**UNIVERSIDADE DE RIBEIRÃO PRETO**
**PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU**
**MESTRADO EM DIREITOS COLETIVOS E CIDADANIA**

**JOSÉ JANDER DIAS FERREIRA JUNIOR**

# SISTEMA PROTETIVO DOS DADOS ESTUDANTIS - A (IN)APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NAS INSTITUIÇÕES PRIVADAS DE ENSINO SUPERIOR

**RIBEIRÃO PRETO**
**2022**

JOSÉ JANDER DIAS FERREIRA JUNIOR

# SISTEMA PROTETIVO DOS DADOS ESTUDANTIS - A (IN)APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NAS INSTITUIÇÕES PRIVADAS DE ENSINO SUPERIOR

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* Mestrado em Direitos Coletivos e Cidadania da Universidade de Ribeirão Preto, como requisito para a obtenção do título de mestre em Direito sob à orientação do Prof. Dr. Rafael Tomaz de Oliveira.

RIBEIRÃO PRETO - SP
2022

Ficha catalográfica preparada pelo Centro de Processamento
Técnico da Biblioteca Central da UNAERP

- Universidade de Ribeirão Preto -

FERREIRA JÚNIOR, José Jander Dias, 1989-

F383s Sistema protetivo dos dados estudantis: a (in)aplicabilidade da Lei Geral de Proteção de Dados nas instituições privadas de ensino superior / José Jander Dias Ferreira Júnior. – Ribeirão Preto, 2022.

119 f. : il.

Orientador: Prof.° Dr.° Rafael Tomaz de Oliveira.

Dissertação (Mestrado) - Universidade de Ribeirão Preto, UNAERP, Mestrado em Direitos Coletivos e Cidadania, 2022.

**JOSÉ JANDER DIAS FERREIRA JUNIOR**

# SISTEMA PROTETIVO DOS DADOS ESTUDANTIS – A (IN)APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NAS INSTITUIÇÕES PRIVADAS DE ENSINO SUPERIOR

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade de Ribeirão Preto para obtenção do título de Mestre em Direito.

Área de Concentração: Direitos Coletivos e Cidadania

Data da defesa: 05 de maio de 2023

Resultado: Aprovado

BANCA EXAMINADORA

Prof. Dr. Rafael Tomaz de Oliveira
Presidente/UNAERP

Prof. Dr. Emerson de Arruda
FASIPE

Prof. Dr. Juvêncio da Silva Borges
UNAERP

RIBEIRÃO PRETO
2023

# DEDICATÓRIA

Dedico este trabalho à memória de minha
saudosa mãe Cely Alves Galvão Ferreira

# AGRADECIMENTOS

Agradeço, primeiramente, a Deus por me manter em condições de saúde física e mental para o desenvolvimento deste trabalho, pois certamente sem Ele nada seria possível. Além disso, tudo se desenvolveu no cenário pandêmico da Covid-19, no qual, por três vezes, me infectei, mas, pela graça de Deus, sobrevivi e não perdi nenhum familiar.

Não foi fácil atravessar essa jornada desafiadora, com sentimentos de angústia e apreensão que, para minha realidade, era algo completamente desconhecido, em meio a uma pandemia, e com a substituição do orientador na reta final da escrita desta dissertação. Todavia, esse desafio só foi possível com o apoio incondicional da minha esposa Rhafaela Salgado, que sempre me apoiou e me motivou nos momentos em que pensava em desistir. Meu agradecimento a ela.

Agradeço também ao apoio recebido da minha irmã, Dra. Fabiana Ferreira, que sempre me serviu de inspiração e me incentivou a trilhar esse caminho acadêmico. Agradeço ainda ao meu pai e aos meus familiares, que me apoiaram e que puderam testemunhar a transformação de uma vida, passando de um menino que dava trabalho na escola para um estudioso profissional do Direito e professor universitário.

Agradeço a todos os professores e equipe do programa de mestrado em Direito da UNAERP e, em especial, agradeço ao Prof. Dr. Rafael Tomaz de Oliveira, que em um momento delicado de substituição de orientador, me auxiliou.

Agradeço aos meus colegas de turma do mestrado, que, em momentos de crise coletiva, havia motivação mútua.

Não poderia deixar de agradecer também ao Prof. Dr. Emerson Arruda, grande apoiador, amigo e incentivador nessa jornada, auxiliando em diversos momentos.

Agradeço ainda ao amigo Henrique da Cruz Monteiro, Bibliotecário Geral do Grupo Fasipe Educacional, que me franqueou acesso ao acervo da biblioteca digital, auxiliando substancialmente no desenvolvimento da pesquisa aqui apresentada.

Por fim, agradeço ao Prof. Deivison Benedito Campos Pinto, diretor presidente do Grupo Fasipe Educacional, que me motivou a seguir a carreira acadêmica, me proporcionando o suporte necessário para permanência no programa de mestrado e o desenvolvimento deste trabalho.

# RESUMO

Esta dissertação propõe analisar a adequabilidade das Instituições Privadas de Ensino Superior (IES) à Lei Geral de Proteção de Dados Pessoais (LGPD) por meio de um estudo de caso realizado no Centro Universitário Unifasipe. O objetivo é avaliar o estágio de adequação à Lei e o nível de compreensão sobre a importância de se adequar à lei, comparando com a literatura visitada sobre proteção de dados. Propõe-se, ao final, um quadro-modelo de adequação que sirva de base para auxiliar outras instituições, observando suas particularidades, na garantia da proteção dos dados estudantis. A pesquisa foi realizada pelo método de estudo de caso, explorando o ambiente e coletando informações internas sobre os stakeholders. Concluímos que a instituição está em fase embrionária de adequação à lei e que o nível de percepção da importância da adequação à lei é baixo. Todavia, a compreensão de que a governança de TI aliada a programas de *compliance* são as melhores soluções para atingir a conformidade à lei.

Palavras-chave: Lei Geral de Proteção de Dados. Instituições de Ensino Superior. Princípios. *Compliance*. Conformidade. Estudantes. Autodeterminação Informativa

# ABSTRACT

This dissertation proposes to analyze the suitability of Private Higher Education Institutions (IES) to the General Data Protection Law (LGPD) through a case study conducted at the Unifasipe University Center. The objective is to evaluate the stage of *compliance* with the Law and the level of understanding about the importance of complying with the law, comparing with the literature visited on data protection. It is proposed, at the end, a *compliance* framework that serves as a basis to assist other institutions, observing their particularities, in ensuring the protection of student data. The research was conducted by the case study method, exploring the environment, and collecting internal information about the stakeholders. We conclude that the institution is in an embryonic stage of *compliance* with the law and that the level of perception of the importance of *compliance* with the law is low. However, the understanding that IT governance allied to *compliance* programs are the best solutions to achieve *compliance* with the law.



Keywords: General Data Protection Law. Higher Education Institutions. Principles. *Compliance*. Conformity. Students. Informational Self-Determination.

# SUMÁRIO

# 1. INTRODUÇÃO

A globalização, informatização ou universalização do mundo trouxe muitos avanços e, com isso, mais problemas ou desafios que nos levam à discussão sobre a proteção de dados pessoais. Na atual fase tecnológica em que a sociedade está, a informação se tornou um bem de alto valor, impulsionado pelo uso das tecnologias da informação que, ao decorrer do tempo, ampliou os dados pessoais coletados, identificando os detentores desses dados e seus comportamentos, se tornando fator determinante de competitividade na economia mundial.

Mesmo que, eventualmente, não se saiba como fazer dinheiro com os dados, vale a pena tê-los, pois eles podem ser a chave para controlar e modelar a vida no futuro (HARARI, 2018).

Identifica-se que há uma tensão entre os interesses econômicos e as esferas das pessoas que têm o livre desenvolvimento da sua personalidade afetado pela circulação de seus dados (BIONI, 2021).

A evolução tecnológica e o desenvolvimento de meios de comunicação altamente eficientes, como a Internet, em que as limitações territoriais são ignoradas, transcendendo as barreiras geográficas, faz com que as redes da Internet proporcionem comunicação livre e global, se tornando essenciais para tudo. Com isso, a manipulação de informação e dados pessoais, algo que anteriormente estava restrito ao papel, se tornou disponível em meio digital (CASTELLS, 2003).

A era da informação está introduzindo uma nova forma urbana, a cidade informacional (CASTELLS, 2011). Entramos então na era da sociedade de informação e, não há dúvida, que o advento da sociedade de informação proporcionou uma releitura ao conceito de privacidade (PODESTÁ, 2019).

Com isso, a manipulação dos dados pessoais se tornou algo relativamente fácil. O tratamento e uso desses dados passaram a ser usados comercialmente e de modo indiscriminado, e, em certos casos, violando o direito de privacidade das pessoas titulares dos dados. Consequentemente, o tratamento e uso desenfreado dessas informações despertou a atenção de juristas e legisladores ao redor do planeta, chamando a atenção do mundo jurídico, haja vista a necessidade da segurança da informação, a proteção dos dados pessoais, os mecanismos de armazenamento desses

dados e a efetiva proteção do cidadão titular dos dados pelas empresas públicas e privadas.

Com o advento da Lei Nº 13.709/2018, a chamada Lei Geral de Proteção de Dados Pessoais, impulsionou-se a necessidade de adequação dos dados e, pensando nas Instituições Privadas de Ensino Superior, é que este estudo foi proposto, a fim de analisar como estas instituições se adequarão a essa nova legislação, já em vigência, para garantir a proteção de dados dos estudantes. Além disso, propôs-se a analisar as soluções que serão adotadas e quais os impactos que a adequação à LGPD proporcionará.

As Instituições de Ensino Superior sempre trabalharam com dados pessoais de seus alunos com a finalidade específica de ensino, emissão de certificados e diplomas, armazenando pastas com o histórico escolar contendo diversas informações pessoais.

Diante à nova legislação, é de grande importância esclarecer a adequação à LGPD e os meios de proteção que deverão ser adotados pelas Instituições Privadas de Ensino Superior, pois é natural que cause impacto direto na operação dessas organizações, devido à manipulação de dados pessoais e/ou dados pessoais sensíveis de centenas de alunos, ex-alunos e colaboradores, o que deverá ser feito com profissionalismo e eficiência, assegurando a proteção desses dados em conformidade com a lei e os princípios de proteção de dados.

