e utilizados. Além de ser sua obrigação estabelecer políticas de segurança e acompanhamento desses dados, possibilitando o diálogo entre empresa e titular, garantindo assim uma maior transparência ao processo de tratamento de dados.

Ainda conforme afirma Giovanini[135], *compliance* refere-se ao cumprimento rígido das regras e das leis, quer sejam dentro ou fora das empresas. No mundo corporativo, *compliance* está ligado a estar em conformidade com as leis e regulamentos internos e externos à organização e, cada vez mais, o *compliance* vai além do simples atendimento à legislação, busca consenso com os princípios da

---

[134] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

[135] GIOVANINI, Wagner. **Compliance**: a excelência na prática. São Paulo, 2014.

empresa, alcançando a ética, a moral, a honestidade e a transparência, em todas as atitudes das pessoas.

Cabe mencionar que, de acordo com Porto[136], a avaliação de risco, também chamada de Mapeamento de Risco de *Compliance*, é extremamente importante dentro do programa de integridade, pois sem sua atuação não seria possível detectar os riscos em a que a empresa está exposta, e assim todo programa de integridade estaria comprometido.

Trazendo para a realidade da LGPD, para que o dado possa ser coletado, ele além de ter uma finalidade especifica, também deverá ter um período certo de uso, passado o momento de sua utilidade, a empresa deverá desfazer-se deste dado, respeitando as regras de segurança previstas na legislação. Diante desta nova realidade, muda-se uma pratica que era antes padrão nas organizações de apropriação infinita dos dados coletados, colocando em riscos direitos fundamentais dos cidadãos.

3.2 Gestão de riscos

A origem da palavra risco é extraída de uma característica fundamental que é válida para a compreensão do fenômeno sendo a incerteza diante da novidade desconhecida e imprevisível. Etimologicamente, a palavra "risco" deriva do italiano *risicare,* que é um termo proveniente das palavras latinas: *risicu* ou *riscu*, que significam "ousar" (*to dare*, em inglês)[137].

De acordo Daniel dos Santos Ferro[138], outras definições mais específicas de risco foram surgindo ao longo do tempo e algumas das principais definições na tabela abaixo:

---

[136] PORTO, Éderson Garin. **Compliance e governança corporativa**: uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020.

[137] MAGALHÃES JUNIOR, Danilo Brum de. Gerenciamento de risco, compliance e geração de valor: os compliance programs como ferramenta para mitigação de riscos reputacionais nas empresas. **Revista dos Tribunais**, São Paulo, v. 107, n. 997, p. 575-594, nov. 2018.

[138] FERRO, Daniel dos Santos. **Gestão de riscos corporativos**: um estudo multicaso sobre seus métodos e técnicas. 2015. Dissertação (Mestrado em Administração) - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2015. doi:10.11606/D.12.2016.tde-19012016-150607. Acesso em: 5 jul. 2022.

Tabela 1 - Definições de Risco

Autores	Definição de Risco
Jorion (1997)	Risco é a probabilidade de acontecer resultados inesperados
Renn (1988)	Risks refer to the possibility that heman actios or events lead to consequences that affects of what humans volue
Darlington et al (2001)	Risco é a ameaça de que um evento ou uma ação afete adversamente a habilidade da organização em maximizar o valor para os stakeholders e atingir seus objetivos e estratégias.
Gitman (2002)	Risco é a probabilidade de que os resultados realizados possam ser diferentes daqueles esperados.
Federation of European Risk Management Association (2003)	Risco pode ser definido como a combinação da probabilidade de um acontecimento e de suas consequências.
COSO (2004)	Risk in the possibility that na event will accur and adversely affect the achievement of objectives
Trapp (2004)	Um evento, esperado ou não, que pode causar um impacto no capital ou em ganhos de uma instituição.
Domadoran (2004)	Nas finanças, nossa definição de risco é diferente e mais ampla. O risco, como o vemos, é a probabilidade de recebermos como retorno sobre um investimento algo inesperado.
Assaf Neto (2008)	Risco pode ser entendido pela capacidade de se mensurar o estado de incerteza de uma decisão mediante o conhecimento das probabilidades associadas à ocorrência de determinados resultados ou valores.
Pindyck e Rubinfeld (2010)	Incerteza é caracterizada pelo termo *risco* nos casos em que cada um dos possíveis resultados e sua correspondente probabilidade são conhecidos.
Aven e Renn, (2011)	O risco é a incerteza sobre as consequências (ou resultados) de uma atividade em relação a algo que as pessoas atribuem valor.
Spikin, (2013)	Risco é a distribuição de possíveis desvios nos resultados e objetivos esperados devido a eventos de incerteza

Fonte: FERRO, 2015[139] e Aven e Renn (2009)[140]; adaptado pela autora.

[139] FERRO, Daniel dos Santos. **Gestão de riscos corporativos**: um estudo multicaso sobre seus métodos e técnicas. 2015. Dissertação (Mestrado em Administração) - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2015. doi:10.11606/D.12.2016.tde-19012016-150607. Acesso em: 5 jul. 2022.

Os conceitos da tabela 1 são de grande importância, destacando-se o risco que pode ser definido como a combinação da probabilidade de um acontecimento e de suas consequências nos resultados e objetivos esperados devido a eventos de incerteza, retrata bem ao riscos em proteção de dados, que eventualmente podem ocorrer em uma instituição de ensino superior (IES), sendo esse conjunto fundamental para o desenvolvimento do presente trabalho. Nesse sentido, Aven e Renn[141] nos ensinam que todos os conceitos de riscos possuem um elemento em comum: a distinção entre realidade e possibilidade. Em outros termos, o que os autores nos mostram é que a partir do reconhecimento de que o futuro não é predeterminado ou independente das ações humanas, pode-se antecipar possíveis resultados adversos decorrentes dessas ações ou do contexto ambiental no qual elas estão inseridas. Consequentemente, a partir desse entendimento pode-se refletir melhor sobre os riscos.

Como descrito por Bessi[142] as definições de risco são importantes pois servem de ponto de partida para os tratamentos tanto regulatório como econômico do risco. Tendo isto em vista, e levando em consideração os diferentes conceitos apresentados, adota-se a concepção de risco e incerteza de Knight[143] e o conceito de risco de COSO[144], que compreende risco como a possibilidade de que um evento ocorra e que ele afete negativamente a consecução de um objetivo.

Para Daniel Silva, o termo risco vem de *risicu* ou *riscu*, em latim, e significa ousar. O mais comum, no entanto, é compreender o conceito de risco como possibilidade de fracasso ou perda decorrente de uma incerteza. O risco é inerente a qualquer atividade na vida pessoal, profissional ou corporativa, e pode envolver perdas, mas também relacionado a oportunidades[145].

---

[140] AVEN, Terje; RENN, Ortwin. Sobre o risco definido como um evento em que o resultado é incerto. Revista de Pesquisa de Risco, v. 12, n. 1, p. 1-11, 2009.

[141] AVEN, Terje; RENN, Ortwin. Sobre o risco definido como um evento em que o resultado é incerto. Revista de Pesquisa de Risco, v. 12, n. 1, p. 1-11, 2009.

[142] BESSIS, Joel. **Risk management in banking**. John Wiley & Sons, 2011

[143] KNIGHT, Frank H**. Risk, uncertainty and profit**. Courier Dover Publications, 2012.

[144] COSO. Committee of Sponsoring Organizations of the Tradeway Commission. Internal Control – **Integrated Framework**, 1992.

[145] SILVA, Daniel C.; COVAC, José R. **Compliance como boa prática de gestão no ensino superior privado**. 2015. 9788502624382. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502624382/. Acesso em: 20 jun. 2022.

Outra definição vem do Blackwell Encyclopedic Dictionary of Finance. De acordo com Paxson e Wood[146]:

> Risco pode simplesmente ser definido como exposição à mudança. É a probabilidade de que algum evento futuro ou conjunto de eventos ocorra. Portanto, a análise do risco envolve a identificação de mudanças potenciais adversas e do impacto esperado como resultado na organização.

Segundo Barrese e Scordis[147], outra especificação de risco é a variação de resultados reais em torno de um resultado médio esperado. Tal assertiva remonta ao conceito de que risco não implica necessariamente em algo indesejável, já que resultados em torno do esperado podem representar tanto benefício quanto malefício para a organização, dependendo de o resultado estar abaixo ou acima do médio esperado. Seguindo esse raciocínio, os autores apontam que organizações de negócio lidam tanto com riscos puros quanto especulativos; risco puro está associado a perigos que só apresentam consequências negativas, enquanto riscos especulativos podem ter consequências positivas ou negativas.

Na visão de Steinberg[148], houve um contraste com a citação anterior, sendo:

> Uma miríade de eventos de origem interna ou externa tem o potencial de afetar a implementação da estratégia e o atendimento dos objetivos. Eventos potencialmente têm impacto negativo, positivo ou uma combinação de ambos. Eventos com impacto potencial negativo representam riscos. Portanto, risco é a possibilidade de ocorrência de um evento que afete negativamente o atendimento dos objetivos. Eventos com impacto potencial positivo podem compensar impactos negativos ou podem representar oportunidades.

Fica evidente que alguns autores optam por uma definição de risco como algo com impacto necessariamente negativo, deixando como ‘oportunidade’ qualquer ocorrência incerta que possa ter impacto positivo.

A NBR ISO 31000[149], define risco como todo efeito de incerteza nos objetivos da organização, sendo esse efeito um desvio em relação ao planejado, seja ele

---

146 PAXSON, Dean; WOOD, Douglas. **The blackwell encyclopedic dictionary of finance**. Oxford: Blackwell, 1998.

147 BARRESE, James; SCORDIS, Nicos. Corporate risk management. **Review of Business**, p.26-29, Fall 2003. Disponível em: https://abepro.org.br/biblioteca/ENEGEP2005_Enegep0305_0688.pdf Acesso em: 14 jul. 2022.

148 STEINBERG, Richard M. *et al.* **Enterprise risk management framework (DRAFT)**. Comittee of Spon- soring Organizations of the Tradeway Commission (COSO), 2003.

149 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de riscos – princípios e diretrizes. Rio de Janeiro, 2009.

positivo, seja negativo. A incerteza é o estado, mesmo que parcial, da deformação das informações relacionadas ao evento.

O IBGC[150] classifica os riscos quanto à sua natureza em: estratégicos, operacionais e financeiros. Nessa categorização, os riscos estratégicos são aqueles que se relacionam com a tomada de decisão da alta administração, podendo acarretar em grandes perdas econômicas. Os riscos operacionais decorrem da ocorrência de falhas e deficiências nos procedimentos, comportamento dos funcionários, sistemas e eventos externos de origens diversas. E os riscos financeiros têm sua origem no gerenciamento do fluxo de caixa, onde as operações financeiras podem resultar de processos internos inadequados.

Nas palavras de Manzi[151], risco pode ser compreendido como qualquer ameaça de que um evento ou ação (interna ou externa) dificulte ou impeça a empresa de atingir os objetivos do negócio. Costuma-se entender risco como a possibilidade de que algo pode não dar certo, mas seu conceito atual envolve graus e tipos tanto de perdas como de ganhos, em termos dos acontecimentos planejados pelo indivíduo ou pela organização.

A gestão de riscos consiste em um conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos. Para elevar a chance de alcançar objetivos, as organizações adotam desde abordagens informais até abordagens altamente estruturadas e sistematizadas de gestão de riscos, dependendo de seu porte e da complexidade de suas operações[152].

Reafirmando o Instituto Brasileiro de Governança Corporativa (IBGC)[153] lembra que a palavra risco é oriunda de risicu ou riscu, em latim, que tem como significado ousar. Nesse sentido, o instituto sugere que risco não necessariamente significa perdas:

---

[150] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBCG). **Guia de orientação para o gerenciamento de riscos corporativos**. São Paulo, 2007. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4656825/mod_resource/content/1/3.pdf. Acesso em: 05 jul. 2022.

[151] MANZI, Vanessa Alessi. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Saint Paul, 2008, p. 93.

[152] REFERENCIAL básico de gestão de riscos. Brasília: TCU, 2018.

[153] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Guia de orientação para gerenciamento de riscos corporativos**. São Paulo, 2017. Disponível em: <http://www.ibgc.org.br/index.php/publicacoescadernos-de- governanca>. Acesso em: 20 jun. 2022.