A presente dissertação tem como metodologia de pesquisa científica o estudo de caso de natureza teórica, com objetivos exploratórios e explicativos, desenvolvido no Centro Universitário Unifasipe, através de revisão bibliográfica. Contudo, a dificuldade de acesso aos dados necessários para a construção do presente trabalho, inclusive em outras instituições privadas de ensino superior, forçou a pesquisa empírica em busca de respostas para uma problemática real e iminente.

Na construção desta dissertação, foi pesquisado os principais trabalhos que discorreram sobre a Proteção de Dados desde a sua gênese, decorrente do direito à privacidade, passando pela análise de obras que se pronunciaram sobre a implementação da Lei Geral de Proteção de Dados Pessoais nas organizações, procedimentos e adequações, para fins de comparação com o modelo a ser adotado pela instituição de ensino superior (IES) em questão.

A partir disso, foi observada a aplicação das disposições legais e literatura sobre a temática em perspectiva com o estágio de adequação observado na IES, servindo como fundamento inicial a hipótese sugerida ao problema de: "O que é necessário para a adequação da Instituição Privada de Ensino Superior para assegurar a proteção dos dados estudantis de acordo com o regramento da Lei Geral de Proteção de Dados?".

A hipótese sugerida para investigação é de que a Instituição Privada de Ensino Superior deverá observar os princípios de privacidade, proteção de dados pessoais e dados pessoais sensíveis no tratamento de dados dos estudantes, diante às inovações tecnológicas, empregando os meios necessários para efetivar a proteção dos dados pessoais sensíveis ou não dos estudantes, implementando técnicas de *compliance*, governança da Tecnologia da Informação (TI) ou outras formas adequadas de gestão para cumprir a legislação de proteção de dados.

Sendo que, em síntese, a hipótese resume-se em uma asserção positiva, negativa ou no meio termo, com seus respectivos desdobramentos.

O método de abordagem da pesquisa de campo exploratória será utilizado, apresentando o tema na sua perspectiva teórica, iniciando pelo estudo dos princípios gerais e regras específicas da Lei Geral de Proteção de Dados Pessoais, Lei Nº 13.709/2018, entre outras normas, para atingir o objetivo da pesquisa e, ao final, termos um trabalho que sirva de auxílio por meio de um modelo conceitual para que a IES possa se adequar à legislação.

O referencial da pesquisa consiste em um marco histórico, sendo este o sancionamento da Lei Geral de Proteção de Dados Pessoais em vigência desde 18 de setembro de 2020. Todavia, para a construção do trabalho, abordou-se a formação do direito à privacidade na União Europeia, pois a Lei Geral de Proteção de Dados Pessoais do Brasil é formada sob forte influência da lei europeia. Por conseguinte, buscou-se autores que discorreram sobre a proteção de dados, privacidade e a fundamentalidade desse direito, bem como os que discorreram sobre a própria LGPD e a implementação nas organizações.

Dentre eles, podemos citar alguns dos autores que nortearam essa jornada, como: Danilo Doneda, Bruno Bioni, Cíntia Rosa Pereira de Lima, Bernardo Menicucci Grossi, Manuel Castells, Márcio Cots, Ricardo Oliveira, Silvano José Gomes Flumignan, Wévertton Gabriel Gomes Flumignan, Newton de Lucca, entre outros.

Portanto, a construção desta dissertação passou também por uma jornada teórica sobre a proteção de dados pessoais, até chegar na proteção de dados nas Instituições de Ensino Superior, com o estudo realizado em campo no Centro Universitário Unifasipe, no Estado de Mato Grosso, pois a implementação da Lei Geral de Proteção de Dados Pessoais é crucial para garantir a segurança e privacidade dos indivíduos, especialmente em uma era em que a informação é um bem valioso e pode ser facilmente manipulada.

A adequação das instituições privadas de ensino superior à essa legislação é fundamental para garantir a proteção dos dados dos estudantes, e é importante analisar as soluções adotadas e os impactos da adequação à LGPD.

Além disso, é importante lembrar que a proteção de dados não é apenas uma responsabilidade das instituições, mas também dos indivíduos, que devem estar cientes dos seus direitos e como proteger suas informações pessoais. A conscientização e a educação sobre a proteção de dados são fundamentais para garantir a privacidade e segurança de todos os indivíduos em uma sociedade cada vez mais conectada e dependente da tecnologia.

Deste modo, o tema pesquisado com os resultados apresentados nesta dissertação estará vinculado à linha de pesquisa em Concreção dos Direitos Coletivos e Cidadania, do programa de Mestrado em Direitos Coletivos e Cidadania da Universidade de Ribeirão Preto.

# 2. DIREITO À PROTEÇÃO DE DADOS PESSOAIS

Legislações sobre privacidade, liberdade e intimidade se desenvolveram face ao avanço tecnológico, ampliando os debates sobre o tema, a fim de assegurar os direitos dos indivíduos. A proteção de dados pessoais é outra forma de privacidade.

A privacidade, considerada por alguns autores como gênero, em que o direito à vida privada e à intimidade são espécies, por um longo período foi negligenciada pela maioria da população. Esses conceitos foram ignorados pelos povos antigos, pois a sociedade se desenvolvia nos espaços públicos, criando aspectos bem diferentes a depender da sociedade da época e suas dimensões político-sociais e econômicas. A ideia de privacidade evoluiu intrinsicamente ligada ao desenvolvimento da personalidade do indivíduo.

Privacidade, enquanto direito, só foi concebida ao final do século XIX, após o reconhecimento pela Declaração Universal de Direitos Humanos de 1948[1] (ONU, 1948), em função das transformações trazidas pela revolução industrial, consolidadas com a definição da Burguesia como classe social.

A privacidade tornou-se então direito autônomo, com estudos doutrinários sobre o tema, inicialmente categorizado como direitos humanos e, atualmente, com a constitucionalização, tornou-se um direito fundamental.

Com o avanço tecnológico, a coleta de informações, o processamento e a utilização se tornaram mais fáceis em função do volume de dados em circulação atualmente, elevando o temor social com a intimidade e privacidade, difundindo o desejo de assegurar o efetivo exercício desses direitos.

Logo, o direito à privacidade, após ser reconhecido internacionalmente, foi se acomodando em nosso ordenamento jurídico, evoluindo ligeiramente, a despeito da tutela propriamente ao direito à privacidade se tornar objeto de discussões mais aprofundadas recentemente.

---

[1] Somente no final do século XIX, o direito à privacidade surge como figura jurídica autônoma e se torna parte da ordem jurídica, expandindo-se à sociedade em geral. Colaborou para esse fenômeno a sua internalização pela Declaração Universal dos Direitos Humanos, proclamada pela Organização das Nações Unidas (ONU), que em seu art. XII, prevê: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra essas interferências ou ataques”.

A revolução tecnológica ocorrida na década de 1970, concretizou um novo estilo de produção, comunicação, gerenciamento e vida, assim como o resultado da revolução tecnológica, o fenômeno da Internet e as novas formas de comunicação desencadearam o início da sociedade digital. (CASTELLS, 2019).

A sociedade, cada vez mais global, está impulsionada pelo crescimento explosivo de tecnologias e ferramentas de comunicação, as quais universalizam o estilo de vida, a cultura e os padrões de produção e consumo, ou seja, um espaço com alto fluxo de informações que promoveu uma nova forma de relacionamento humano, sendo necessário repensar a questão da privacidade.

O volume de dados produzidos adquiriu grande valor, extrapolando a esfera da privacidade, tornando-se então fonte de poder. Ao deter a informação, significa controlar as riquezas principalmente com as novas tecnologias na sociedade digital, que permite o processamento e transmissão sem limites geográficos e em larga escala, algo inimaginável anteriormente.

Em função desse grande volume de informações em circulação, houve a necessidade de uma solução para armazenar de forma organizada essas informações, criando-se assim os bancos de dados, permitindo coletar, armazenar e distribuir diversos dados. (DONEDA, 2020).

O banco de dados, em sua forma inteligente de transformação e utilização, pode contribuir para instrumentalizar uma fonte de riquezas, permitindo assim sua monetização. Paralelamente, pode possibilitar a geração de informes de diferentes naturezas e, com seus resultados precisos, auxiliar nas escolhas e tomadas de decisões, possuindo clara função econômica. Isso possibilita a melhoria da experiência de consumo e a multiplicação de negócios de os matizes, com reflexos no desenvolvimento (SIMÃO FILHO, 2019).

Com novas soluções, novos conflitos e abusos também são criados, principalmente os relacionados à vida pessoal dos sujeitos, que passaram a observar a violação de direitos fundamentais, como a privacidade. Isso ocorre devido à alavancagem na utilização de dados, que fez com que a manipulação das informações pessoais ganhasse evidência no meio social, culminando em abusos de direitos fundamentais.

O conceito de privacidade, ante essas novas perspectivas, passou por uma nova significação, saindo de uma liberdade negativa para uma liberdade positiva. Antes,

quando se pensava em privacidade, o intuito era proteger a pessoa do Estado. (BIONI, 2019).

Diante às novas tecnologias e ao processo acelerado dos mecanismos computacionais, o pensamento sobre a privacidade passou a requerer a tutela do Estado, com o objetivo de efetivar esse direito, em função das sucessivas violações ocorridas no meio cibernético.

O perfil da privacidade agora se molda conforme as informações pessoais são condicionadas pela tecnologia, onde o objeto central passou a ser os dados. A sociedade vive o momento em que os dados são o "novo petróleo"[2], de modo que o processamento em larga escala é explorado de forma comercial através da utilização de potentes softwares e inteligência artificial, que permitem o acesso, o armazenamento e a alteração de dados pessoais. (Doneda, 2020).

Essas novas ferramentas permitem a manipulação das informações de forma completamente automatizada, definindo os perfis de consumo dos indivíduos com base nos dados pessoais coletados, comercializando essa informação aos grandes conglomerados para direcionar o conteúdo promocional de acordo com o perfil de consumo.

A era da informação permite que o mercado acompanhe a vida dos cidadãos, conhecendo seus hábitos, seja quando compram algo na internet ou sabem os lugares que frequentam ao usarem um cartão de crédito. Entendem suas preferências por bancos, carros, revistas e jornais. Com todos esses dados gerados diariamente, é possível tratá-los para que se torne informação disponibilizada por outros fornecedores. Em termos de tecnologia, várias mensagens publicitárias são enviadas para os e-mails de potenciais compradores, com base nesses tratamentos de dados.

O contexto de sociedade global permite que os indivíduos sejam bombardeados diariamente com um volume gigantesco de informação, seja nas redes sociais, sites de busca ou notícias na internet. Muitas vezes, há a necessidade de realizar algum cadastro e inserir informações pessoais para acessar determinado conteúdo. Na sociedade digital, com os dados pessoais se tornando o objeto central na ótica da privacidade, a necessidade de garantir a proteção desses dados se torna cada vez mais

[2] TOONDERS, J. Data Is the New Oil of the Digital Economy. WIRED. Disponível em: https://www.wired.com/insights/2014/07/data-new-oil-digital-economy/. Acesso em: 05 mai. 2022.

latente, emergindo a tutela do direito à proteção dos dados pessoais derivado da privacidade.

Como menciona Bruno Bioni (2021, p. 95), "o direito à proteção de dados pessoais angaria autonomia própria. É um novo direito da personalidade que não pode ser amarrado a uma categoria específica, em particular ao direito à privacidade", sendo esse direito observado atualmente em diversos países, reconhecido, inclusive, como direito fundamental, demonstrando assim a relevância da autonomia desse direito bem como estudos mais aprofundados.

Não podemos deixar de perceber que são intrínsecos os direitos de personalidade, e fazem com que esse direito seja entendido pela perspectiva constitucional e como direito fundamental do indivíduo, pois os dados pessoais nada mais é que uma extensão da personalidade do ser.

A fim de efetivar os direitos à liberdade, privacidade, intimidade, honra e à imagem, contemplados pela Constituição Federal de 1988, não apenas no meio real, mas também no ambiente virtual, o Brasil, que estava atrasado em relação ao tema, desenvolveu legislação específica para a Proteção de Dados, seu uso e transferência. Isso foi impulsionado por escândalos de uso indevido de dados pessoais como nas eleições americanas de 2016 envolvendo a Cambridge Analytica[3].

Foi realizado manipulação em massa de indivíduos na sociedade, coletando dados em diversos países desde 2014, traçando inclusive perfis psicológicos dos mesmos e bombardeando-os com informação de conteúdo direcionado, levando alguns países como Alemanha, Argentina, Austrália a implementar legislação com intuito de proteger os dados. (KAISER, 2020).

No Brasil, a ideia de direito à proteção de dados como um direito fundamental foi intensificada após o advento da Lei Geral de Proteção de Dados (LGPD), Lei 13.709 de 14 de agosto de 2018, com redação dada pela Lei Nº 13.853 de 2019. Ela implementa uma série de proteções da coleta, tratamento e uso de dados pessoais, instituindo inclusive uma Autoridade Nacional de Proteção de Dados (ANPD).

A Lei Geral de Proteção de Dados, em vigência desde 18 de setembro de 2020, concebeu um arcabouço de regras norteadoras, direitos, obrigações e penalidades para o uso indevido e tratamento de dados pessoais. O Senado Federal ampliou o rol de

[3] Cambridge Analytica (UK), Ltd. (CA) foi uma empresa privada que combinava mineração e análise de dados com comunicação estratégica para o processo eleitoral. Foi criada em 2013, como um desdobramento de sua controladora britânica, a SCL Group para participar da política estadunidense.

garantias individuais em nossa Constituição Federal ao aprovar a PEC (Proposta de Emenda à Constituição) 17/2019, alterando o artigo 5º, inciso XII, e o artigo 22, inciso XXX, para adicionar de forma expressa o direito à proteção de dados pessoais.

Em 2020, os debates sobre o tema se elevaram, ganhando destaque em função da Ação Direta de Inconstitucionalidade (ADI) nº 6387 MC/DF, no qual o Supremo Tribunal Federal, em decisão inédita, reconheceu um direito fundamental à proteção de dados, suspendendo a eficácia da Medida Provisória (MP) 954/2020.

A MP 954/2020 determinava que as empresas de telecomunicações prestadoras de Serviço Telefônico Fixo disponibilizassem os dados pessoais dos clientes, para que o Instituto Brasileiro de Geografia e Estatística (IBGE) realizasse a Pesquisa Nacional por Amostra de Domicílios (Pnad) Contínua, de forma remota em função da pandemia do Coronavírus.

A observância dos princípios da proteção de dados afeta a forma como as empresas lidam com os dados pessoais, sejam de seus clientes ou colaboradores. De igual modo, as Instituições de Ensino Superior (IES) também estão sujeitas a essa nova legislação e precisam adequar o modo como tratam os dados dos estudantes.

## 2.1. CONSTITUIÇÃO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS

A evolução tecnológica e o desenvolvimento constante das tecnologias de informação e comunicação, bem como a alteração social promovida pela internet, que não é apenas uma mera ferramenta, mas sim uma extensão da sociedade, transformou a percepção sobre o conceito de privacidade. Isso ocorreu porque alterou significativamente o limiar entre o público e o privado e as formas de armazenamento de informações, pois este armazenamento se tornou global.

Com a escalada tecnológica e a disponibilidade de informações existentes ao mesmo tempo e em todas as partes, trouxe o desenvolvimento de poderosos softwares coletores de dados, possibilitando a verificação cruzada de informações, aumentando a integridade e a qualidade dos dados, bem como o uso em diversas finalidades, inclusive com o potencial de influenciar as relações sociais.

A sociedade está em uma nova forma de organização, onde a informação é o elemento nuclear para o desenvolvimento da economia, como menciona Bruno Bioni (2021), destacando que esses dados são fontes novas de geração de riquezas, pois, ao conhecer sobre os comportamentos ou hábitos da população, entre outros dados, possibilita os setores públicos e privados a explorar isso no desenvolvimento das atividades da Administração Pública ou atividades comerciais.

A informação ganha um novo ponto focal em função da aplicação de novas tecnologias informacionais, mais potentes, eficientes e maleáveis, notadamente aumentando a capacidade produtiva da própria informação, tornando-a um produto no processo produtivo. Isso passa a ser reconhecido como um fenômeno relevante juridicamente, necessitando assim de uma efetiva proteção, evitando o uso indevido ou manipulações. (DONEDA, 2019).

Stefano Rodotà (2008) afirma que a proteção de dados pessoais tem ganhado autonomia própria e provocado o desenvolvimento paralelo de leis relacionadas ao tema, criando uma nova fronteira.

A demanda regulatória específica surge permeando os interesses Estatais nos pós Segunda Guerra Mundial, quando a máquina administrativa percebe que as informações pessoais de seus cidadãos são úteis para planejar e coordenar suas ações para um crescimento ordenado (BIONI, 2021).

Alguns países, como os Estados Unidos, cogitaram criar um banco de dados nacional, desenvolvendo então o projeto National Data Centers, idealizado como uma base central unificada de dados sobre a população norte-americana para uso dos interesses do Estado.

Esta base de dados reuniria, simultaneamente, informações de censo, fiscais, trabalhistas, previdência social, entre outros, o que possibilitaria controlar e monitorar ilimitadamente os dados dos cidadãos. Entretanto, discussões sobre a violação de liberdades individuais forçou o projeto não ir adiante, a despeito do governo dos Estados Unidos da América acreditar que, diante dos avanços tecnológicos, seria natural essa implementação na estrutura administrativa. (DONEDA, 2020).

De igual modo, outros países europeus seguiram a mesma ideia dos norte-americanos e, tal qual ocorreu lá, debates acirrados sobre a privacidade dos cidadãos foram travados, subsistindo em uma reação negativa ao controle da Administração Pública dos dados dos indivíduos. (DONEDA, 2020).

A primeira geração de leis de proteção de dados pessoais, segundo Bruno Ricardo Bioni (2021), decorre da preocupação com o processamento massivo dos dados pessoais dos cidadãos na conjuntura da formação do Estado Moderno.

Logo, a primeira geração de leis passou a existir devido à grande preocupação com a manipulação massiva de dados pessoais. Essas leis marcam a primeira geração de leis de proteção de dados, como registra Danilo Doneda (2011), "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".

O primeiro texto legal editado foi a Lei do Estado Alemão de Hesse de 1970, conhecida como Hessisches Datenschutzgesetz, que regulamentava os bancos de dados do governo, sendo uma legislação precursora em se ater às questões de coleta e tratamento de dados pessoais, porém, tratava o assunto apenas de forma genérica.

Destaca-se também a lei sueca de 1973, reconhecida como Datalegen, e a Lei Federal de Proteção de Dados da Alemanha de 1977, que, de igual modo, possuíam características equivalentes às leis de primeira geração, sobre o controle da criação dos bancos de dados pelo governo com regimes de concessões e autorização prévia.

Essas leis não possuíam a participação ativa do cidadão, mas a estrutura normativa se destinava aos agentes responsáveis pelo processamento dos dados. As leis até traziam em seu bojo princípios de proteção, mas, muitas vezes, eram abstratos e amplos, focalizados basicamente na atividade do processamento de dados. (DONEDA, 2020).

Danilo Doneda (2019) destaca que as leis de primeira geração sobre proteção se tornaram desatualizadas, pois “diante da multiplicação dos centros de processamento de dados, que tornou virtualmente difícil propor um controle baseado em um regime de autorizações, rígido e detalhado, que demandava um minucioso acompanhamento”.

A evolução tecnológica e a expansão dos grandes centros de tecnologia que extrapolaram a esfera pública e adentraram também a esfera privada tornou essas leis ineficientes, embora tenham sido de grande relevância como inspiração para diversas outras legislações ao longo dos anos.

Movidos por um novo paradigma voltado à privacidade do cidadão, os mecanismos de controle se destinaram a preocupar mais com as liberdades individuais gerais, por decorrência das novas tecnologias informacionais e o uso significativo dos

bancos de dados em rede, nascendo assim a segunda geração de leis sobre proteção de dados, como por exemplo as leis da França sobre proteção de dados em 1978, a lei austríaca, dinamarquesa e norueguesa.

Destaca-se ainda as cartas Magnas de Portugal e Espanha que trouxeram pela primeira vez o conceito de privacidade informacional, o que significou para a época uma mudança de padrão pois, conforme Danilo Doneda (2019) “o fornecimento de dados pessoais pelos cidadãos tinha se tornado um requisito indispensável para a sua efetiva participação na vida social”.

Essas leis da segunda geração, ao contrário das leis de primeira geração, trouxeram a participação ativa do cidadão, com o objetivo de proteger sua privacidade e garantir seus direitos individuais, tornando-se assim mais eficientes e adequadas às necessidades da sociedade contemporânea.

A segunda geração de leis sobre proteção de dados surge como consequência dos debates sobre o direito ao acesso das pessoas as suas informações pessoais e sobre consentimento, estabelecendo ainda a transparência em relação à existência dos bancos de dados com informações pessoais e seus critérios básicos de funcionamento (DONEDA, 2011).