> [...] pode envolver perdas, bem como oportunidades. Em Finanças, a relação risco- retorno indica que quanto maior o nível de risco aceito, maior o retorno esperado dos investimentos.

O risco é inerente ao processo de desenvolvimento de países, empresas e pessoas. Para exemplificar esse conceito a instituição diz que uma empresa, ao expandir seus negócios, precisa se submeter a empréstimos e, por isso, às mudanças de políticas de créditos e de demanda. Da mesma forma, famílias que migram do interior para cidades em buscas de oportunidades de educação, emprego e saúde também ficam mais vulneráveis a criminalidade e desigualdade social. Essas exposições ao risco nos quais pessoas e empresas se submetem são as buscas por novos ganhos[154].

A questão relacionada à gestão de riscos vem apresentando crescente importância no contexto empresarial, visto que com o aumento da interdependência dos mercados, as empresas tornam-se mais vulneráveis aos diversos fatores de risco. Aspectos econômicos, financeiros e até mesmo movimentações competitivas propagam-se rapidamente, podendo afetar consideravelmente os resultados das empresas[155].

Toda organização, não importando se é de grande, médio ou pequeno porte, sofre a influência de fatores internos e externos que criam a incerteza, responsável por determinar sua capacidade de atingir seus objetivos. O efeito dessa incerteza como já vimos anteriormente é o risco, e ele é um fator inerente a todas as atividades. Foi elaborada a norma ISO 31000:2009[156] para auxiliar a indústria e comércio, públicas e privadas, estabelecendo princípios, estrutura e um processo para gerenciar qualquer tipo de risco, de forma transparente, sistemática e credível em qualquer âmbito ou contexto.

---

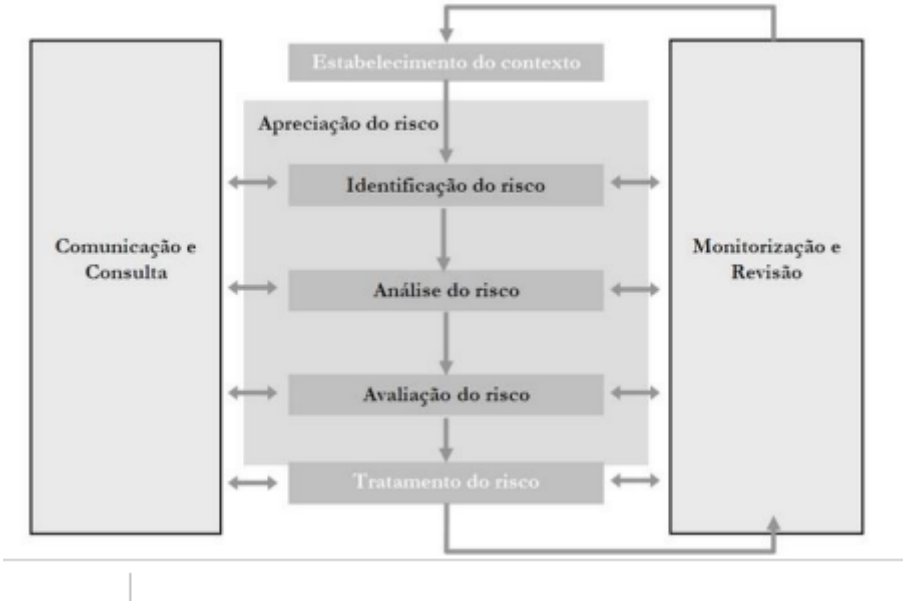
[154] BANCO MUNDIAL. **Risco e oportunidade**: gestão de risco para o desenvolvimento. Washington, 2013. Disponível em http://documents.worldbank.org/curated/pt/120341468157793859/Relat%C3%B3rio-Sobre-o-Desenvolvimento-Mundial-2014-risco-e-oportunidade-gerenciamento-de- riscos-para-o-desenvolvimento-vis%C3%A3o-geral. Acesso em: 20 jun. 2022.

[155] PADOVEZE, Clóvis L.; BERTOLUCCI, Ricardo G. **Gerenciamento do risco corporativo em controladoria**: enterprise risk management (ERM). 2. ed. 2013. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522482962/. Acesso em: 14 jul. 2022.

[156] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de riscos. Disponível em: http://www.iso31000qsp.org/2010/09/visualize-nova-nbriso-31000-de-gestao.html. Acesso em: 19 nov. 2022.

O outro elemento fundamental da norma ISO 31000[157] é o próprio processo de Gestão do Risco, constituído pelas atividades que conduzem à redução e ao controle do risco. Este processo decorre das definições já apresentadas. Convém que o processo de gestão de riscos seja parte integrante da estrutura, incorporado na cultura e nas práticas e adaptado aos processos de negócios da organização. Como toda organização almeja atingir suas metas, a gestão de riscos busca identificar e tratar essas incertezas, tendo como objetivo agregar valor máximo sustentável para todas as atividades e processos da organização. Para a norma ISO 31000, cada setor específico traz consigo necessidades particulares. Portanto, uma característica chave dessa norma é a inclusão do estabelecimento do contexto da organização como uma atividade no início do processo de gestão de risco, capturando objetivos da organização, o ambiente em que ela está inserida, as partes interessadas e a diversidade de critérios de risco. O processo estabelecido pela ISO 31000 para gestão de risco é dividido nas seguintes etapas: Identificação do risco, Análise do risco, Avaliação do risco e Tratamento do risco (Figura 3).

Figura 3 - Processo de gerenciamento ISO 31000:2009



Fonte: ABNT NBR ISSO 31000[158]

[157] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de riscos. Disponível em: http://www.iso31000qsp.org/2010/09/visualize-nova-nbriso-31000-de-gestao.html. Acesso em: 19 nov. 2022.

[158] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de riscos. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso 19 nov. 2022.

A implantação e o aprimoramento da gestão de riscos em uma organização constituem um processo de aprendizagem, que começa com o desenvolvimento de consciência sobre a importância de gerenciar riscos e avança com a implementação de práticas e estruturas necessárias[159].

Damodaran[160], diz que, minimizar a exposição ao risco, também conhecido como perigo, reduz, igualmente, a exposição às oportunidades. Dessa forma, como uma definição, pode-se dizer que:

> O risco é, portanto, inerente a qualquer atividade, pode ser de qualquer natureza e ter dimensões e efeitos que podem ser negativos e positivos. O risco sempre estará presente, podendo haver baixo ou alto nível de perigo, dependendo das medidas preventivas e de segurança existentes[161].

Diante do exposto, percebe o quanto o risco é inerente às atividades corporativas e como pode influenciar o futuro e continuidade de qualquer empresa. Isso justifica a importância de trata-los, sob a ótica de gestão empresarial. O IBGC[162] lembra que riscos envolvem a sua quantificação e qualificação, diretamente relacionadas a determinadas circunstâncias. E para fazer o que propõe esse instituto, o gerenciamento de riscos se torna fundamental. Por isso, os próximos parágrafos irão abordar esse tema, algumas definições a respeito e como ele é essencial à sustentabilidade das organizações.

Vale lembrar que perdas e oportunidades estão diretamente relacionadas aos resultados esperados pela empresa. Um componente crítico das atividades de uma organização é a identificação de riscos, afinal quando se fala em riscos, sempre leva em consideração a subjetividade, pois eles podem ou não correr[163]. Essa situação demonstra que é um desafio às organizações transformarem situações que, muitas vezes, estão fora de seu controle, ou então, não são percebidas, em um processo contínuo que poderá incorporar novas perspectivas nas empresas e ajudá-las a manter a sustentabilidade do negócio.

---

159 REFERENCIAL básico de gestão de riscos. Brasília: TCU, 2018.

160 DAMODARAN, Aswath. **Gestão estratégica do risco**. Porto Alegre: Bookman, 2008.

161 ASSI, Marcos. **Gestão de riscos com controles internos**: ferramentas, certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul, 2012.

162 INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBGC). **Guia de orientação para gerenciamento de riscos corporativos**. São Paulo, 2017. Disponível em: <http://www.ibgc.org.br/index.php/publicacoescadernos-de- governanca>. Acesso em: 20 jun 2022.

163 ASSI, Marcos. **Gestão de riscos com controles internos**: ferramentas, certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul, 2012.

As avaliações de risco é um componente central. O Art. 50º da LGPD estabelece que as organizações devem levar em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos.

Para Bezerra[164], a gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho, referente à segurança e saúde das pessoas, à conformidade legal e regulatória, à aceitação pública, à proteção do meio ambiente, à qualidade do produto, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação.

A segurança informacional, outrora favorável às organizações, é sensivelmente prejudicada por incidentes como fraudes e roubo de dados, os quais, ano após ano atingem índices alarmantes, favorecidos principalmente pelo alcance da internet, com isto, posicionando-se como o quarto maior risco organizacional do mundo em termos de probabilidade e registrando aumentos exponenciais nas violações de dados e seu intrínseco impacto financeiro.

De acordo com Hilary Tuttle[165], vários regulamentos entraram em vigor ou sofreram atualização recente, incluindo o Regulamento Geral de Proteção de Dados da União Europeia (GDPR - UE), Lei de Privacidade da Austrália (Notificable Data Breaches), Lei de Segurança Cibernética da China, em vigor desde 2017 e a Lei Geral da Proteção de Dados (LGPD – Brasil) buscando a regulação do risco informacional, particularmente no que tange à segurança de dados e privacidade.

O gerenciamento de riscos pode oferecer às organizações a oportunidade de identificar esses riscos e, por consequência, assimilá-los. Neste sentido, Lam[166] indica que as organizações que realizaram práticas de gerenciamento de riscos estão entre as empresas que mais geraram rentabilidade e tiveram melhores performances em avaliação de mercado.

---

[164] BEZERRA, Edson Kowask. **ABNT NBR 27005**: Tecnologia da informação – Técnicasde segurança - Gestão de riscos de segurança da informação. Rio de Janeiro: RNP/ESP, 2013.

[165] TUTTLE, Hilary. Global regulation landscape: data protection in 2018. **Risk Management**, v. 65, n. 11, p. 28-34, 2018.

[166] LAM, James. **Risk management**: the ERM guide from AFP. Las Vegas: Association for Financial Professionals, 2011. Disponível em: http://www.jameslam.com/images/PDF/AFP%20Enterprise%20Risk%20Management%20Guide_Lam%202012.pdf>. Acesso em: 20 jun 2020.

Segundo Damodaran[167], a organização precisa tomar decisões corretas frente a um ambiente de incerteza e de diferentes tipos de riscos. E neste contexto, uma decisão pode gerar benefícios ou prejuízos às organizações.

O principal desafio é fazer com que a estratégia global e a perspectiva de risco sejam comunicadas e entendidas por todos em todos os níveis da organização, refletindo no processo de tomada de decisões, uma vez que todos devem entender e identificar os riscos inerentes as atividades, e somente com essa conscientização pode gerenciá-los melhor[168].

Portanto, para Marcos Assis[169], tem como principal característica a probabilidade de ocorrer ou não, dada determinada alternativa escolhida pelo gestor. Por essa ótica, o risco pode ser interpretado como uma ameaça ao alcance dos objetivos organizacionais. As categorias de riscos a que uma atividade está exposta dependem da natureza dessa atividade e de como tratamos a sua possibilidade.

Dependendo do escopo e dos objetivos da gestão de riscos, diferentes métodos podem ser aplicados. O método também pode ser diferente para cada interação do processo[170]. Convém selecionar um método de gestão de riscos apropriado podendo ser selecionado ou desenvolvido e considere critérios básicos, como: critérios de avaliação de riscos, critérios de impacto e critérios de aceitação do risco[171]:

> Executar o processo de avaliação de riscos e estabelecer um plano de tratamento dos riscos; definir e implementar políticas e procedimentos, incluindo implementação dos controles; monitorar controles, e monitorar o processo de gestão de riscos de segurança da informação.

Para tanto deve ser elaborada uma métrica de quais os riscos mais eminentes apresentados pela empresa, e assim selecionados os métodos mais adequados às suas peculiaridades.

---

[167] DAMODARAN, Aswath. **Gestão estratégica do risco**: uma referência para a tomada de riscos empresariais. Porto Alegre: Bookman, 2009.

[168] ASSI, Marcos. **Gestão de riscos com controles internos**: ferramentas, certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul, 2012.