Com o objeto ampliado à medida que a tecnologia avança e os limites da esfera privada adquire maior relevância jurídica, proporcionalmente ao crescimento da preocupação dos indivíduos com a privacidade. Consequentemente, “a extensão da área abrangida pela tutela da privacidade fez com que aumentasse, paralelamente, o número de sujeitos interessados em tal proteção bem como sua relevância social” (RODOTÀ, 2008).

Com isso, o indivíduo passa a ser o personagem principal na proteção de seus dados, modificando o tratamento do tema inclusive pelo reconhecimento por Constituições como direito fundamental, fortalecendo assim a formulação de leis mais abrangentes sobre a proteção de dados que foram formuladas posteriormente.

Essa nova geração de leis trouxe uma maior autonomia ao indivíduo para controlar suas informações, dando origem na década de 80 a terceira geração de legislações sobre a proteção de dados, marcada pela extensão das liberdades decorrentes das leis de segunda geração, conhecida como autodeterminação informativa.

Essa terceira geração de leis visa garantir aos indivíduos o direito de controlar e decidir sobre o uso de suas informações pessoais, incluindo a possibilidade de acesso, correção e exclusão de dados. Além disso, essas leis também incluem medidas de segurança para garantir a proteção dos dados contra acessos não autorizados e violações.

Com a evolução constante da tecnologia e o crescimento do comércio eletrônico, a proteção de dados pessoais se torna cada vez mais importante e essas leis de terceira geração são essenciais para garantir a privacidade e os direitos individuais dos cidadãos.

A terceira geração de legislações sobre proteção de dados é marcada pelas normas que entregam o protagonismo ao indivíduo, no qual este tem a participação sobre os movimentos de seus dados desde a coleta até o compartilhamento (Bioni, 2021, p.130). Com isso, tem-se a ideia de autodeterminação informacional notoriamente evidenciada pela Corte Constitucional Alemã, em 1983, ao declarar, em decisão, a inconstitucionalidade parcial da Lei do Censo Alemão (Volkszählungsgesetz), na qual discorria sobre o censo populacional.

A Lei do Censo previa a possibilidade de utilizar os dados coletados cruzando-os com outros registros públicos, em atividades administrativas, prevendo inclusive multa para os que se recusassem a responder às perguntas. Todavia, a finalidade da lei não era específica. Por ser genérica e levantar muitos questionamentos, a corte alemã, em decisão, determinou o compartilhamento apenas para fins de recenseamento, pois "estaria caracterizada a diversidade de finalidades, o que impediria que o cidadão conhecesse o uso efetivo que seria feito de suas informações" (DONEDA, 2019).

Com a decisão do Tribunal Constitucional Alemão, passou-se a vislumbrar a autodeterminação informativa para além do consentimento. Com efeito, temos uma ideação decorrente desse termo sobre a perspectiva da proteção de dados como um direito de personalidade autônomo, creditando a proteção de dados como uma parte do direito geral da personalidade, conferindo ao sujeito, então, decidir qual a proporção dos aspectos pessoais de sua vida poderia ser divulgada.

Tal legislação estaria em desacordo com a dignidade da pessoa humana, pois, como é possível conhecer no compilado de cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão em coletânea de Jürgen Schwabe (2005), no

centro da ordem constitucional, está o valor e a dignidade da pessoa que age com livre autodeterminação.

Caberia a coleta e uso de dados pessoais com destinações estatísticas apenas, reconhecendo ainda a necessidade de que o cidadão obtivesse a informação prévia sobre a coleta e processamento dos dados que lhes pertencem, assegurando o princípio da finalidade.

A constitucionalidade parcial da lei foi declarada, o censo foi mantido, mas o Tribunal Alemão determinou que fossem adotadas as medidas necessárias para garantir aos cidadãos a segurança de seus dados, inclusive proibindo o compartilhamento com outros órgãos de governo, dados como endereço e nome dos cidadãos.

Com isso, pressupõe-se que ao indivíduo seja garantido a liberdade de decidir, garantindo a autodeterminação informativa e assegurando-a como um direito fundamental, demonstrando a preocupação com os avanços tecnológicos da época. Stefano Rodotà (2008) demonstra que o reconhecimento da autodeterminação informativa como um direito fundamental do cidadão se concretizou pela presença de riscos conexos ao uso das informações coletadas, e não uma vocação natural ao sigilo de certos dados pessoais.

Deste modo, ocorreu uma modificação social, pois o indivíduo obteve o poder de definir e administrar o uso de suas informações pessoais mediante seu consentimento, seguindo assim como referência para a quarta geração de legislações seguintes.

Nesse novo momento em que a quarta geração de legislações sobre proteção de dados se inicia, torna-se uma marca desse novo sistema jurídico a aplicação de princípios como o da publicidade, da exatidão, do livre acesso, da segurança física e lógica e o da finalidade, no qual deve "obedecer a finalidade comunicada ao interessado antes da coleta de seus dados", fazendo com que essa nova geração tenha "a parte mais aparente de uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua consideração como um direito fundamental em diversos ordenamentos" (DONEDA, 2011).

Essas legislações tiveram o objetivo de atestar o desequilíbrio na relação entre o indivíduo e o controle de seus dados, aplicando os princípios mencionados. Tornou-se possível consolidar a posição dos indivíduos, pois nessa quarta geração de leis incidiram a previsão de autoridades autônomas para tutelar esses dados, sendo

necessário instrumentos que elevassem o padrão coletivo de proteção, garantindo assim resultados concretos na tutela dos direitos dos cidadãos.

O Tribunal Alemão teve um papel de destaque, pois a decisão da lei do Censo estabeleceu a verdadeira gênese na proteção de dados, sendo tal posição uma grande influência para as legislações posteriores, doutrinas e jurisprudência pelo mundo sobre a autodeterminação informacional no seio constitucional, marcando assim o direito à proteção de dados como um direito decorrente do direito à privacidade.

Em resumo, o direito à proteção de dados é uma extensão dos direitos de personalidade, pois ela marca características individuais únicas, em que a violação expõe a autonomia do indivíduo à situação de vulnerabilidade, e a quarta geração de legislações sobre proteção de dados procura garantir essa autonomia, através de princípios como a publicidade, exatidão, livre acesso, segurança física e lógica e finalidade, e autoridades independentes para fiscalizar essas leis e garantir os direitos dos cidadãos.

## 2.3. INÍCIO DO MODELO EUROPEU DE PROTEÇÃO DE DADOS

O direito europeu expressa o desenvolvimento em quantidade e qualidade do direito à proteção de dados, tendo como marco inicial a autodeterminação informacional que promoveu a disseminação de muitos instrumentos jurídicos que se destinavam à proteção de dados. O controle sobre a coleta e o uso de dados, impulsionados pelo desenvolvimento e utilização de novas tecnologias, tornou-se uma grande preocupação na comunidade europeia. Desta forma, houve a necessidade de reestruturação supranacional, dando ensejo à necessidade de uma uniformização legislativa destinadas à proteção de dados.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) [4], organismo internacional, com suas *guidelines*, ou diretrizes, teve um papel importante nesse contexto de uniformização legislativa, no qual ressaltam a *Protection of Privacy* e

[4] Organização para a Cooperação e Desenvolvimento Econômico sendo um organismo internacional multilateral criado após a Segunda Guerra Mundial com o objetivo de promover o desenvolvimento econômico e o bem-estar social.

*declaration on transborder data flows*[5]. Essas diretrizes foram adotadas por vários países e contribuíram para a harmonização das leis de proteção de dados a nível internacional.

A OCDE também tem atuado como fórum para discussões sobre questões relacionadas à privacidade e proteção de dados, promovendo a cooperação entre os países membros.

Essas diretrizes foram de grande influência para o desenvolvimento das questões de privacidade e proteção de dados entre os países-membros. O resultado desejado era criar um ambiente regulatório uniforme entre os países-membros e, ante a inexistência de disparidades regulatórias, garantir o livre trânsito de informações (BIONI, 2021).

Em 1981, a Convenção 108[6], "incita os estados-membros do Conselho da Europa e demais signatários da Convenção a adotar normas específicas para o tratamento de dados pessoais, consonantes aos seus próprios parâmetros de proteção" (DONEDA, 2019). Diversos países-membros ratificaram a Convenção 108, adequando a legislação ao seu padrão. Logo, este foi o primeiro instrumento internacional a vincular a proteção de dados e, por conseguinte, tornou-se parâmetro, pois tratava a proteção de dados como Direitos Humanos.

Destacamos o fato de ser estendido o esforço de harmonização legislativa de forma "progressiva, [...] padronizaram o que significava para um país a busca pela proteção adequada de dados e para as organizações processarem dados pessoais com responsabilidade"[7]. Assim, conforme os países adotavam a padronização sobre a proteção de dados, maior era a influência para os outros países seguirem o mesmo caminho em suas legislações.

Em 1995, o Conselho da União Europeia e o Parlamento publicou a Diretiva 95/46/CE, motivados pelo ideal de um modelo único de proteção de dados, buscando efetivar as proposições da Convenção 108. Trouxe em seu bojo informações sobre a

---

[5] *Protection of Privacy* editada em 1980, em tradução livre Proteção da privacidade e *declaration on transborder data flows* editada em 1985, em tradução livre declaração sobre fluxos de dados transfronteiriços, sofreram atualizações em 2013

[6] *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* em tradução livre Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais Disponível em: https://www.coe.int/en/web/data-protection/convention108-and-protocol, esta convenção também era conhecida como Convenção de Strasbourg ou apenas Convenção 108 em círculos especializados (Doneda 2019)

[7] Bennett, Colin J. The European General Data Protection Regulation: An instrument for the globalization of privacy standards? Information Polity, n. 23, p. 239–246, 2018. DOI 10.3233/IP-180002 Versão Original: *Progressively, these harmonization efforts standardized what it meant for a country to pursue adequate data protection, and for organizations to process personal data responsibly.*

proteção de dados singulares, tratamento e circulação de dados, com a intenção de que os estados-membros pudessem harmonizar suas legislações. Essa diretiva foi uma das principais referências para a criação do regulamento geral de proteção de dados (RGPD) da União Europeia, que foi implementado em 2018, e que é considerado como a quarta geração de legislação de proteção de dados.

A Diretiva 95/46/CE demonstra interesse na proteção da pessoa, principalmente pelo fato de se referir a direitos fundamentais para garantir a proteção dos dados, todavia, garante a livre circulação dos dados entre os estados-membros.