[169] ASSI, Marcos. **Gestão de riscos com controles internos**: ferramentas, certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul, 2012.

[170] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27005**: tecnologia da informação — técnicas de segurança — gestão de riscos de segurança da informação. 3. ed. 2019.

[171] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27005**: tecnologia da informação — técnicas de segurança — gestão de riscos de segurança da informação. 3. ed. 2019.

O processo de gestão de riscos envolve a identificação, a análise e a avaliação de riscos, a seleção e a implementação de respostas aos riscos avaliados, o monitoramento de riscos e controles, e a comunicação sobre riscos com partes interessadas, internas e externas[172]. Esse processo é aplicado a uma ampla gama das atividades da organização, em todos os níveis, incluindo estratégias, decisões, operações, processos, funções, projetos, produtos, serviços e ativos, e é suportado pela cultura e pela estrutura de gestão de riscos da entidade.

Segundo Barrese e Scordis[173] outra especificação de risco é a variação de resultados reais em torno de um resultado médio esperado. Tal assertiva remonta ao conceito de que risco não implica necessariamente em algo indesejável, já que resultados em torno do esperado podem representar tanto benefício quanto malefício para a organização, dependendo de o resultado estar abaixo ou acima do médio esperado. Seguindo esse raciocínio, os autores apontam que organizações de negócios lidam tanto com riscos puros quanto especulativos; risco puro está associado a perigos que só apresentam consequências negativas, enquanto riscos especulativos podem ter consequências positivas ou negativas.

3.3 Responsabilidade civil dos operadores no tratamento de dados pessoais

O legislador na elaboração da LGPD empregou uma técnica legislativa imprecisa, ao definir qual seria o regime de responsabilização geral definido na Seção III, que trata da responsabilidade e ressarcimento de danos. Ocorre que isto deveria ter sido discriminado de forma clara, pois evitaria uma série de controvérsias que, inevitavelmente, vão surgir em consequência dessa falta de clareza[174]. Ao invés disso, limitou-se o legislador a estabelecer, no art. 42, a hipótese de responsabilização dos agentes de tratamento nos casos de violações à legislação. Já no art. 44, indicou que há responsabilização nos casos de ofensa às normas técnicas relacionadas ao dever de segurança na proteção de dados[175].

---

[172] REFERENCIAL básico de gestão de riscos. Brasília: TCU, 2018.

[173] BARRESE, James; SCORDIS, Nicos. Corporate risk management. **Review of Business**, p.26-29, Fall 2003. Disponível em: https://abepro.org.br/biblioteca/ENEGEP2005_Enegep0305_0688.pdf Acesso em: 14 jul. 2022.

[174] GUEDES, Gisela Sampaio da Cruz**. Regime de responsabilidade adotado pela lei de proteção de dados brasileira**. São Paulo: Revista dos Tribunais, 2019. Caderno Especial LGPD, p. 167-182.

[175] CAPANEMA, Walter Aranha. A responsabilidade civil na lei geral de proteção de dados. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 163-170, jan./mar. 2020. Disponível em:

Ratifica-se esse posicionamento de incerteza em relação ao regime escolhido pelo legislador com a interpretação dada por Anderson Schreiber[176], indicando que, se:

> A LGPD não foi extremamente feliz no desenho das normas atinentes à responsabilidade civil. Há falhas e omissões que podem e precisam ser sanadas pelo intérprete, em busca de um regime de responsabilidade civil que se afigure, a um só tempo, coerente e eficaz. As diferentes soluções interpretativas devem ser construídas a partir de elementos constantes não apenas da LGPD em si, mas também de outras normas que compõem o tecido normativo brasileiro, em especial as normas constitucionais. [...]
>
> [...] Por um lado, o art. 42 não alude, em sua literalidade, à culpa, o que poderia indicar a adoção de um regime de responsabilidade objetiva. Por outro lado, o art. 42 não emprega a expressão independentemente de culpa", como fizeram o Código Civil (arts. 927, parágrafo único, e 931) e o Código de Defesa do Consumidor (arts. 12, caput, e 14, caput), podendo-se extrair da omissão uma preferência pela responsabilidade subjetiva.

Referente ao regime adequado de responsabilização civil dos agentes de tratamentos de dados, observa-se que na doutrina uma dicotomia tradicional da seara jurídica. Há expoentes como Rafael Zanatta[177] em 2017 e Laura Schertel Mendes[178], já em 2018, que defendem o regime de responsabilização objetiva, visto considerarem que na ação de tratamento de dados revela-se um risco intrínseco, pois há um potencial danoso significativo nos casos de infracção, dado que tais direitos estão relacionados à personalidade e à liberdade.

Do outro lado da doutrina, tem-se a linha de pensamento, que pela interpretação da LGPD, o regime de responsabilidade pertinente seria o de responsabilização subjetiva, tendo como expoente a doutrinadora Gisela Sampaio da Cruz Guedes[179], em 2019. Dentre os argumentos apresentados pelos autores, destaca-se o que alude sobre a legislação estabelecer padrões de procedimentos a serem respeitados pelos agentes de tratamento de dados, com a finalidade de

---

https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em: 19 nov. 2022.

[176] SCHREIBER, Anderson. **Responsabilidade civil na lei geral de proteção de dados pessoais**: tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2020.

[177] ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica? *In:* ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro.

[178] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor,** v. 27, n. 120, p. 469-483, nov.-dez. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116/991. Acesso em: 19 nov. 2022.

[179] GUEDES, Gisela Sampaio da Cruz**. Regime de responsabilidade adotado pela lei de proteção de dados brasileira**. São Paulo: Revista dos Tribunais, 2019. Caderno Especial LGPD, p. 167-182.

fornecer maior segurança, discrição e boas práticas em administração de dados, sendo este um dos fatores elencados como justificativa para a constatação da responsabilidade subjetiva.

Segundo Guedes[180], a LGPD estabelece duas hipóteses para a configuração da responsabilidade civil dos agentes de tratamento de dados: a “violação à legislação de proteção de dados pessoais” e a “violação da segurança dos dados”. Ambos são calibrados pela noção de tratamento irregular, previsto no artigo 44, o qual procura sistematizar critérios para aferição da culpa dos agentes de tratamento de dados a esse respeito. Ressalta-se desde logo, contudo, que não parece haver razão para tal bifurcação, uma vez que as consequências são as mesmas (obrigação de indenizar) e, em especial, que essas duas hipóteses de reponsabilidade civil são reunidas no artigo 44 sob a noção ampla de “tratamento irregular”:

> **Art. 44**. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:
> I - O modo pelo qual é realizado;
> II - O resultado e os riscos que razoavelmente dele se esperam;
> III - as técnicas de tratamento de
> dados pessoais disponíveis à época em que foi realizado.
> **Parágrafo único**. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano[181].

Um ponto muito importante a ser observado é a forma como tratada a questão da responsabilidade civil pela LGPD, a ser considerado no gerenciamento em matéria de proteção de dados.

De forma geral a responsabilidade civil, é entendida como uma visão obrigacional de reparar um dano antijuridicamente causado a um terceiro, podendo ser compreendida em duas modalidades. A primeira delas é a decorrente de danos resultantes do inadimplemento, má execução ou atraso no cumprimento de obrigações contratuais, denominada de responsabilidade contratual. A segunda, também chamada de responsabilidade civil extracontratual, diz respeito à obrigação

---

[180] GUEDES, Gisela Sampaio da Cruz**. Regime de responsabilidade adotado pela lei de proteção de dados brasileira**. São Paulo: Revista dos Tribunais, 2019. Caderno Especial LGPD, p. 167-182.

[181] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

de reparação de danos resultantes da violação de outros direitos alheios, como os direitos da personalidade.

A responsabilidade civil extracontratual é, portanto, diretamente ligada à violação de um direito. Assim, aquele que viola um direito e ocasiona dano a outrem será responsável pela reparação do dano causado. No Código Civil, a responsabilidade civil é fundada em dois conceitos, o de ato ilícito (art. 186) e o de abuso de direito (art. 187) da seguinte forma:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes[182]

O ato ilícito, portanto, é aquele praticado em desacordo com a ordem jurídica, que ocasiona a violação de direitos e causa prejuízos a outrem. O ato ilícito pode ser penal, administrativo ou civil bem como pode acarretar dupla ou tripla responsabilidade, por exemplo, um crime ambiental que ofende os particulares (ilícito civil), a sociedade (ilícito penal) e é passível de sanções administrativas. A consequência do ato ilícito civil é a obrigação geral de reparar o dano, disposta no caput do art. 927 do Código Civil de 2002. Além disso, existem situações em que se responde por terceiros, devendo existir uma conexão entre o responsável e o executor do ato. Há também a hipótese de dano causado por coisa da qual se é proprietário. Por outro lado, nos moldes do art. 187 do CC, a noção de ato ilícito foi ampliada, para considerar como ilícito aquele ato que, originalmente é lícito, mas foi exercido fora dos limites impostos pelo seu fim econômico ou social, pela boa-fé objetiva ou pelos bons costumes.

Desse modo, para que exista a responsabilidade civil é necessária a conjugação de três pressupostos, quais sejam a conduta, o nexo de causalidade e o dano. A conduta pode ser ação ou inação; comissiva ou omissiva; própria ou de terceiros; lícita ou ilícita; derivada de fato, coisa, produto ou animal. O nexo de causalidade liga a conduta do agente ao dano sofrido pela vítima. Para que surja o

---

[182] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. **Diário Oficial da União**, Brasília, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm/. Acesso em: 31 out 2022.

dever se indenizar é preciso que o dano verificado seja consequência da ação ou omissão do agente. O dano é a lesão a um bem jurídico.

Conforme entendimento do doutrinador Carlos Roberto Gonçalves[183]: A responsabilidade civil tem, pois, como um de seus pressupostos, a violação do dever jurídico e o dano. Há um dever jurídico originário, cuja violação gera um dever jurídico sucessivo ou secundário, que é o de indenizar o prejuízo. Cabe destacar que os pressupostos traduzem em condições previamente necessárias para que se possa iniciar determinado ato jurídico, nos casos em que se verifica a responsabilização civil de determinada pessoa, faz-se necessário observar três requisitos, sendo eles a conduta ilícita imputada ao agente, o nexo de causalidade desta e por último analisar a extensão do dano sofrido.

Em análise voltada aos pressupostos da responsabilidade civil com prisma voltado para LGPD, verifica-se: i) conduta que ensejaria reparação; ii) nexo de causalidade da conduta do agente com o ilícito; iii) e o que se entende como dano. Pela simples leitura da LGPD, evidencia-se a existência de duas antijuridicidades que dão ensejo à responsabilização dos agentes de tratamentos, são elas: i) O agente de tratamento, que no exercício da atividade, violar a legislação de proteção de dados[184], causando dano patrimonial ou extrapatrimonial a terceiros (Art. 42, LGPD). Assim, incorre em conduta ilícita, com consequente violação da legislação o operador que no tratamento de dados não observa as bases legais impostas pela LGPD; ii) Pelo não fornecimento de um nível adequado de segurança de dados esperado pelo titular (Art. 44 c/c 46, LGPD)[185]. Relacionado a esta antijuridicidade, cabe destaque para o que se entenderá como nível adequado, visto a complexidade da atividade de segurança da informação, devendo ser consideradas apenas aquelas medidas previstas em padrões devidamente reconhecidos, como as denominadas normas da Organização Internacional de Normalização (ISO)[186].

---

[183] GONÇALVES, Carlos R. **Responsabilidade civil**. 21. ed. São Paulo: Saraiva, 2022.

[184] CAPANEMA, Walter Aranha. A responsabilidade civil na lei geral de proteção de dados. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 163-170, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em: 19 nov. 2022.

[185] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

[186] ISO é o acrônimo de *International Organization for Standardization*, uma entidade internacional que estabelece normas e padrões. O padrão ISO 27001, por exemplo, é destinado a segurança da Informação. Disponível em: https://www.iso.org/home.html. Acesso em: 15 set. 2022

O que se destaca de importante nesse ponto é perceber que o legislador criou duas condutas antijurídicas passíveis de responsabilização: a primeira específica, fundamentada na violação direta da legislação de proteção de dados pessoais, e uma segunda relativa aos deveres gerais de segurança dos agentes de tratamento no exercício da atividade.