Observamos que os seus objetivos se definem em dois eixos, em torno dos quais a disciplina se estrutura – a proteção da pessoa e a necessidade de proporcionar a livre circulação de "pessoas, mercadorias, serviços e capitais" no espaço comunitário, o que implica a circulação de dados pessoais – bem como a presença de um critério de equilíbrio entre ambos, que é a referência ao homem e aos seus direitos fundamentais, reconhecida como base e fundamento de toda a disciplina, pontua Doneda (2019).

Ressalta-se alguns aspectos importantes, trazidos pela Diretiva 95/46/CE sobre a atividade de processamento de informações pessoais, como por exemplo: o conceito de dados pessoais; conceito de destinatários dos dados; a previsão do tratamento de dados pessoais por meios automatizados ou não; a figura do responsável pelo tratamento; a possibilidade de consentimento do titular dos dados, garantindo o controle sobre suas informações ao indivíduo.

A Diretiva 95/46/CE tratava, como lembra Bruno Bioni (2021) de uma "[...] abordagem regulatória que se centra nesses dois atores – o titular das informações pessoais e quem as processa – para, por meio de direitos e obrigações simétricas, ser garantido o prometido controle dos dados pessoais."

Assim, exigia que os estados-membros adotassem a previsão de uma agência ou comissário de proteção de dados para assegurar "o controle e a fiscalização da aplicação dos diplomas de proteção de dados" (LIMA, PEROLI, 2019).

A Diretiva Europeia 2002/58/CE, que buscava regulamentar o tratamento e a proteção da privacidade, em especial nas comunicações eletrônicas, não veio para gerar inovação em relação à Diretiva 95/46/CE, mas sim, como uma sequência, no entanto, sem revogá-la, conformando tais disposições para se adequarem à realidade tecnológica no ambiente eletrônico, ficando conhecida então como "ePrivacy Directive".

Conforme pontua Cíntia Rosa Pereira de Lima (2020, p. 59), a "ePrivacy Directive foi uma resposta à economia informacional [...] na medida em que impõe limites à coleta, armazenamento e utilização de dados pessoais no contexto das comunicações eletrônicas".

A Diretiva 2002/58/CE coloca em evidência o direito à proteção de dados pessoais como um direito fundamental, pois em suas considerações iniciais faz menção direta à Carta de Direitos Fundamentais da União Europeia, em especial, aos artigos 7º e 8º que, respectivamente, dispõem sobre o respeito pela vida privada e familiar, e à proteção de dados pessoais.

A Carta consagrou a proteção de dados como um direito individual dos cidadãos europeus e destacou a proteção de direitos fundamentais. Assim, deu origem a um novo direito, segundo Rodotà (2008), como um direito "novo" e "autônomo", distinto da acepção tradicional de privacidade, contribuindo para a "constitucionalização da pessoa".

Em 2006, a Diretiva 2006/24/CE alterou a Diretiva 2002/58/CE, com o objetivo de harmonizar as disposições dos Estados-membros, para que os prestadores de serviços telefônicos mantivessem determinados dados para fins de investigação e repressão de crimes graves (LUCCA; MACIEL, 2019).

Nessa época, a Europa já possuía um sistema bem definido e estabilizado de normas, no entanto, apesar do modelo europeu de proteção de dados ser consolidado, passou por grandes debates em 2016, sofrendo uma grande alteração com a introdução do Regulamento (UE) 2016/679, que substituiu a Diretiva 95/46/CE, mais conhecida como *General Data Protection Regulation* (GDPR) ou Regulamento Geral de Proteção de Dados (RGPD) em português.

Com a entrada em vigor da RGPD, por meio de regulamento, substituindo uma diretiva, abrangeu os anseios de unificação do sistema, pois dispensava a necessidade de incorporação do texto supranacional por lei interna (GUIDI, 2019).

A RGPD, com vigência a partir de 25 de maio de 2018, elevou os padrões de privacidade internacionalmente, tornando-se um modelo global de confluências políticas e comerciais e sendo condição para aderir a esses padrões e participar da economia global. Este novo modelo europeu, que faz parte da quarta geração de legislações sobre o tema, iniciou uma nova fase para garantir a proteção de dados pessoais baseada no consentimento.

Rodotà (2008, p. 148) afirma que "os elementos-chave desse modelo são, portanto, o consentimento do interessado e o seu direito de acesso a todas as coletâneas de informações".

O GDPR, além de revogar a Diretiva 95/46/CE e trazer princípios, padrões e regulamentos novos para o tratamento de dados pessoais, incluindo aumento de penalidades, teve grande influência na legislação brasileira sobre proteção de dados, a chamada Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no Brasil em 18 de setembro de 2020.

Como demonstrado neste capítulo, o direito à proteção de dados é condição para o ingresso na vida pública devido à importância do tema e à elevação a classe de direito fundamental por diversos países em seus ordenamentos, em um efeito "dominó", pois a proteção de dados tornou-se a tutela da esfera relacional da pessoa humana. Assim, é uma exigência aderir a sistemas de proteção de dados para os países que desejarem manter relações comerciais com os países membros da União Europeia.

A implementação de regulamentos como a RGPD e a LGPD, bem como a influência do GDPR no âmbito internacional, reforçam a importância da proteção de dados como um direito fundamental e a necessidade de se garantir a privacidade e segurança dos dados pessoais.

A adesão a esses sistemas de proteção de dados é fundamental para garantir a confiança e a transparência no tratamento de dados pessoais, bem como para assegurar a conformidade com as normas internacionais. Além disso, é crucial para proteger a privacidade e os direitos individuais dos cidadãos, o que é fundamental para o desenvolvimento de uma sociedade democrática e justa.

# 3. A LEI GERAL DA PROTEÇÃO DE DADOS PESSOAIS

O atual modelo legal brasileiro foi influenciado pelo modelo europeu de proteção de dados pessoais, desta sorte se aproxima em seus anseios principiológicos e idealistas, abarcando normas que, na maior parte, difundem condutas aconselháveis e outras obrigatórias. Todavia, os padrões de interpretação restam aos aplicadores do Direito.

O consentimento ocupa papel de destaque na Lei Brasileira de Proteção de Dados (LGPD) igualmente acontece na legislação europeia (RGPD). Entretanto, em nossa lei, podemos perceber a ascensão desse direito a uma categoria autônoma. Isso ocorre em função do próprio exercício da proteção de dados pessoais, pois foge da bifurcação entre o público e o privado.

Difere-se significativamente do direito à privacidade, pois, conforme nos ensina Bruno Bioni (2021):

> “cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas. Hoje vivemos em uma sociedade e uma economia que se orientam e movimentam a partir desses *signos identificadores* do cidadão, há, portanto, uma série de liberdades individuais, atreladas ao direito à proteção de dados pessoais, que não são abraçadas pelo direito à privacidade”. (BIONI, 2021, p. 57):

Destaca a importância da proteção de dados pessoais em nossa sociedade e economia atual, onde o processamento de dados tem uma grande influência na vida das pessoas. Aponta que, como resultado, existem liberdades individuais que estão relacionadas ao direito à proteção de dados pessoais, mas que não são totalmente abrangidas pelo direito à privacidade. Isso sugere que a proteção de dados pessoais é uma questão importante e complexa que precisa ser considerada de forma adequada para garantir a privacidade e os direitos individuais dos cidadãos.

Com a elevação do direito à proteção de dados a uma categoria autônoma de direito, deixamos o pensamento desvinculado da privacidade e vinculamos à tutela da própria personalidade do ser, por estar intimamente relacionada com as liberdades individuais, como podemos observar no artigo 1º da Lei Geral de Proteção de Dados (Lei nº 13.709/2018):

> 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**. (BRASIL, 2018) (destacamos)

Ao longo do tempo, a evolução legislativa sobre a proteção de dados na Europa consolidou esse entendimento, firmado originalmente pela decisão do Tribunal Constitucional Alemão que declarou parcialmente inconstitucional a Lei do Censo em 1983, denotando a ideia de que a proteção dos dados é uma extensão do ser e sua personalidade, constituindo "elementos substanciais de nossa singularidade, podendo ser compreendidos como reflexos pessoais capazes de nos identificar em nossas particularidades e enquanto seres sociais" (COSTA; OLIVEIRA, 2019, p.11).

Os dados pessoais necessitam de tutela jurídica, pois essas informações constituem uma representação virtual do ser social. Por meios de informações corriqueiras coletadas nos meios digitais, revelam atributos intrínsecos da personalidade do indivíduo, tais como 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, classificados como dados sensíveis.[8]

Esses dados sensíveis podem ser coletados de modo a traçar um perfil individual ou coletivo que pode ser direcionado a usos indevidos dos dados pessoais, possibilitando inclusive práticas discriminatórias. Sendo assim, violações podem ocorrer caso não haja um controle adequado e legalmente estabelecido para o uso de dados pessoais.

O direito à proteção de dados ultrapassa a esfera da tutela da privacidade, tornando-se, portanto, um direito fundamental autônomo, vinculado de forma direta à proteção da personalidade. Desta forma, é errôneo utilizar, seja na literatura jurídica, legislação ou jurisprudência, que "o direito fundamental à proteção de dados consiste em mera evolução do direito à privacidade", sendo essa ideia uma "construção dogmática falha", conforme nos alerta Bruno Bioni (2021).

---

[8] A Lei Geral de Proteção de Dados Pessoais lei 13.709/2018, em seu artigo 5º inciso II, nos traz a definição de dado pessoal sensível, que pode ser constituído de informações relacionadas a 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

No Brasil, o direito à proteção de dados foi adicionado à Constituição Federal de 1988, por meio da Emenda Constitucional nº 115/2022, na qual altera o artigo 5º para adicionar o inciso LXXIX, que assegura a proteção de dados pessoais tanto em meios físicos quanto digitais, tornando assim o direito à proteção de dados um direito fundamental autônomo.

A EC nº 115/2022, além de adicionar o direito à proteção de dados ao inciso 5º da CF88, acrescentou ao artigo 21, o inciso XXVI, que deixa a cargo da União a competência de fiscalizar e organizar a proteção de dados e o tratamento de dados pessoais nos termos da lei.

Ainda acrescentou ao artigo 22 o inciso XXX, que faz competência legislativa sobre proteção de dados ser privativa à União. Assim, para melhor elucidação desta dissertação, abordaremos alguns aspectos da Lei Geral de Proteção de Dados Pessoais, passando por uma rápida análise pela evolução histórica e legislações relacionadas. Ademais, serão realizadas considerações à lei, discorrendo sobre os fundamentos, objetivos, aplicações e princípios.

## 3.1. PROGRESSO HISTÓRICO, LEIS E REGULAMENTOS SETORIAIS

Ao longo do tempo, a sociedade passou por diferentes tipos de organização social, de modo que, em cada período, existiu um elemento principal para o desenvolvimento. Como já mencionado anteriormente, após a Segunda Guerra Mundial, percebeu-se a importância das informações pessoais dos cidadãos para planejar ações com a intenção de promover o constante crescimento.

O avanço tecnológico e a globalização trouxeram uma dependência maior de bases de dados pessoais, diante dos negócios da economia digital (PINHEIRO, 2018). Portanto, a sociedade atual tem a informação como elemento central para o desenvolvimento da economia, sendo necessário normas para a proteção de dados pessoais.

Observa-se que existe uma zona de desigualdade no direito de proteção da privacidade e intimidade das pessoas em relação ao aumento no processamento de

dados, compartilhamento de informações impulsionado pelo desenvolvimento tecnológico e progresso da inteligência artificial (COTS, OLIVEIRA, 2021).

O Brasil dispunha apenas de normas setoriais sobre a proteção de dados pessoais até a sanção da Lei Geral de Proteção de Dados Pessoais (LGPD). Anteriormente, se valia do Código de Defesa do Consumidor (CDC), da Lei do Cadastro Positivo, da Lei de Acesso à Informação, da Lei Carolina Dieckmann, do Marco Civil da Internet e da Constituição Federal, entre outras legislações.

A Constituição Federal estabelece o direito à inviolabilidade da intimidade, da vida privada, honra e imagem das pessoas, possibilitando o direito à reparação pelo dano material ou moral decorrente da violação desses direitos. A CF/88 ainda permite a impetração de habeas data para efetivar o conhecimento de informações contidas em bancos de dados ou registros de entidades governamentais ou de caráter público, relacionadas ao impetrante, para retificação de seus dados, quando não for possível realizar por meio de processo administrativo ou judicial ordinário.

Já no CDC, no artigo 43, que disciplina os bancos de dados de informações de consumidores, destaca-se a possibilidade de conceder aos consumidores direitos como acesso, retificação e cancelamento, bem como a transparência e limite de tempo para que o consumidor possa exercer o controle de suas informações, consignando assim a autodeterminação informativa.

A Lei 12.414/2011, conhecida como a Lei do Cadastro Positivo, aborda questões sobre a formação de bancos de dados de adimplentes (bons pagadores) com o intuito de concessão de crédito. Conforme aponta Bruno Ricardo Bioni (2021), entre os direitos previstos, destaca-se "a orientação de que o titular dos dados pessoais deve ter o direito de gerenciá-los", denotando, assim, novamente a referência da autodeterminação informativa.

A Lei 12.527/2011, Lei de Acesso à Informação, estabelece procedimentos a serem adotados pelos órgãos públicos, com o objetivo de salvaguardar o direito de acesso à informação para todos, de acordo com a previsibilidade do direito fundamental consagrado na nossa Constituição Federal em seu artigo 5º inciso XXXIII.

A Lei 12.737/2012, conhecida como Lei Carolina Dieckmann, veio tipificar o crime de invasão de dispositivos informáticos, como computadores e celulares de terceiros, proporcionando assim uma elevação ao nível de proteção da privacidade dos indivíduos.

O Marco Civil da Internet, consagrado pela Lei 12.965/2014, no qual a iniciativa ocorreu influenciada pela denúncia efetuada por Edward Snowden[9], no escândalo de espionagem do governo americano, estabelece direitos e garantias ao cidadão para utilização da internet no Brasil.

Conforme depreende da análise dos dispositivos desta legislação, observa-se também como característica a autodeterminação informacional, não obstante ainda nos demonstra expressamente em seu artigo 3º, II e III, a previsão do direito à proteção de dados pessoais e à proteção da privacidade como elementos autônomos[10].

A temática se elevou na União Europeia, particularidade em que ocasionou a aprovação do RGPD, com o intuito de abordar sobre a proteção de dados pessoais de pessoas físicas, assim como o modo como são realizadas as operações com essas informações.

A instituição do regulamento europeu exigiu que os países com relações comerciais com a Europa dispusessem em seus ordenamentos uma legislação que efetivasse a proteção de dados pessoais em nível equivalente ao modelo europeu, sob pena de tornar-se mais difícil manter a realização de negócios.

A despeito da existência de leis esparsas que abordavam de certa forma a proteção dos dados pessoais, houve então a necessidade de criar uma normatização específica capaz de atender aos anseios e princípios internacionalmente consagrados.

A Lei Geral de Proteção de Dados, Lei nº 13.709 de 14 de agosto de 2018, foi sancionada com grande inspiração no modelo europeu, o RGPD, e dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, seja por pessoas naturais ou pessoas jurídicas de direito público ou privado. Portanto, esta lei tem como objetivo a tutela dos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, visto que o legislador entendeu a situação vulnerável

[9]Edward Snowden, ex-analista, da Agência Nacional de Segurança dos EUA, ficou conhecido por denunciar o episódio notório de invasões de privacidade cometidas pelos Estados Unidos, cuja referência ficou conhecida como a inauguração de uma nova era denominada de “pós-Snowden”. (LIMA, Cíntia Rosa, (Coord.) Comentários à lei geral de proteção de dados: Lei n. 13.709/2018, com alteração da lei n. 13.853/2019 / coordenadora Cíntia Rosa Pereira de Lima. – São Paulo: Almedina 2020, p. 269)

[10] O Dr. Adalberto Simão Filho no livro Direito e Internet IV, p.177 nos mostra que “no Brasil, a proteção de dados pessoais e a privacidade, foram previstas como elementos autônomos expressa no artigo 3º, II e III da lei 12.965/12, assim como ocorreu na União Europeia nos artigos 7º e 8º da Carta de Direitos Fundamentais calcados nos princípios vários adotados pelo legislador, sempre observando-se uma conduta de boa-fé.” (Direito & Internet IV: Sistema de Proteção de Dados Pessoais, 2019)

dos titulares dos dados em face aos responsáveis pelo tratamento desses dados (COTS; OLIVEIRA, 2021).

Observando o artigo 2º da LGPD, a temática sobre proteção de dados pessoais tem como fundamentos:

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

É evidente a ligação com o texto constitucional, no que tange à proteção dos direitos fundamentais, a fim de assegurar a privacidade, intimidade, honra, imagem e dignidade, assegurando então o controle sobre os dados pessoais ao indivíduo, garantindo a autodeterminação informativa.

Marcio Cots e Ricardo Oliveira (2021) discorrem sobre o tema e esclarecem que "[...] o fundamento da autodeterminação informada soma a possibilidade de manifestação de vontade do titular, que não poderá ser impedida por terceiros, com a obrigação do controle em prestar informações sobre os seus dados." Respeitar a privacidade está relacionado à possibilidade de o indivíduo ter controle sobre o que permite em sua vida privada, podendo decidir sobre a inclusão ou não de terceiros.

A LGPD consagrou o dever do Estado de desenvolver os interesses relacionados ao desenvolvimento econômico e tecnológico e à inovação, com a intenção de incentivar e promover o desenvolvimento científico, a pesquisa e a capacitação tecnológica. A lei se baseia nos princípios de garantir a livre-iniciativa e a livre concorrência, decorrentes do princípio da ordem econômica, como fundamento da República Federativa do Brasil.

## 3.2. APLICABILIDADE DA LGPD

No artigo 3º da LGPD fica delimitado a aplicabilidade da lei, *in verbis*:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - A operação de tratamento seja realizada no território nacional;
> II - A atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

A Lei Geral de Proteção de Dados Pessoais possui uma amplitude em relação aos destinatários, uma vez que a aplicabilidade incide em qualquer operação de tratamento de dados realizada por pessoas físicas ou jurídicas de direito público ou privado, sejam elas controladoras ou operadoras de dados.

A aplicabilidade da lei inova por recair sobre operações realizadas em qualquer meio, físico ou digital, ou seja, a lei deve ser aplicada até mesmo nos tratamentos off-line, e não somente nos meios digitais, como definido no Marco Civil da Internet.

Quanto ao tratamento de dados na internet, o Marco Civil da Internet se apresenta como uma lei geral, enquanto a LGPD é uma lei específica. Cabe destacar que a LGPD não revoga tacitamente o Marco Civil da Internet, pois este trata ainda assuntos como as diretrizes para a atuação do Poder Público e outros fundamentos e princípios relacionados ao uso da rede mundial de computadores no Brasil (MENEZES; COLAÇO, 2019).

A relação entre as legislações, como o Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei Geral de Proteção de Dados e a Lei de Acesso às Informações, deve prevalecer para garantir "ampla tutela aos titulares de dados submetidos a processamento no meio virtual" (MENEZES; COLAÇO, 2019, p.87).

A aplicabilidade da lei não está vinculada à localização da empresa ou origem dos dados, desde que alguma fase do tratamento ocorra no Brasil. Portanto, se qualquer

fase do tratamento de dados ocorrer em território nacional, seja na coleta ou processamento, será aplicada a LGPD.

De igual forma, a LGPD se aplica às atividades que têm como objetivo a oferta ou fornecimento de bens ou serviços, bem como ao tratamento de dados de pessoas localizadas em território nacional. Portanto, "o dado pessoal tratado por uma empresa de serviço de *cloud computing* que armazene o dado fora do país terá que cumprir as exigências da LGPD" (PINHEIRO, Patrícia Peck, 2021, p. 17).

Para que seja aplicada a LGPD, critérios como cidadania, nacionalidade e residência do indivíduo são irrelevantes, uma vez que a aplicação não está vinculada apenas a brasileiros. Como pontua Cíntia Rosa Pereira de Lima (2020, p. 85), "a LGPD vai além, pois prevê a aplicação da lei brasileira não apenas aos cidadãos brasileiros, mas toda e qualquer pessoa que esteja no Brasil, quando qualquer operação de tratamento de dados pessoais tenha sido realizada." Deste modo, a LGPD se aplica a toda e qualquer pessoa, independentemente da nacionalidade, mesmo que em trânsito no Brasil, estando assim resguardado pela legislação brasileira.