De acordo com Vieira[187], quando se fala em responsabilidade civil, entende-se haver uma relevante exigência para consertar um dano causado à terceiro, de forma antijurídica.

Tal instituto pode abarcar duas espécies:

a) a responsabilidade contratual: que é aquela decorrente de prejuízos resultantes de inadimplência, do atraso em cumprir cláusulas contratuais, podendo derivar, inclusive da imperícia na execução de uma obra[188];

b) a responsabilidade civil extracontratual, concernente ao dever de reparar os danos que são resultantes da quebra de direitos alheios, dos direitos da personalidade, por exemplo, ou seja, é aquela que está estritamente relacionada à quebra de um direito. Então, o sujeito que o viola e causa dano a um terceiro, terá a obrigação de reparar o dano causado[189].

A LGPD, a seu turno, define a responsabilidade dos agentes de tratamento de dados, que são os controladores e os operadores, pelos danos causados em razão do exercício da atividade de tratamento, de forma semelhante à sistemática do Código de Defesa do Consumidor (CDC), na seção III do Capítulo VI. A Lei, conforme art. 43, exime de responsabilidade os agentes quando provarem que: não realizaram o tratamento de dados em questão; que não houve violação à legislação; ou que houve culpa exclusiva do titular dos dados ou de terceiro pela ocorrência dos danos.

---

[187] VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados**: uma análise da tutela dos dados pessoais em casos de transferência internacional. 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/handle/123456789/26233. Acesso em: 31 out. 2022.

[188] VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados**: uma análise da tutela dos dados pessoais em casos de transferência internacional. 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/handle/123456789/26233. Acesso em: 31 out. 2022.

[189] VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados**: uma análise da tutela dos dados pessoais em casos de transferência internacional. 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/handle/123456789/26233. Acesso em: 31 out. 2022.

Conforme art. 42 da LGPD, o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, será obrigado a repará-lo. A LGPD traz, ainda, previsão expressa de responsabilidade solidária dos operadores e controladores. Nesse sentido, conforme disposição do inciso I do §1º do art. 42, o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da LGPD ou quando não tiver seguido as instruções lícitas do controlador. Já os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, conforme inciso II do §1º do art. 42 da LGPD, respondem solidariamente. O direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso, é assegurado àquele que reparar o dano ao titular dos dados consoante §4º do art. 42 da LGPD.

Nos termos do art. 44 da LGPD, será considerado irregular o tratamento de dados pessoais quando for inobservada a legislação ou quando não for fornecida ao titular a segurança que ele poderia esperar, levando-se em conta as seguintes circunstâncias: o modo pelo qual o tratamento é realizado; o resultado e os riscos que razoavelmente dele se esperam; as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

A gestão de risco é obrigatória ao controlador e ao operador. Nesse processo é importante ter visibilidade sobre todas as atividades da organização que envolvam tratamento de dados pessoais, o que pode ser feito por meio do registro das operações de tratamento de dados pessoais (artigo 37, LGPD). A lei brasileira, tal qual o regulamento europeu que a inspirou, exige, em algumas situações, que o controlador elabore o relatório de impacto de proteção de dados, como no caso de tratamento de dados tendo como hipótese legal o legítimo interesse (artigo 10, § 3º) ou envolvendo o uso de dados sensíveis (artigo 38).

4 PROTOCOLO PARA GERENCIAMENTO DE RISCO ADEQUADO À PROTEÇÃO DE DADOS PESSOAIS EM INSTITUIÇÃO DE ENSINO SUPERIOR

Para iniciarem o processo de adequação, as IES devem estar prontas para que cada tratamento de dado esteja de acordo com a LGPD, estendendo-se além do tempo de um aluno na sua instituição, por exemplo. Nesses casos, bancos de dados e arquivos exigem políticas documentadas para proteção, retenção e arquivamento.

As instituições de ensino terão que se adequar na forma jurídica, metodológica e tecnologicamente para sustentar os direitos dos titulares dos dados. Sobre o conceito de titular, a LGPD define que é a pessoa natural a quem se referem os dados pessoais, que são objeto de tratamento, segundo determina o Inciso V, do Artigo 5º[190]. As normas de proteção de dados pessoais, especialmente a LGPD, servem como guarda-chuva normativo, fundamentando-se no livre desenvolvimento da personalidade e dignidade da pessoa humana.

Para tratar os dados pessoais de uma IES, deverão os responsáveis agir de forma ética e com boa-fé, observando os seguintes princípios, que estão expressos no artigo 6º da LGPD[191], sendo:

> **Finalidade:** Não será mais possível tratar dados pessoais com finalidades genéricas ou indeterminadas. O tratamento de cada informação pessoal deve ser feito com fins específicos, legítimos, explícitos e informados.
> **Adequação**: Os dados pessoais tratados devem ser compatíveis com a finalidade informada pela empresa.
> **Necessidade**: As startups e empresas em geral devem utilizar apenas os dados estritamente necessários para alcançar as suas finalidades.
> **Livre acesso**: A pessoa física titular dos dados tem o direito de consultar, de forma simples e gratuita, todos os dados que a empresa detenha a seu respeito.
> **Qualidade dos dados**: Deve ser garantido aos titulares que as informações que a empresa tenha sobre eles sejam verdadeiras e atualizadas. É necessário ter atenção à exatidão, clareza e relevância dos dados, de acordo com a necessidade e com a finalidade de seu tratamento.
> **Transparência**: Todas as informações passadas pela empresa, em todos os seus meios de comunicação, devem ser claras, precisas e verdadeiras. Além disso, a empresa não pode compartilhar dados pessoais com outras pessoas de forma oculta.
> **Segurança:** É responsabilidade das empresas buscar procedimentos, meios e tecnologias que garantam a proteção dos dados pessoais de

[190] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

[191] BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

> acessos por terceiros, ainda que não sejam autorizados, como nos casos de invasões por *hackers*.
> **Prevenção**: O princípio da prevenção objetiva que as empresas adotem medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais. Ou seja, as empresas devem agir antes dos problemas e não somente depois.
> **Não Discriminação**: Os dados pessoais jamais podem ser usados para discriminar ou promover abusos contra os seus titulares. A própria LGPD já criou regras específicas para o tratamento de dados que frequentemente são utilizados para discriminação, os chamados dados pessoais sensíveis como os que tratam sobre origem racial ou étnica, convicção religiosa.
> **Responsabilização e Prestação de Contas**: Além de se preocuparem em cumprir integralmente a Lei, as empresas devem ter provas e evidências de todas as medidas adotadas, para demonstrarem a sua boa-fé e a sua diligência[192].

O princípio da finalidade carrega de forma mais incisiva os traços característicos da proteção de dados, pois o motivo da coleta deve ser compatível com o objetivo final do tratamento dos dados[193]. Como o dado pessoal é expressão direta da personalidade do indivíduo nunca perde seu elo com este.

De acordo com Dhiulia Santos[194] (2019), o consentimento do titular dos dados da mesma forma deve ser compreendido de tal forma que sigam os princípios regidos no artigo 6º da LGPD. O uso de princípios na análise de dados tem por finalidade demarcar o manuseio destes dados. Em vista disso, o desenvolvimento dos princípios contidos no artigo 6°, subdivididos de I a X da LGPD não anula o vigor dos princípios da jurisdição brasileira.

Um processo de gerenciamento de riscos tem a finalidade de construir uma estrutura capaz de mitigar potenciais problemas (Figura 4). Dessa forma as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas, reduzindo surpresas e custos ou prejuízos associados, na qual demandam soluções rápidas para que suas consequências não prejudiquem o bom andamento da empresa. A tendência é que a área de gestão de riscos caminhe para fatores de interesse de seus *stakeholders*, com forte atenção à imagem e à reputação das organizações. Por essa razão a amplitude cresceu e acabou

---

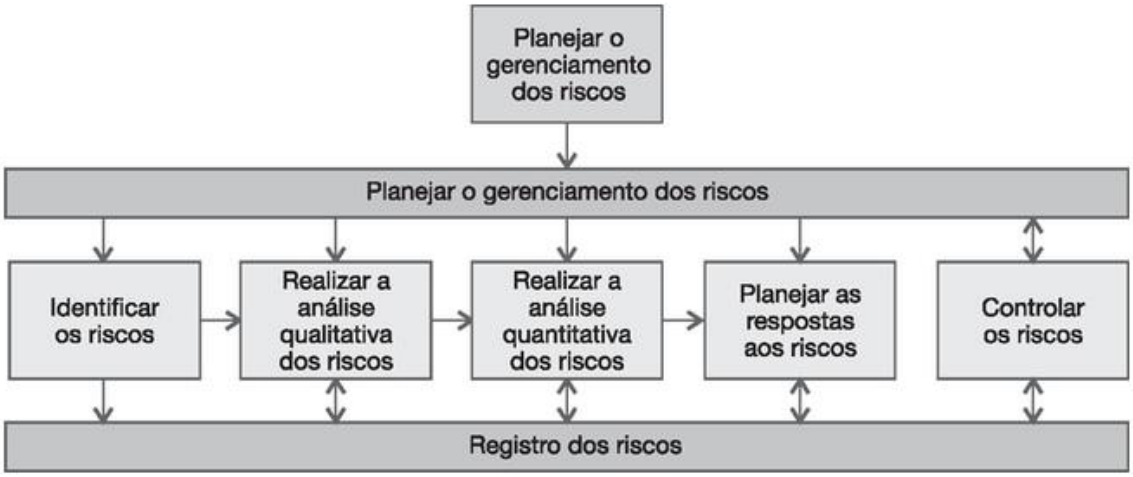
192 DONEDA, Danilo. **Princípios de Proteção de Dados Pessoais**. *In*: LUCCA, Newton de Simão Filho; Adalberto; Lima, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: Marco civil de internet. Quartier Latin, 2015.

193 DONEDA, Danilo. **Princípios de Proteção de Dados Pessoais**. *In*: LUCCA, Newton de Simão Filho; Adalberto; Lima, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: Marco civil de internet. Quartier Latin, 2015.

194 SANTOS, Dhiulia de Oliveira. A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais: lei n. 13.709/2018. 2019. 50 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Centro Universitário de Brasília - Uniceub, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13802. Acesso em: 31 out. 2022.

abrangendo a organização como um todo, envolvendo as médias gerências como responsáveis na gestão de riscos corporativos. Com o advento da LGPD, o gerenciamento de riscos tornou-se fundamental para demonstrar *compliance* com a lei.

Figura 4 - Fases do gerenciamento de risco



Fonte: A partir de estudo desenvolvido em PM[195]I, 2013.

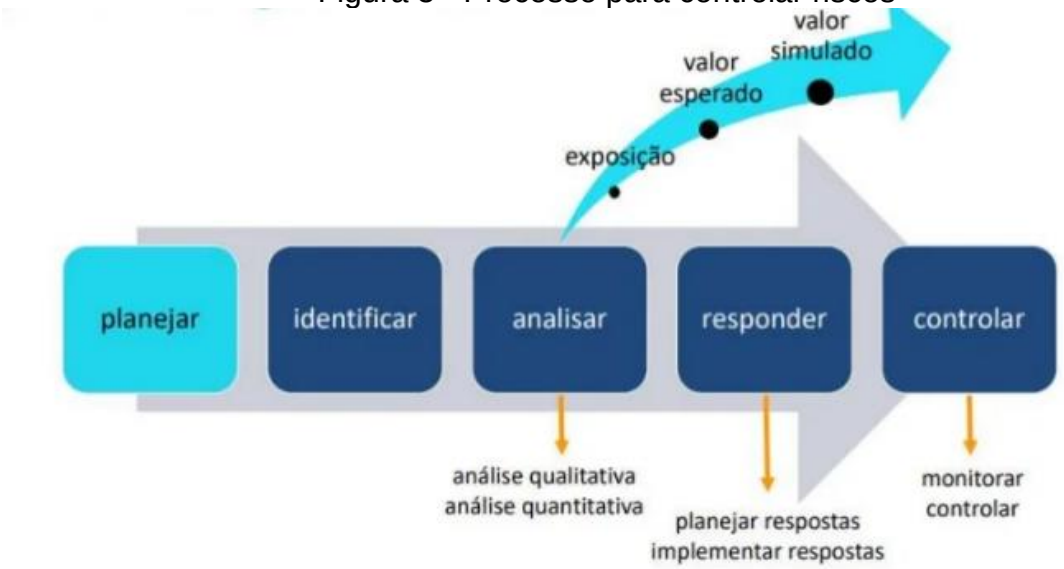
- Planejar o gerenciamento dos riscos – define como conduzir os demais processos de gerenciamento dos riscos de um projeto.
- Identificar os riscos – identifica os riscos que podem afetar o projeto.
- Realizar a análise qualitativa dos riscos – analisa os riscos identificados de forma a priorizar e subsidiar o seu tratamento.
- Realizar a análise quantitativa dos riscos – estima numericamente a probabilidade e o impacto dos riscos antes analisados qualitativamente, bem como o risco geral do projeto.
- Planejar as respostas aos riscos – define e desenvolve ações de respostas aos riscos analisados e priorizados, visando a reduzir a exposição do projeto a riscos negativos (ameaças) e aumentar a exposição a riscos positivos (oportunidades).
- Controlar os riscos – garante a execução das ações de respostas e a reavaliação dos riscos do projeto, bem como a avaliação da eficácia do gerenciamento dos riscos em si, durante todo o projeto.

A identificação e o tratamento dos riscos ocorrem mais intensamente no início do projeto e em cada de uma de suas fases, mas esses processos devem ser

[195] PROJECT MANAGEMENT INSTITUTE. **A guide to the project management of body of knowledge:** Guia PMBOK®. 5. ed. Pensilvânia: Project Management Institute, 2013.

repetidos periodicamente ou em determinadas situações definidas pelo processo de planejar o gerenciamento dos riscos. O processo de controlar os riscos garante que os demais processos sejam repetidos quando necessários. O processo de gerenciamento de risco é composto por cinco atividades: Identificar os riscos, analisar riscos, avaliar riscos, efetuar tratamento dos riscos (responder) e monitorar (controlar) e comunicar a evolução dos riscos.

Figura 5 - Processo para controlar riscos



Fonte: Pimentel[196]

De acordo com Antonio Celso[197], é importante que exista a conscientização e o comprometimento com o gerenciamento de riscos por parte da alta administração da empresa. Nesse contexto, os tomadores de decisão são os responsáveis por esse gerenciamento, ou seja, mediante a matriz de riscos deve-se identificar qual a resposta a ser adotada para tratamento do risco. A seguir, as estratégias que podem ser adotadas para o tratamento dos riscos:

• Evitar o Risco: Decisão de não se envolver ou agir de forma a se retirar de uma situação de risco. Necessário preencher o formulário padrão de Risco Assumido.

• Aceitar o Risco: Nesse caso, apresentam-se três alternativas: reter, reduzir ou transferir/compartilhar o risco.

---

[196] PIMENTEL, Isabela. **Gestão de risco** reputacional. 2019. Disponível em: https://comunicacaointegrada.com.br/gestao-de-riscos-reputacionais. Acesso em: 05 ago. 2022.

[197] BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos**: gestão integrada em riscos corporativos São Paulo: Sicurezza, 2016.

• Reter: Manter o risco no nível atual de impacto e probabilidade. Necessário preencher o formulário padrão de Risco Assumido.
• Reduzir: Ações são tomadas para minimizar a probabilidade e/ou o impacto do risco.
• Transferir e/ou Compartilhar: Atividades que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco por meio da transferência ou, em alguns casos, do compartilhamento de uma parte do risco.

Para Antonio Celso[198] o risco é assumido quando um tomador de decisão decide assumir risco, tendo em vista a relação custo–benefício ou por questões estratégicas. Esse tipo de decisão vai contra as boas práticas de mercado. Sempre que um tomador de decisão resolver assumir riscos deve fazê-lo de maneira documentada para manter assim um registro, possibilitando que esse registro seja acionado caso o risco assumido venha a se concretizar.

4.1 Protocolo para conformidade na proteção de dados no ensino superior

1- Especificamente para instituições de ensino e pesquisa, o primeiro passo para se adequar à LGPD é fazer um levantamento para identificar onde estão depositados os dados pessoais e sensíveis de todos os envolvidos: alunos, pais, pesquisadores e colaboradores;
2- Depois, é hora de verificar se há vulnerabilidade de segurança. Ou seja, se eles podem ser facilmente acessados, violados e vazados. Vale dedicar especial atenção aos procedimentos internos de coleta e tratamento de dados pessoais, especialmente os mais sensíveis, conforme disposição legal. Assim, as áreas de potencial criticidade dentro da operação da instituição são identificadas.
3- Com as informações em mãos, é preciso fazer uma análise de cenário, riscos e ações necessárias para adequação. Nessa etapa, a instituição avalia como está a aplicação de controles como governança de proteção de dados, gestão de dados pessoais, segurança da informação, gestão de riscos, gestão de dados pessoais em terceiros e gestão de incidentes. Além disso, confere se há transmissão interna, externa e compartilhamento de dados, a quantidade de empresas com que são feitas essas trocas, se há e com quantos países é feita essa transferência

[198] BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos**: gestão integrada em riscos corporativos São Paulo: Sicurezza, 2016.

internacional, o volume dos dados, entre outros. Tudo para mensurar a gestão de risco e incidentes e garantir uma melhor governança dos dados;

4- Essa análise de vulnerabilidades será essencial para criar um plano de ação, com iniciativas que deverão reduzir os riscos mapeados e aprimorar a gestão dos dados pessoais. Bons exemplos dessas ações podem ser treinamentos de equipes sobre Segurança da Informação, procedimentos de legitimação da coleta e gestão do consentimento para tratamento de dados pessoais, gestão de identidades na rede, melhores práticas e ferramentas para controle de acesso.

5- Também baseado na LGPD, é importante que as instituições criem normas de proteção de dados pessoais para seguirem como política interna. São princípios e delimitações para guiar o fluxo das informações, desde a definição do que é dado pessoal e sensível, quais dados serão coletados, como serão processados e qual para finalidade, as funções dos encarregados responsáveis, até as medidas de segurança e processos para mitigação de riscos.

6- Após definir essas diretrizes, o banco de dados com informações pessoais que a empresa possuir deverá ser revisado, mesmo que esteja formado por materiais coletados antes da vigência da lei. Para que possam ser usadas, essas informações deverão ser legitimadas e se enquadrarem em uma das hipóteses previstas na LGPD;

São elas: Hipótese de Tratamento de Dados Pessoais (art. 7º), que ressalta a garantia da anonimização dos dados pessoais, sempre que possível, desde o fornecimento de consentimento pelo titular até a realização dos estudos pelo órgão de pesquisa, ou hipótese de Tratamento de Dados sensíveis (art. 11), quando o titular, responsável legal consentir, de forma específica e destacada, para finalidades específicas, tratamento compartilhado de dados necessário à execução, pela administração pública, de políticas públicas previstas em lei ou regulamentos até a realização de estudos por órgão de pesquisa, o anonimato dos dados pessoais sensíveis deve ser garantido, sempre que possível.

7- Com a lei, empresas e organizações não podem mais guardar dados pessoais indefinidamente, somente enquanto eles forem imprescindíveis para cumprir os objetivos legítimos do tratamento. Dessa forma, é preciso estabelecer prazos para o armazenamento de cada categoria de dados pessoais, difundir o vencimento desse uso entre os colaboradores e fiscalizar seu efetivo cumprimento.

8- Consoante o princípio da segurança, devem ser utilizadas medidas técnicas e organizacionais efetivas para a proteção dos dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, como a adoção de criptografia para armazenamento e transmissão de dados pessoais e a assinatura de Acordos de Confidencialidade específicos para o processamento de dados pessoais, por parte de todos os colaboradores e terceiros envolvidos na coleta, uso, armazenamento, transferência e eliminação desses dados pessoais.

4.2 Estrutura para implantação da LGPD em uma IES

Com base nessa estrutura, pretende-se alcançar o objetivo geral dos trabalhos da comissão: Adequar sistemas, processos e procedimentos institucionais de uma IES a fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade de seus usuários.

As ações para implementação da LGPD em IES em quatro eixos temáticos: (Quadros 1, 2 e 3):

- Estruturante;
- Treinamento e Conscientização;
- Diagnóstico;
- Segurança da Informação.

Apresenta-se a seguir descrição de eixos e seus objetivos específicos.

Quadro 1 - Implantação da LGPD - objetivos 1 à 4

EIXOS DE TRABALHO	EIXOS DE TRABALHO	AÇÕES	RESPONSÁVEIS
ESTRUTURANTE	OBJETIVO 1 CONSTITUIR E ESTRUTURAR COMISSÃO DE IMPLEMENTAÇÃO DA LGPD/ IES	1.1 Constituir comissão interna de implementação	Gestão Superior
		1.2 Designar o encarregado	Gestão Superior
		1.3 Alinhar as premissas de trabalho	Comissão de Implementação
		1.4 Elaborar plano de implementação/conformidade uma IES à LGPD	Comissão de Implementação
		1.5 Definir cronograma de trabalho da comissão de implementação.	Comissão de Implementação
		1.6 Definir divisão de tarefas/ações por grupo de membros	Comissão de Implementação
		1.7 Estabelecer um interlocutor com cada unidade administrativa/ acadêmica e publicizar a lista na página LGPD	Presidente da Comissão
COMUNICAÇÃO E TREINAMENTO	OBJETIVO 2 IMPLEMETAR FERRAMENTA DE COMUNICAÇAO SOBRE A LGPD	2.1 Criar página LGPD no portal da IES	Diretoria de Comunicação Social
		2.2 Incluir regularmente na página LGPD/IES o andamento dos trabalhos da comissão de implementação a fim de dar ampla publicidade à comunidade acadêmica	Controlador IES
			Controlador IES

		2.3 Criar identidade visual para as peças gráficas	
		2.4 Elaborar peças gráficas com orientações sobre a LGPD	Controlador IES
		2.5 Disponibilizar as peças gráficas na página LGPD/IES e em formato impresso (estabelecer periodicidade de divulgação)	Controlador IES
		2.6 Realizar campanha de sensibilização sobre a temática e conscientização dos principais aspectos da lei para toda a comunidade acadêmica	Controlador IES
		2.7 Realizar campanha de sensibilização sobre a temática e conscientização dos principais aspectos da lei para público específico (identificado por meio dos resultados coletados no formulário de pesquisa do Diagnóstico da Cultura Organizacional)	Controlador IES
DIAGNÓSTICO	**OBJETIVO 3 AVALIAR A REALIDADE ATUAL SOBRE O TRATAMENTO DE DADOS PESSOAIS NA IES**	3.1 Aplicar questionário aos servidores das unidades administrativas e acadêmicas com questões sobre o processo de tratamento de dados para efetivação dos serviços públicos ofertados pela IES	Comissão de Implementação
		3.2 Realizar diagnóstico sobre o estágio de maturidade na página da Secretaria do Governo Digital, disponível em: https://pesquisa.sisp.gov.br/index.php/798411?lang=pt-BR	Representante Unidades Acadêmicas + Controlador IES

		3.3 Analisar os dados obtidos a fim de orientar o planejamento das ações continuadas de adequação à LGPD, principalmente, subsidiar a modelagem do Inventário de Dados Pessoais	Representante Unidades Acadêmicas + Controlador IES
		3.4 Elaborar um Inventário de Dados Pessoais – IDP-PILOTO: conforme orientações do Guia Inventário de Dados Pessoais – IDP de https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf	Repesentante Unidades Acadêmicas Controlador IES
COMUNICAÇÃO E TREINAMENTO	**OBJETIVO 4 QUALIFICAR COMISSÃO INTERNA DE IMPLEMENTAÇÃO DA LGPD E ORIENTAR A CAPACITAÇÃO DOS SERVIDORES DA IES**	4.1 Definir os cursos de participação obrigatória dos membros da Comissão e indicar, periodicamente, materiais para estudo e atualização.	Presidente da Comissão
		4.2 Indicar aos servidores da IES cursos básicos relativos ao tema (disponibilizar as indicações na página LGPD)	Presidente da Comissão
		4.3 Publicizar na página LGPD/IES os guias orientadores da ANPD e da Secretaria de Governo Digital que possam orientar os servidores sobre o tema	Controlador IES
		4.4 Elaborar e publicizar breves arquivos orientadores sobre a LGPD no e-mail institucional e/ou em outros meios de comunicação analisados como viáveis para atingir o objetivo	Controlador IES

		4.5 Elaborar Guia Prático com orientações sobre a LGPD na IES (perguntas e respostas, links úteis, agentes de tratamento, entre outros)	Controlador IES
		4.6 Esclarecer possíveis dúvidas relativas à implementação da LGPD apresentadas por unidades e/ou Servidores (ação realizada sob demanda)	Presidente da Comissão

Fonte: Elaborado pela autora, com base em estudo junto à UFVJM[199].