Além disso, a LGPD também se aplica a tratamentos de dados realizados por empresas estrangeiras que ofereçam bens ou serviços no Brasil ou que realizem operações de tratamento de dados de pessoas no território nacional. Isso mostra a importância da lei para garantir a proteção de dados pessoais, independentemente da origem ou localização das empresas e das pessoas envolvidas.

### 3.2.1. Excluídos da Aplicação da LGPD

A LGPD em seu artigo 4º traz exceções, quanto à aplicação da lei a pessoa natural que realizar o tratamento de dados pessoais para fins exclusivamente particulares e não econômicos, com finalidade exclusivamente jornalística, acadêmica ou artística, ou então para fins de interesse público pontuais ou para dados tratados fora do território nacional como é possível verificar no artigo 4º:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> I - Realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

> II - Realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - Provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. [...]

Temos como exemplo da primeira possibilidade de exclusão elencada no artigo 4º da LGPD o uso da agenda telefônica do celular ou anotações, possuir fotos de terceiros com você, não caracterizaria uma transgressão à lei ou violação de direitos.

O tratamento realizado por pessoa natural sem fins econômicos e exclusivamente particulares, ou seja, para uso pessoal, não caracteriza uma violação, visto que as relações de comunicação humana prescindem da troca de informações. Portanto, ainda que o exemplo retro citado possua dados de terceiros, não existe a figura da obtenção de vantagem financeira, não ensejando a aplicação da lei.

A aplicação da LGPD possui o objetivo primordial de tutelar a privacidade da pessoa natural, em função do desequilíbrio nas relações, pois quem detém o poder informacional são os agentes econômicos e o Estado, não sendo necessário, então, a aplicação da lei na comunicação entre sujeitos em pé de igualdade de informação.

Não é possível arguir a inaplicabilidade da Lei Geral de Proteção de Dados Pessoais no intento de causar dano ao bem jurídico; personalidade do titular, violando o direito de privacidade, honra ou imagem, que pode resultar em dano moral ou, mais gravosamente, se tornar um ilícito penal.

A segunda possibilidade retratada na lei se relaciona com o objetivo jornalístico, artístico ou acadêmico, pois a atividade jornalística, aquela exercida com propósito informativo, tendo como primórdio fins sociais, atendendo ao interesse público, não se confunde com intentos pessoais de manipular o público para determinado objetivo, seja pessoal ou comercial.

Caso a atividade seja realizada por órgão, empresa ou conglomerado econômico e constituir banco sem especificar claramente quanto ao uso ou tratamento

das informações contidas neste banco de dados, estará vinculado, sujeito aos desígnios da LGPD. (MENEZES; COLAÇO, 2019).

Já em relação à atividade artística, compreende-se que seja algo que expresse o direito de personalidade, através da capacidade criativa, não se sujeitando, também, à LGPD, ou seja, submete-se à "disciplina geral do ordenamento jurídico" (Menezes; Colaço, 2019, p. 88).

A lei 9.610/98, conhecida como Lei de Direito Autoral, em seu artigo 7º inclui a obra artística no rol de obras, frutos do intelecto e criatividade humana. Todavia, é importante destacar que "o direito de autor não protege as ideias, mas a sua expressão específica e concreta" (Vilela, C. M, 2021, p. 141).

Em relação à finalidade acadêmica, importa dizer que é a atividade realizada para elevação do conhecimento e produção científica, ou seja, é aquela relativa ao ambiente acadêmico, sendo assim, uma atividade vinculada às pesquisas desenvolvidas nas universidades, com autonomia concedida pela Carta Magna[11] brasileira em seu artigo 207. Portanto, a fiscalização da pesquisa é realizada pelos comitês de ética, não se sujeitando ao controle da LGPD neste ponto.

Ao passo em que não se sujeita à LGPD, esta faz menção expressa à aplicação dos artigos 7º e 11 nas circunstâncias de tratamento de dados pessoais e dados pessoais sensíveis, respectivamente, sendo, assim, uma aplicação parcial da lei no que tange à finalidade acadêmica.

Patrícia Pinheiro (2021) aduz que em "caso do uso acadêmico, precisa considerar que a utilização dos dados pessoais no tratamento em sala de aula, materiais didáticos, pesquisas universitárias fazem parte da exceção do art. 4º." A autora ainda destaca a existência de um anteprojeto, elaborado por uma comissão de juristas, que visa regulamentar o art. 4º da LGPD.

Prosseguindo então, nessa breve análise, adentramos na terceira possibilidade de não aplicação da LGPD, que se relaciona ao tratamento de dados pessoais, nas atividades de interesse público de finalidade exclusiva de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais.

No instante em que se identificar a prática delituosa, o tratamento de dados utilizado com a finalidade exclusiva de investigação, não estará mais plenamente

[11] Termo utilizado para se referir e Constituição Federal de algum país.

tutelado pela LGPD. Entretanto, às demais operações de tratamento de dados utilizadas pelo Poder Público, implicará a aplicação da LGPD integralmente.

A inaplicabilidade da lei não é irrestrita, pois a Lei Geral de Proteção de Dados Pessoais estabeleceu a regulamentação do inciso III por meio de legislação específica, a fim de que sejam observado o devido processo legal e os princípios gerais de proteção e os direitos do titular consignados na referida lei. (Abreu, 2020).

A legislação proíbe o tratamento de dados nestas atividades por pessoas jurídicas de direito privado, mas há exceções se o tratamento estiver sob responsabilidade de pessoas jurídicas de direito público.

Nesse caso, deverá ser feito um informe específico à Autoridade Nacional de Proteção de Dados, desde que o tratamento não seja sobre a totalidade dos dados, exceto se a pessoa jurídica de direito privado tiver capital integralmente constituído pelo Poder Público.

Por fim, a última possibilidade apresentada na LGPD, mais precisamente no artigo 4º do inciso IV, se refere ao tratamento de dados provenientes do exterior, que não sejam manipulados por agentes brasileiros e que não se refiram a pessoas localizadas em território nacional. Sobre essa possibilidade, é argumentado que esta exceção:

> [...] deverá beneficiar as empresas brasileiras, aumentando sua competitividade. Isso porque, ao tratar dados oriundos do exterior, na qualidade de operador, nunca de controlador, desde que os mesmos não sejam relativos às pessoas localizadas no território nacional, não haverá aplicação da LGPD. (COTS; OLIVEIRA, 2021, p. 85 - 86)

Relacionado ao tratamento de dados fora do Brasil, a interpretação será dada de forma restrita, pois caso ocorra qualquer etapa de tratamento de dados no Brasil, mesmo que proveniente do exterior, será aplicada a lei brasileira.

As inaplicabilidades apresentadas no artigo 4º da lei utilizam como justificativas direitos fundamentais, como o direito à liberdade de informação (atividade jornalística). No entanto, as inaplicabilidades da LGPD elencadas no artigo 4º se põem como absolutas, visto que no texto legal o § 1º deixa claro o dever de observar os princípios gerais de proteção ao titular previstos na lei.

Os dados continuarão sendo tutelados, assegurando aos titulares o direito de requerer o acesso, correção, anonimização ou eliminação desses dados, pois "um dos

pressupostos fundamentais da lei é que o tratamento de dados não poderá ser realizado sem que haja uma base normativa que o autorize". (DONEDA, 2018, p. 472).

## 3.3. PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Princípios são normas basilares, norteadoras, que servem como apoio teórico e fundamentação. São normas fundantes e nucleares de um sistema, que se apresentam como demarcadores do ponto inicial dos estudos de uma disciplina jurídica. Assim, sobre princípios, podemos compreendê-los como um arcabouço de regras capazes de afetar fatos jurídicos. (ABBOUD, CARNIO, OLIVEIRA, 2020, p. 403).

A LGPD, em seu artigo 6º, estabelece princípios a serem seguidos nas atividades de tratamento de dados, determinando, desde o início, a observância ao princípio da boa-fé.

### 3.3.1. Princípios da Boa-Fé

Dentre os princípios relacionados na lei, estão os princípios da boa-fé (art. 6º, caput), finalidade (I), adequação (II), necessidade (III), livre acesso (IV), qualidade dos dados (V), transparência (VI), segurança (VII), prevenção (VIII), não discriminação (IX), responsabilização e prestação de contas (X).

Compreende-se que a boa-fé consista em atender fielmente às expectativas de terceiros, levando em consideração a lealdade, honestidade e confiança, pautando a atuação em relação aos direitos e interesses alheios de forma justa e sem abusos, obstruções ou lesão. (SOARES, 2001, apud COTS, OLIVEIRA, 2021).

Sobre a boa-fé Silvano José Gomes Flumignan e Wévertton Gabriel Gomes Flumignan (2020, p.126) lecionam que:

> “A boa-fé também deve ser encarada sob o aspecto objetivo a partir de um padrão de comportamento leal, baseado na lisura, correção e probidade. Dessa noção decorrem as funções de corrigir, de suplementar, de interpretar e a de limitar o exercício de direitos.”

A boa-fé, portanto, é um princípio que deve ser respeitado nas operações com dados pessoais pelas Instituições de Ensino Superior Privada ao passo que guardar este princípio revela uma limitação em relação ao cometimento de abusos no tratamento de dados.

### 3.3.2. Princípio da Finalidade

Previsto no artigo 6º, inciso I da LGPD, fica expresso a necessidade de uma finalidade com propósitos legítimos, claros e objetivos, com a informação ao titular desses dados para que seja possível o tratamento, assim "[...] o princípio da finalidade constitui ferramenta de controle do uso e destinação dos dados pessoais coletados e tratados[...]" (Benacchio; Maciel, 2020, p. 64).

O princípio da finalidade deve ser respeitado, pois não é admissível que os dados sejam utilizados conforme o desejo do controlador, mas sim com o objetivo específico cientificado ao titular. Entendimento corroborado por Flumignan, S.; Flumignan, W. (2020, p. 129):

> Pode ser concebido também como decorrência da boa-fé objetiva já que está ligada à restrição do manejo das informações aos propósitos pretendidos com a coleta. Depreende-se do dispositivo legal que o tratamento dos dados pessoais não pode ser feito ao bel prazer de quem o controle.

De outro modo, Danilo Doneda (2020, p.216) completa que:

> Este princípio possui grande relevância prática: com base nele, fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que pode-se, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade).

É necessário, então, providenciar a cientificação do titular sobre qual é a finalidade do tratamento dos dados, impossibilitando, assim, o tratamento posterior com finalidade diversa da previamente informada ou definida.