Conforme quadro, encontram-se as medidas de nível estratégico que envolvem principalmente a gestão superior, visando demonstrar o comprometimento da instituição, especialmente do Controlador, em adotar políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais (art.50, LGPD). Compilar informações necessárias que possam retratar a realidade (Diagnóstico da Cultura Organizacional).

Quadro 2 - Implantação LGPD - Objetivos 5 e 6

EIXOS DE TRABALHO	OBJETIVOS ESTRATÉGICOS	AÇÕES	RESPONSÁVEIS
SEGURANÇA DA INFORMAÇÃO	**OBJETIVO 5 ELABORAR DOCUMENTOS DE PRIVACIDADE**	5.1 Elaborar política de privacidade e proteção de dados pessoais	Controlador IES
		5.2 Elaborar template/guia para Aviso de privacidade e Termo de Uso e template para Termo de Consentimento para tratamento de dados	Controlador IES

[199] O presente quadro foi construído a partir da comparação com a UFVJM. O quadro foi parametrizado segundo os estudos realizados, sendo agregado e complementado com os resultados alcançados. Universidade Federal dos Vales do Jequitinhonha e Mucuri - UFVJM - Campus do Mucuri. Disponível em https://portal.ufvjm.edu.br/page/lgpd/PlanodeConformidadedaLGPDA409ago2022FINAL.pdf acesso em 20 nov. 2022.

		5.3 Elaborar relatório (s) de impacto de proteção de dados (RIPD)	Controlador IES
		5.4 Elaborar plano (s) de resposta a incidentes	Controlador IES
COMUNICAÇÃO E TREINAMENTO	**OBJETIVO 6 ORIENTAR ADEQUAÇÃO DOS INSTRUMENOS DE COLETAS DE DADOS DA IES DE ACORDO COM A LGPD**	6.1 Orientar os servidores da IES sobre como adequar os instrumentos de coleta de dados, tais como requerimentos e declarações, às diretrizes da LGPD	Controlador IES
		6.2 Orientar os servidores da IES sobre como adequar os instrumentos de coleta de dados, tais como requerimentos e declarações, às diretrizes da LGPD	Controlador IES
		6.3 Orientar os servidores sobre como adequar os instrumentos de coleta de dados, tais como requerimentos e declarações, às diretrizes da LGPD	Controlador IES
		6.4 Orientar os servidores sobre como adequar os instrumentos de coleta de dados, tais como requerimentos e declarações, às diretrizes da LGPD	Controlador IES
		6.5 Orientar os servidores de Unidades Acadêmicas sobre como adequar os instrumentos de coleta de dados, tais como requerimentos e declarações, às diretrizes da LGPD	Controlador IES

		6.6 Orientar os servidores de outras unidades administrati-vas sobre como adequar os instrumentos de coleta de dados, tais como requerimentos e declarações, às diretrizes da LGPD	Controlador IES

Fonte: Elaborado pela autora, com base em estudo junto à UFVJM [200]

Este visa ação na segurança e suas boas práticas destinadas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Orientar os colaboradores que são os agentes de tratamento dos dados sob a tutela da instituição. Concentrou esforços para conscientizá-los e orientá-los sobre a importância de tratar dados de maneira adequada e adotar medidas de segurança a fim de proteger dados pessoais (art. 46, LGPD).

Quadro 3 - Implantação LGPF - Objetivo 7

EIXOS DE TRABALHO	OBJETIVOS ESTRATÉGICOS	AÇÃO	RESPONSÁVEIS
ESTRUTURANTE	**OBJETIVO 7 CONSTITUIR A ESTRUTURA DE MONITORAMENTO DA LGPD**	7.1 Constituir Equipe de Governança ou Comissão Permanente de Proteção de Dados Pessoais da LGPD	Gestão Superior
		7.2 Definir atribuições da equipe	
		7.3 Definir atividades de monitoramento contínuas (gerenciamento de riscos, auditorias)	

Fonte: Elaborado pela autora, com base em estudo junto à UFVJM [201].

[200] O presente quadro foi construído a partir da comparação com a UFVJM. O quadro foi parametrizado segundo os estudos realizados , sendo agregado e complementado com os resultados alcançados. Universidade Federal dos Vales do Jequitinhonha e Mucuri - UFVJM - Campus do Mucuri. Disponível em https://portal.ufvjm.edu.br/page/lgpd/PlanodeConformidadedaLGPDA409ago2022FINAL.pdf acesso em 20 nov. 2022.

[201] O presente quadro foi construído a partir da comparação com a UFVJM. O quadro foi parametrizado segundo os estudos realizados, sendo agregado e complementado com os resultados

A conformação à proteção de dados pessoais evolui com o tempo. Por isso, as IES devem acompanhar mudanças regulatórias, alterações estruturais da instituição, novos projetos que envolvam atividades de tratamento de dados, e aquisição de novas tecnologias, entre outros. O monitoramento deve ser conduzido por uma equipe qualificada para a tarefa constante de identificar lacunas e pontos de melhoria para aperfeiçoar a conformidade à LGPD.

alcançados. Universidade Federal dos Vales do Jequitinhonha e Mucuri - UFVJM - Campus do Mucuri. Disponível em https://portal.ufvjm.edu.br/page/lgpd/PlanodeConformidadedaLGPDA409ago2022FINAL.pdf acesso em 20 nov. 2022.

5 CONSIDERAÇÕES FINAIS

A pesquisa teve como objetivo apresentar no atual cenário a proteção de dados pessoais em uma Instituição de Ensino Superior e a importância de implementação de estrutura de gerenciamento com finalidade principal de evitar riscos de vazamento dos dados pessoais da comunidade acadêmica, bem como antecipar riscos e atender às exigências normativas e, principalmente, afastar danos, não só financeiros como também de credibilidade e confiança de toda a comunidade. Um dos fatores que dificultam a implantação da gestão de risco é a crença de que os riscos, em especial de *compliance*, não irão se materializar. A escolha do tema deste estudo, evidenciou-se pela literatura disponível sobre o assunto e pelos resultados das recentes pesquisas sobre maturidade de risco de *compliance* no Brasil, permitindo compreender os principais aspectos referentes ao gerenciamento de risco voltado para Instituições de Ensino Superior.

O problema da pesquisa é identificado no fato de como se implantará a análise em gestão de risco em uma organização de ensino superior buscando concretizar práticas de responsabilidade proativa pelos agentes de tratamento. No primeiro capítulo tratou-se da proteção de dados, sendo características gerais, evolução histórica, Lei Geral de Proteção de Dados Pessoais de forma geral. No segundo capítulo enfatizou a governança de dados para gestão de riscos em proteção de dados pessoais, com atenção especial para as boas práticas e controle de risco. Por fim, protocolo para gerenciamento de risco adequado à proteção de dados pessoais e uma estrutura para implantação da LGPD em uma IES em instituição de ensino superior.

Os processos de adequações das IES deverão estar prontos para que cada tratamento de dado esteja de acordo com a LGPD, estendendo-se além do tempo de um aluno na sua instituição, por exemplo. Nesses casos, bancos de dados e arquivos exigem políticas documentadas para proteção, retenção e arquivamento. As instituições de ensino terão que se adequar na forma jurídica, metodológica e tecnologicamente para sustentar os direitos dos titulares dos dados. Para tratar os dados pessoais de uma IES, deverão os responsáveis agir de forma ética e com boa-fé.

Para tanto, antes de adentrar na análise do tema central, foi necessária a contextualização sobre as características gerais de proteção de dados pessoais,

evolução histórica da proteção de dados no Brasil e no Mundo, bem como a gestão de riscos. Essa explanação foi relevante no sentido de ter contribuído para o entendimento de como as Instituições de Ensino superior podem adentrar e se resguardar perante à LGPD. Fez tal referência no primeiro capítulo, sendo abordada a parte conceitual, vigência e classificações de dados, a real motivação da criação da Lei Geral de Proteção de Dados tendo como principal objetivo tratar das lacunas existentes e trazer melhorias no tratamento de dados pessoais inserido no ordenamento jurídico pátrio, baseada na Regulamentação europeia (GDPR). A LGPD visa um equilíbrio entre o direito à privacidade e o uso massivo das informações pessoais, sua missão, portanto, não é outra, senão proteger os direitos fundamentais dos brasileiros, tais como a liberdade, a privacidade, o livre desenvolvimento e a personalidade, enquanto a GDPR tem como objetivo proteger os cidadãos de países da UE.

Abordou-se a LGPD, expondo seu contexto histórico, sua tramitação, conceito e como vem sendo utilizada ao longo desses anos e o que isso influenciou nos dias atuais, demonstrando a real importância da criação da sua criação, veio, não para ser mais um ramo do direito, mas sim para interdisciplinar os ramos que já existem e trazer uma solução de forma mais completa e possível lide. Verificou-se que as empresas que atuam no mercado, além de estarem bastante suscetíveis aos riscos de mercado, têm que demonstrar com seu exemplo o quanto é importante esta proteção, oriunda de dados pessoais.

Demonstrou-se também a influência de forma direta do Regulamento Geral sobre a LGPD, ou seja, uma lei nova multidisciplinar inclusive o Direito Internacional. Percebeu-se a necessidade da evolução junto á proteção dos dados pessoais, os quais estão evoluindo e o direito precisa acompanhar essa demanda, mas de maneira mais eficaz e rápida. Fez-se necessário desenvolver uma cultura preventiva.

A proteção de dados não tem uma valoração apenas no Brasil, mas também no mundo é um valor do qual jamais fora abandonado. Pelo contrário, o direito à privacidade vem sendo cada vez mais fortalecido, diante de inúmeras denúncias de utilizações de informações pessoais de forma abusiva, invasiva e indevida, sem mesmo que o titular tivesse qualquer controle sobre elas, havendo, inclusive, a sua utilização para fins políticos, econômicos ou sociais.

De acordo com os fundamentos da LGPD, pode-se destacar a respeito à privacidade, liberdade de expressão, inviolabilidade da intimidade, livre iniciativa, defesa do consumidor, direitos humanos, dignidade e exercício da cidadania. Na prática, a LGPD se aplica aos governos e às empresas, tendo que garantir maior segurança aos dados pessoais, sempre observando os principais princípios estipulados em nossa legislação bem como um conjunto de regras que passou a serem encontrados na norma como a finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, responsabilização e a prestação de contas de tudo que se refere aos dados pessoais, conforme bem explicado durante o presente trabalho.

A tutela jurídica brasileira e o direito comparado, ele traz á tona a Autoridade Nacional de Dados Pessoais (ANPD) fornecendo um regulamente do qual se faz homogêneo na aplicabilidade dos dados pessoais na Europa, sendo aplicada de forma direta e eficaz, tendo como um vínculo aplicado aos Estados-Membros, disposto certo grau de autonomia perante evolução de diligências específicas de adaptações e execuções. As sanções administrativas estão previstas na lei e em vigência desde 01 de agosto de 2021, pela ANPD.

De forma geral, conforme delineado neste trabalho, os pontos mais importantes do panorama geral da LGDP podem ser sintetizados da seguinte forma: a LGPD é uma regra para todos, ou seja, ele tem uma abrangência no cenário de segurança jurídica válido para todo o país; estabelecido de maneira clara, o que são os dados pessoais e como deve ser realizado o seu correto tratamento; regra geral, para o tratamento de dados pessoais, o consentimento do titular deve ser, com exceção dos casos em que seja necessário cumprir os critérios legais. Em caso de descumprimento do regulamento, são aplicadas penalidades severas a lei traz consigo as definições de que são dados pessoais essenciais para uma boa compreensão da legislação. A Lei destaca as responsabilidades de cada agente de processamento e suas funções.

Portanto, é necessário que os agentes de tratamento busquem diversas maneiras de proteger os dados pessoais, mas também informar o titular, levar a informação do que está acontecendo de maneira clara e precisa, gerando uma cultura de proteção de dados. Neste contexto faz-se necessário uma forma de tratar estes dados em Instituição de Ensino Superior, que além de ter o dever de cumprir a norma, tem também a incumbência de dar o exemplo. Por este motivo é

imprescindível que as IES coletem os dados e os processe, esclareçam aos usuários a finalidade de adquirir tais informações, indicando como serão utilizados, podendo as mesmas exercerem a prerrogativa de autorizar ou não o processamento, tendo assim um controle efetivo dos seus dados pessoais. Com o intuito de minimizar e orientar os usuários e as IES, elaborou-se protocolo para melhor uso dos dados pessoais e a forma mais segura de executar de acordo com a norma.

No futuro que não está muito distante, a transparência e zelo com o consumidor serão requisitos essenciais para a contratação de um serviço ou para a compra de um produto.

Evidentemente, não utilizar dados pessoais não é nem remotamente uma opção em uma sociedade cada vez mais dependente das informações deles extraídas. Contudo, é preciso que haja uma honesta autoavaliação das condições em que cada uma dessas instituições vem se beneficiando do uso dos dados. A verdade é que se, por um lado, o uso dos dados possibilita a extração de informações valiosas, por outro lado, cria uma grande responsabilidade que muitas vezes se torna custosas para quem os detém.

Assim, como a implementação da LGPD ocorre a partir de uma abordagem baseada nos riscos, quanto mais dados forem tratados, mais abrangentes precisam ser o controle e o programa de governança dos agentes de tratamento. É preciso aplicar a prática de uma gestão de riscos, com a adoção de um conjunto de ações coordenadas, com o objetivo de controlar os possíveis impactos que um determinado tratamento pode gerar. Aderir a uma gestão de riscos com a sistematização e metodologia apropriadas é um elemento essencial em qualquer organização. Isso fica evidente a partir dos princípios da segurança (artigo 6º, VII), da prevenção (artigo 6º, VIII) e da responsabilização e prestação de contas (artigo 6º, X), bem como a partir da leitura da Seção III do Capítulo VI e do Capítulo VII da lei brasileira, que, respectivamente, dispõem sobre a responsabilidade e ressarcimento dos danos e sobre a segurança dos dados dos titulares.

A questão é que, para ter uma promoção efetiva dos direitos fundamentais tutelados pelas normas de proteção de dados, não basta que riscos sejam compensados. É preciso, em primeiro lugar, preveni-los. Afinal, prevenir e avaliar danos são medidas necessárias em uma sociedade que se preocupa em alocar corretamente os custos dos riscos e danos causados por aqueles que ofertam bens

e serviços. E a prevenção se inicia com a avaliação da necessidade de tratamento dos dados. É essa a direção apontada pelo princípio da necessidade (art. 6º, III), o qual estabelece que os tratamentos de dados deverão limitar-se ao mínimo necessário para a realização de suas finalidades, abrangendo dados pertinentes e proporcionais, sem exceder ao limite da finalidade.

Por fim, criou-se protocolo e estrutura para implantação da LGPD a partir de comparação com universidades que fazem uso da LGPD e seguem à risca a verificação dos possíveis riscos para efetivarem a conformidade de acordo com a proteção de dados no ensino superior. Sendo: Adequação, verificação, informação, análise, definição de diretrizes, organização e segurança. Tendo como foco principal a gestão de risco, e o processo de gerenciamento de riscos que como tem a finalidade de construir uma estrutura capaz de mitigar potenciais problemas. Dessa forma as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas, reduzindo surpresas e custos ou prejuízos associados, na qual demandam soluções rápidas para que suas consequências não prejudiquem o bom andamento da empresa (IES).

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005

ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2008.

ARTIGO 50 da Lei nº 13.709 de 14 de agosto de 2018. Disponível em: https://www.jusbrasil.com.br/topicos/200398676/artigo-50-da-lei-n-13709-de-14-de-agosto-de-2018 Acesso em: 15 jul. 2022.

ASSI, Marcos. **Gestão de riscos com controles internos**: ferramentas, certificações e métodos para garantir a eficiência dos negócios. São Paulo: Saint Paul, 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de riscos – princípios e diretrizes. Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de riscos. Disponível em: http://www.iso31000qsp.org/2010/09/visualize-nova-nbriso-31000-de-gestao.html. Acesso em: 19 nov. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000**: gestão de riscos. Disponível em: https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf. Acesso 19 nov. 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27005**: tecnologia da informação — técnicas de segurança — gestão de riscos de segurança da informação. 3. ed. 2019.

AVEN, Terje; RENN, Ortwin. Sobre o risco definido como um evento em que o resultado é incerto. **Revista de Pesquisa de Risco**, v. 12, n. 1, p. 1-11, 2009.

BANCO MUNDIAL. **Risco e oportunidade**: gestão de risco para o desenvolvimento. Washington, 2013. Disponível em http://documents.worldbank.org/curated/pt/120341468157793859/Relat%C3%B3rio-Sobre-o-Desenvolvimento-Mundial-2014-risco-e-oportunidade-gerenciamento-de-riscos-para-o-desenvolvimento-vis%C3%A3o-geral. Acesso em: 20 jun. 2022.

BARBIERI, C. **Governança de dados**: práticas, conceitos e novos caminhos. [*S.l.*]: Alta Books, 2020.

BARRESE, James; SCORDIS, Nicos. Corporate risk management. **Review of Business**, p.26-29, Fall 2003. Disponível em: https://abepro.org.br/biblioteca/ENEGEP2005_Enegep0305_0688.pdf Acesso em: 14 jul. 2022.

BECKERS, K.; SCHMIDT, H.; KÜSTER, J. C. & FAßBENDER. S. Pattern-Based **Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing.** Sixth International Conference on Availability, Reliability and Security, 2011, p.327-333.

BESSIS, Joel. **Risk management in banking**. John Wiley & Sons, 2011

BEZERRA, Edson Kowask. **ABNT NBR 27005**: Tecnologia da informação – Técnicasde segurança - Gestão de riscos de segurança da informação. Rio de Janeiro: RNP/ESP, 2013.

BIONI, Bruno R. **Proteção de dados pessoais**: a função e os limites do consentimento. 2021. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 14 jun. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 jun. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**: emendas constitucionais de revisão. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 14 set. 2022.

BRASIL. **Lei 10.406, de 10 de janeiro de 2002**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso: 20 jun. 2020.

BRASIL. **Lei n. 13.709 de 14 de ago. de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 15 jun. 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. **Diário Oficial da União**, Brasília, 10 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm/. Acesso em: 31 out 2022.

BRASIL. Ministério da Justiça. **Debate público**: proteção de dados pessoais. Disponível em: http://pensado.mj.gov.br/dadospessoais2011/debata-a-norma/ Acesso em: 23 jun. 2022.

BRASIL. Ministério da Justiça. **Multa Oi por monitorar navegação de consumidores na internet**. Disponível em: https://www.justica.gov.br/news/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em 27 jun. 2022.

BRASIL. Ministério da Justiça. **Proteção de dados pessoais**. Disponível em: https:// http://pensando.mj.gov.br/dadospessoais/. Acesso em 27 jun. 2022.

BRASIL. Ministério da Justiça. Departamento de Defesa e Proteção do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília: SDE/DPDC, 2010. Disponiel em: htttps;/www.justica.gov/seus-direitos/consumidor/Anexo/manual-de-protecao-de-dados-pessoais.pdf. Acesso em: 20 jun. 2022.

BRASIL. Ministério de Ciência e Tecnologia, Inovações e Comunicações. **Estratégia brasileira para a transformação digital**: e-digital. Brasília, 2018. Disponível em: https://www.mctic.gov.br/mctic/export/site. Acesso em 27 jun. 2022.

BRASILIANO, Antonio Celso Ribeiro. **Inteligência em riscos**: gestão integrada em riscos corporativos São Paulo: Sicurezza, 2016.

CAMURÇA, Lia Carolina Vasconcelos. **Sociedade de vigilância, direito à privacidade e proteção de dados pessoais**: uma análise sobre a influência de técnicas de publicidade comportamental na internet no consumidor-usuário. Brasília: Conselho da Justiça Federal, Centro de Estudos Jurídicos, 2021.

CANCELIER, Mikhail Vieira de Lorenzi; CRISTO, Camila Kohn de; MAFRA, Gabriela. Evasão de informações privadas: proteção à privacidade nos casos de pornografia de vingança. *In*: CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE, 4., 2017, Santa Maria. **Anais...** p. 1. Disponível em: https://egov.ufsc.br/portal/conteudo/evas%C3%A3o-de-informa %C3%A7%C3%B5es-privadas-prote%C3%A7%C3%A3o-%C3%A0- privacidade-nos-casos-de-pornografia-de-vingan%C3%A7. Acesso em: 2 jun. 2022.

CANDELORO, Ana Paula P.; RIZZO, Maria Balbina Martins de; PINHO, Vinícius. **Compliance 360º**: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan, 2012.

CAPANEMA, Walter Aranha. A responsabilidade civil na lei geral de proteção de dados. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 163-170, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em: 19 nov. 2022.

CAPEZ, Fernando. **Lei geral de proteção de dados**: as competências da ANPD e o Procon, 2020. Disponível em: https://economia.ig.com.br/colunas/defesa-doconsumidor/2020-06-12/lei-geral-de-protecao-de-dados-as-competencias-da-anpd-eo-procon.html. Acesso em: 07 nov, 2022.

CARDOSO, André Gushow. **O art 50 da LGPD e a competência da ANPD para reconhecer e divulgar regras de boas práticas e governança**. Disponível em: https://www.migalhas.com.br/depeso/351510/o-art-50-da-lgpd-e-a-anpd-para-reconhecer-e-divulgar-regras Acesso em 15 jul 2022.

CASTELLS, Manuel. **A sociedade em rede**. 9. ed. rev. ampl. São Paulo: Paz e Terra, 2008.

CASTRO, Alexandra Ramírez; BAYONA, Zulima Ortiz. Gestão de riesgos tecnológicos baseada na ISO 31000 e ISO 27005 e suporta a continuidade dos negócios. **Ingeniería**, v. 16, n. 2, p. 56-66, 2011.

CAVALCANTE, Pedro Peres. **Privacidade e proteção de dados pessoais**: uma análise comparativa dos quadros regulatórios brasileiro e europeu. 2018. 62 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Pernambuco, Recife, 2018. Disponível em: https://repositorio.ufpe.br/handle/123456789/34357. Acesso em: 24 nov. 2022.

CEARÁ. Tribunal de Justiça. **Dado pessoal, dado pessoal sensível e dado anominizado.** Disponível em: https://www.tjce.jus.br/lgpd/lgpd-dados-pessoais/. Acesso em 13 nov. 2022.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi. **Manual de compliance**: preservando a boa governança e a integridade das organizações. São Paulo: Atlas: 2010.

COLOMBO, Cristiano; BERNI, Duílio Landell de Moura. **Privacy no Direito Italiano: Tríade de Decisões Judiciais Rumo a insights sobre limites conceituais, deslocamento Geográfico e transparência do corpo eletrônico**. In: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura. Tutela jurídica do corpo eletrônico: novos desafios ao direito digital. [S.l.]: Foco, 2022. p. 53-72.

COSO. Committee of Sponsoring Organizations of the Tradeway Commission. Internal Control – **Integrated Framework**, 1992.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

CRAVO, Victor *et al.* **Guia de boas práticas**: lei geral de proteção de dados (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-dedados/GuiaLGPD.pdf. Acesso em: 22 ago. 2022.

DAMODARAN, Aswath. **Gestão estratégica do risco**. Porto Alegre: Bookman, 2008.

DAMODARAN, Aswath. **Gestão estratégica do risco**: uma referência para a tomada de riscos empresariais. Porto Alegre: Bookman, 2009.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. Princípios da proteção de dados pessoais. *In:* DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de (Coord.). **Direito Internet III**. São Paulo: Quartier Latin, 2015. v. 1: Marco Civil da Internet (Lei n.12.965/2014).

DONEDA, Danilo. A proteção de dados pessoais como direito fundamental. **Revista Espaço Jurídico**, Joaçaba, v. 12, n. 103, 2011.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, v. 12, n. 2, p. 91-108, 2011.

DONEDA, Danilo; CUNHA, Mario Viola de Azevedo. Risco e informação pessoal: o princípio da finalidade e a proteção de dados no ordenamento brasileiro. **Revista Brasileira de Risco e Seguro**, v. 5, n. 10, 85-102, 2009. Disponível em: http://hdl.handle.net/1814/13485. Acesso em: 3 out. 2022.

DONEDA, Danilo. **Princípios de Proteção de Dados Pessoais**. *In*: LUCCA, Newton de Simão Filho; Adalberto; Lima, Cíntia Rosa Pereira de (Coord.). *Direito & Internet III*: Marco civil de internet. Quartier Latin, 2015.

DUMBILL, Edd. Getting up to speed whit big data. *In:* BIG data now. 2012.

FEIGELSON. Bruno, SIQUEIRA. Antônio Henrique Albani. **Comentários à lei geral de proteção de dados**: Lei 13.709/2018. São Paulo: Thomson Reuters Brasil, 2019.

FERNANDES, Aguinaldo Aragón; ABREU, Vladimir Ferraz de. **Implantando a governança de TI**: da estratégia à gestão de processos e serviços. [*S.l.*]: Brasport, 2014.

FERRO, Daniel dos Santos. **Gestão de riscos corporativos**: um estudo multicaso sobre seus métodos e técnicas. 2015. Dissertação (Mestrado em Administração) - Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2015. doi:10.11606/D.12.2016.tde-19012016-150607. Acesso em: 5 jul. 2022.

FLOWTI. **Governança de TI**: saiba tudo sobre este conceito. 2021. Disponível em: https://flowti.com.br/blog/governanca-de-ti-saiba-tudo-sobre-este-conceito > Acesso em: 19 nov. 2022.

FONSECA, Marcos De Lucca; MIGLIO Marcelo. **LGPD para Startups**. Disponível em: https://mmiglio.com.br/advocacia-sp/artigo-lgpd-startup.html. Acesso em: 08 set. 2022.

FONTES, Edison. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2008.

FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de compliance. *In:* CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance**: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. [*S.l.*]: Thomson Reuters Brasil, 2019.

GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha.** 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da- protecao-de-dados-na-alemanha-29052019. Acesso em 14 jun. 2022.

GIOVANINI, Wagner. **Compliance**: a excelência na prática. São Paulo, 2014.

GITMAN, Lawrence J. **Princípios de administração financeira**. São Paulo: Pearson Prentice Hall, 2010.

GONÇALVES, Carlos R. **Responsabilidade civil**. 21. ed. São Paulo: Saraiva, 2022.

GUEDES, Gisela Sampaio da Cruz**. Regime de responsabilidade adotado pela lei de proteção de dados brasileira**. São Paulo: Revista dos Tribunais, 2019. Caderno Especial LGPD, p. 167-182.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBCG). **Guia de orientação para o gerenciamento de riscos corporativos**. São Paulo, 2007. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4656825/mod_resource/content/1/3.pdf. Acesso em: 05 jul. 2022.

ISO CENTRAL SECRETARY. **Security techniques — extension to iso/iec 27001 and iso/iec 27002 for privacy information management — requirements and guidelines. Standard ISO/IEC TR 27701:2019**, International Organization for Standardization, Geneva, CH, 2019.

JOUINI, Moura; RABAI, Latifa Bem Arf. Comparative study of information security risk assessment models for cloud computing systems. **Procedia Computer Science**, n.83, p. 1084–1089, 2016.

KANWAL, T., SHAUKAT, S. A. A., ANJUM, A., CHOO, K.-K. R., KHAN, A., AHMAD, N., AHMAD, M., KHAN, S. U., ET AL. **Privacy-preserving model and generalization correlation attacks** for 1: M data with multiple sensitive attributes. Information Sciences 488 (2019), 238–256.

KLEE, Antônia Espindola Longoni, NOGUEIRA NETO, Alexandre Pereira. **Proteção de dados pessoais**: privacidade versus avanço tecnológico. 2019. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em: 08 nov. 2022.

KNIGHT, Frank H. **Risk, uncertainty and profi**t. Courier Dover Publications, 2012.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do Brasil (lei nº 13.709/18)**. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, 2019. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 12 jun. 2022.

LAM, James. **Risk management**: the ERM guide from AFP. Las Vegas: Association for Financial Professionals, 2011. Disponível em: http://www.jameslam.com/images/PDF/AFP%20Enterprise%20Risk%20Management%20Guide_Lam%202012.pdf>. Acesso em: 20 jun 2020.

LGPD: multas e sanções previstas na lei. Disponível em: https://blconsultoriadigital.com.br/lgpd-multas-e-sancoes/. Acesso em: 19 nov. 2022.

LIMA, Cíntia Rosa Pereira D. **Autoridade nacional de proteção de dados e a efetividade da lei geral de proteção de dados**. Coimbra: Almedina, 2020. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 12 set. 2022.

MAGALHÃES JUNIOR, Danilo Brum de. Gerenciamento de risco, compliance e geração de valor: os compliance programs como ferramenta para mitigação de riscos reputacionais nas empresas. **Revista dos Tribunais**, São Paulo, v. 107, n. 997, p. 575-594, nov. 2018.

MALHEIROS, Luíza Fernandes. **O consentimento na proteção de dados pessoais na Internet**: uma análise comparada do Regulamento Geral de Proteção de Dados Europeu e do Projeto de Lei 5.276/2016. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade de Brasília, 2017. Data da publicação: 8 jan. 2018. Disponível em: bdm.unb.br/handle/10483/18883. Acesso em: 13 jun. 2022.

MANZI, Vanessa Alessi. **Compliance no Brasil**: consolidação e perspectivas. São Paulo: Saint Paul, 2008.

MCLENNAN, Marsh. **O relatório de riscos globais.** 16. ed. 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor,** v. 27, n. 120, p. 469-483, nov.-dez. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116/991. Acesso em: 19 nov. 2022.

NUCCI, Guilherme de S. **Estatuto da criança e do adolescente:** comentado. 5. ed. 2020. Disponível em: https://online.minhabiblioteca.com.br. Acesso em: 2021.

OLIVEIRA, Felipe. **Senado decide que LGPD entra em vigor agora, mas prazo depende da sanção.** Disponível em: https://bit.ly/33rXZDE. Acesso em: 14 set. 2020.

OLIVEIRA, Marco Aurélio Belizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

OLIVEIRA, Ricardo. **LGPD**: Como evitar as sanções administrativas. São Paulo: Saraiva, 2021. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 19 nov. 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Digital government review of Brazil. **OCDE Digital Government Studies**, p.1-146, 2018. Disponível em: http//www.ocde.org/governance/digital-government-review-of-brazil-97899264307636-em.html Acesso em: 27 jun. 2022.

PADOVEZE, Clóvis L.; BERTOLUCCI, Ricardo G. **Gerenciamento do risco corporativo em controladoria**: enterprise risk management (ERM). 2. ed. 2013. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788522482962/. Acesso em: 14 jul. 2022.

PAXSON, Dean; WOOD, Douglas. **The blackwell encyclopedic dictionary of finance**. Oxford: Blackwell, 1998.

PIMENTEL, Isabela. **Gestão de risco** reputacional. 2019. Disponível em: https://comunicacaointegrada.com.br/gestao-de-riscos-reputacionais. Acesso em: 05 ago. 2022.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 – LGPD. 2. ed. São Paulo: Saraiva Educação, 2020. E-book. Disponível: https://books.google.com.br/books?hl=ptBR&lr=&id=oXPWDwAAQBAJ&oi=fnd&pg=PT13&dq=Autoridade+nacional+de+prote%C3%A7ao+de+dados&ots=k8_mBpMKYJ&sig=b6-fTVclEUdJOpK4jzMU0F5v3Zg#v=onepage&q=Autoridade%20nacional%20de%20prote%C3%A7ao%20de%20dados&f=false. Acesso em: 07 out. 2022.

PONTICELLI, Murilo Meneghel**. O direito fundamental à privacidade no âmbito da rede mundial de computadores com o advento da Lei Geral de Proteção de Dados**. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade do Sul de Santa Catarina, Tubarão, 2018. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/6124/1/TCC%20Murilo%20Assinado.pdf. Acesso em: 2021.

PORTO, Éderson Garin. **Compliance e governança corporativa**: uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020.

PROJECT MANAGEMENT INSTITUTE. **A guide to the project management of body of knowledge:** Guia PMBOK®. 5. ed. Pensilvânia: Project Management Institute, 2013.

PROTIVIT.com.brpor?utm_source=google&utm_medium=cpc&utm_campaign=icts&utm_id=pesquisa&utm_term=protivitiinstitucional&gclid=Cj0KCQjwwJuVBhCAARIsAOPwGAQl6BGoOIYe5bELYCkQ2IwpLbdFMSXgeIR3T-3vDMrCMaQ9GP8uNgwaAqxKEALw_wcB. Acesso em: 10 jun. 2022.

REFERENCIAL básico de gestão de riscos. Brasília: TCU, 2018.

RODOTA, Stefano. **Uno statuto giuridico globale dela pesona elettronia**. Discurso proferido na 23ª Conferência Internacional sobre a Privacidade e a proteção de Dados Pessoais em Paris. 24 set. 2001. Disponível em http://intelex .it/675/rodotat.htm. Acesso em 20 jun.2022.

SANTOS, Dhiulia de Oliveira. A validade do consentimento do usuário à luz da lei geral de proteção de dados pessoais: lei n. 13.709/2018. 2019. 50 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Centro Universitário de Brasília - Uniceub, Brasília, 2019. Disponível em: https://repositorio.uniceub.br/jspui/handle/prefix/13802. Acesso em: 31 out. 2022.

SARLET, Ingo W.; DONEDA, Danilo; MENDES, Laura S. **Estudos sobre protecao de dados pessoais**. São Paulo: Saraiva, 2022. Coleção Direito, tecnologia, inovação e proteção de dados num mundo em transformação.

SCHREIBER, Anderson. **Responsabilidade civil na lei geral de proteção de dados pessoais**: tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2020.

SILVA, Daniel C.; COVAC, José R. **Compliance como boa prática de gestão no ensino superior privado**. 2015. 9788502624382. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502624382/. Acesso em: 20 jun. 2022.

STEINBERG, Richard M. *et al.* **Enterprise risk management framework (DRAFT)**. Comittee of Spon- soring Organizations of the Tradeway Commission (COSO), 2003.

STEINBERG, Richard M. **Governance, risk management, and compliance**: it can't happen to us--avoiding corporate disaster while driving success. [*S.l.*]: John Wiley, 2011.

STOLTZ, Brenda. A new california privacy law could affect every u.s. business – will you be ready? **Forbes**, 2019. Disponível em: https://www.forbes.com/sites/allbusiness/2019/09/07/california-consumer-privacy-act-could-affect-your-business/?sh=6aa04d5c36ac. Acesso em: 22 jun. 2022.

TAVARES, Daiane Gabriela Lucas. **Quais são as etapas de um processo de gestão de riscos?** Disponível em: https://www.mmpcursos.com.br/blog/quais-etapas-processo-gestao-riscos. Acesso em: 14 jul 2022.

TUTTLE, Hilary. Global regulation landscape: data protection in 2018. **Risk Management**, v. 65, n. 11, p. 28-34, 2018.

UNIÃO EUROPEIA. **Article 29 working party**. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Disponível em:https://ec.europa.eu/justice/article 29/documentation/opinionrecommendation/files/2014/wp217_en.pdf. Acesso em: 2022.

UFVJM Universidade Federal dos Vales do Jequitinhonha e Mucuri. Campus do Mucuri. **Plano de Conformidade da UFVJM à Lei Geral de Proteção de Dados** Disponível em https://portal.ufvjm.edu.br/page/lgpd/PlanodeConformidadedaLGPDA409ago2022FINAL.pdf acesso em 20 nov. 2022

VIEIRA, Victor Rodrigues Nascimento. **Lei geral de proteção de dados**: uma análise da tutela dos dados pessoais em casos de transferência internacional. 2019. 77 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2019. Disponível em: https://repositorio.ufu.br/handle/123456789/26233. Acesso em: 31 out. 2022.

WARREN, Samuel; BRENDEIS, Louis. The right to privacy. **Harvard Law Review,** v. 4, n. 5, p. 193-220, 15 dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 13 nov. 2022.

ZANATTA, Rafael A. F. **Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?** *In:* ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, 1., 2017, Rio de Janeiro.