Haverá lesão ao princípio da finalidade quando se informar que os dados a serem coletados se destinam ao faturamento de determinado produto ou serviço, entretanto, a destinação real é voltada para uma finalidade diversa, como, por exemplo, o uso desses dados em campanhas de marketing, ou seja, uma finalidade completamente diversa da informada anteriormente.

### 3.3.3. Princípio da Adequação

No inciso II do artigo 6º fica contemplado o princípio da adequação, que prescreve o dever de existir a compatibilidade do tratamento de dados com a finalidade informada ao titular, de acordo com o contexto do tratamento. Assim, novamente nos esclarece Flumignan, S.; Flumignan, W. (2020, p.130):

> Depreende-se de uma leitura atenta da definição legal dada à adequação que este princípio estará respeitado quando as finalidades informadas ao titular dos dados pessoais por quem realize o tratamento estejam em consonância com o contexto do tratamento ao titular dos dados pessoais por quem realize o tratamento estejam em consonância com o contexto do tratamento.

Portanto, o uso dos dados deve ser claro e justificado para o titular e deve estar de acordo com as razões pelas quais os dados foram coletados. É possível observar que o princípio da adequação está intrinsecamente relacionado ao princípio da finalidade, pois não é possível consignar o princípio da adequação se não estiver em harmonia com a finalidade, conforme depreende-se do posicionamento de Flumignan, S.; Flumignan, W. (2020, p. 131):

> Percebe-se, portanto, que a adequação está intimamente ligada ao princípio da finalidade, mas em um contexto mais objetivo. Observa-se o serviço prestado ou o produto fornecido e a necessidade de coleta dos dados. Somente se existir compatibilidade entre o serviço ou produto e o dado coletado, a exigência será legítima

Não se vislumbra então o distanciamento destes dois princípios que estão intimamente ligados e devem ser observados estritamente o cumprimento e a harmonia para que não haja nenhuma lesão aos direitos individuais dos titulares dos dados.

### 3.3.4. Princípio da Necessidade

O princípio da necessidade, previsto no inciso III do artigo 6º da LGPD, se relaciona à finalidade desejada, pois somente serão tratados os dados que forem necessários. Portanto, a intenção é a limitação da operação ao mínimo necessário para que concretize a finalidade.

Esse princípio assume duas características relevantes. A primeira se materializa pela elevação da responsabilidade de quem promove a coleta dos dados. A segunda característica verifica-se no fato de impossibilitar a coleta não essencial. Sobre essas características Flumignan, S.; Flumignan, W. (2020, p.131 - 132) afirmam que:

> [...] o primeiro aspecto, o próprio agente coletor deverá fazer uma ponderação sobre o que é essencial para o negócio. Isso ocorrerá porque quanto mais dados forem tratados, maiores serão as responsabilidades, pois os riscos com vazamentos e incidentes aumentam significativamente.
>
> A segunda faceta significa uma ideia de minimização do tratamento de dados, ou seja, apenas os dados imprescindíveis para a finalidade pretendida deverão ser tratados e, ainda que o agente coletor se responsabilize, aquilo que não for efetivamente útil, não deverá ser tratado sob pena de configuração de abuso de direito.

Verifica-se que a solicitação de dados relacionados à orientação sexual, para admissão em emprego, ou cor da pele para fornecimento de produtos e serviços incorre na violação desse princípio, pois não se trata de dados essenciais para a efetivação da contratação ou fornecimento do produto ou serviço e devem ser evitados para que não incorra em violação ao princípio da finalidade e do princípio da necessidade. É importante que as empresas e organizações sejam criteriosas na coleta de dados e façam uso somente do que é realmente necessário para a finalidade desejada, a fim de garantir a privacidade e os direitos dos titulares dos dados.

### 3.3.5. Princípio do Livre Acesso

O princípio do livre acesso encontra guarida no inciso IV do artigo 6º da Lei Geral de Proteção de Dados. Ele está relacionado ao princípio da transparência e assegura a consulta de forma facilitada e sem ônus para os titulares dos dados pessoais sobre a duração e forma do tratamento de seus dados, respeitando a integralidade destes dados.

A despeito de ser mencionado como um princípio na referida lei brasileira de proteção de dados pessoais, este princípio demonstra-se mais relacionado à figura da boa-fé, como um dever decorrente da necessidade de informação. (Flumignan, S.; Flumignan, W.; 2020)

A LGPD garante o princípio do livre acesso de diversas formas, como por exemplo, estabelecendo que os titulares dos dados têm o direito de obter informações sobre as finalidades do tratamento, as categorias de dados pessoais que estão sendo tratadas, as pessoas ou entidades com quem os dados foram compartilhados, entre outros.

Além disso, a lei também estabelece que os titulares dos dados têm o direito de acessar esses dados pessoais e solicitar sua correção ou exclusão, caso julguem ser necessário.

Outra forma pela qual a LGPD garante o princípio do livre acesso é a obrigação dos controladores dos dados de manter registros detalhados sobre as operações de tratamento de dados, incluindo as finalidades e categorias de dados envolvidos, os titulares dos dados, entre outras informações relevantes. Esses registros devem estar disponíveis para consulta pelos órgãos de fiscalização e os titulares dos dados também podem solicitar acesso a eles.

Além disso, a LGPD também estabelece a obrigação dos controladores dos dados de estabelecer mecanismos de consulta e solicitação de informações pelos titulares dos dados, como canais de comunicação eletrônica, telefone, entre outros.

O princípio do livre acesso garantido pela LGPD assegura aos titulares dos dados o direito de obter informações sobre o tratamento de seus dados, acessá-los e solicitar sua correção ou exclusão.

### 3.3.6. Princípio da Qualidade dos Dados

Ainda no artigo 6º, no inciso V, encontramos o princípio da qualidade dos dados, que se sustenta sobre o fundamento de garantir aos titulares dos dados transparência, clareza, exatidão, relevância e atualização dos dados, conforme se revele necessário para cumprir a finalidade do tratamento desses dados. O princípio da qualidade, conforme Flumignan, S.; Flumignan, W. (2020, p. 132):

> [...] impõe ao controlador um dever de verificação de correção em todos os procedimentos e operações. Outro aspecto é a necessidade de atualização regular dos dados e a garantia de segurança no caso concreto. A necessidade de atualização somente não ocorrerá em situações em que é proibido a atualização unilateral, como ocorre em áreas sensíveis como a da saúde do usuário.

Na qualidade dos dados, verifica-se a clareza da lei em determinar que a correção dos dados deve ser realizada imediatamente, assegurando assim a qualidade da informação. Verifica-se essa disposição então no artigo 18, III, §§ 3º e 4º.

### 3.3.7. Princípio da Transparência

O princípio da transparência, consagrado no inciso VI do artigo 6º, assegura aos titulares dos dados que as informações sejam fidedignas e precisas, garantindo acesso facilitado às características e informações relacionadas ao tratamento de seus dados, bem como às informações dos agentes de tratamento. No entanto, há ressalva sobre questões consideradas segredos industriais e comerciais. Neste sentido, verifica-se que:

> [...] pode-se citar o fato de que não é possível o compartilhamento de dados pessoais com terceiros de forma oculta. Caso quem efetue o tratamento de dados pessoais deseje repassá-los a terceiros, inclusive para operadores que sejam essenciais à execução do serviço, é necessário informar e obter o consentimento do titular dos dados pessoais. (FLUMIGNAN, S.; FLUMIGNAN, W. 2020, p.133).

O princípio da transparência, então, faz uma ressalva visando à proteção de segredos industriais e comerciais, fazendo com que sempre que houver o compartilhamento de dados com terceiros seja necessário informar o titular e obter sua autorização.

### 3.3.8. Princípio da Segurança

O princípio da segurança, previsto no inciso VII da LGPD, estabelece a utilização de meios técnicos e administrativos que garantam a segurança física e lógica dos dados pessoais, evitando o acesso não autorizado, situações ilícitas ou acidentais de destruição, perda, divulgação, alteração, difusão ou comunicação. Este princípio é abordado por Danilo Doneda (2020, p. 217) como sendo o “princípio da segurança física e lógica, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.”

Este princípio também pode ser encontrado em outras legislações, tratados, convenções ou acordos entre privados, sendo o núcleo das questões a serem abordadas pelo ordenamento para fornecer uma solução adequada à proteção dos dados pessoais. (FLUMIGNAN, S.; FLUMIGNAN, W. 2020).

### 3.3.9. Princípio da Prevenção

O princípio da prevenção, consagrado no inciso VIII do art. 6º da LGPD, faz aceno ao princípio da segurança, pois são muito próximos, justamente por utilizarem meios com o intuito de prevenir a incidência de danos em função do tratamento inadequado dos dados pessoais. Deste modo, compreende-se:

> [...] que o princípio da prevenção atua de forma a determinar que sejam adotadas medidas prévias para evitar ocorrências futuras de danos em virtude do tratamento de dados pessoais. Em outras palavras, as empresas devem atuar antes de eventuais danos, e não somente após a ocorrência destes. [...]

> [...]
> Neste sentido, o papel de quem realiza o tratamento de dados pessoais deve se dar de forma preventiva com o escopo de assegurar que os dados pessoais não sejam violados e nem que gerem eventuais danos aos seus titulares. (FLUMIGNAN, S.; FLUMIGNAN, W. 2020, p.135 -136)

O princípio da prevenção no tratamento de dados pessoais fala sobre a necessidade de adotar medidas prévias para evitar danos futuros. Ele destaca que as empresas devem agir preventivamente e não somente reagir após ocorrências de violação de dados. É reforçado o papel de quem trata dados pessoais deve ser preventivo, para garantir a segurança dos dados e evitar danos aos titulares.

### 3.3.10. Princípio da Não Discriminação

O princípio da não discriminação, com previsão legal no inciso IX, do art. 6º da LGPD, assinala o impedimento da realização do tratamento de dados pessoais para fins discriminatórios, abusivos ou ilícitos. Deste modo, ocorre o descumprimento do aludido princípio ao simplesmente "realizar oferta de produtos ou serviços apenas para pessoas de determinada nacionalidade" ou a segregação em função da identidade de gênero ou afins. (COTS; OLIVEIRA, 2021).

Deve-se observar que não é permitido utilizar os dados pessoais para discriminar e/ou promover abusos contra os titulares. Portanto, a exemplo de violação (FLUMIGNAN, S.; FLUMIGNAN, W. 2020, p.137) apregoa:

> [...] exemplo plausível de violação ao princípio da não discriminação é o de um determinado usuário que utiliza um aplicativo para controlar suas performances em exercícios físicos. Este aplicativo pode armazenar dados como batimentos cardíacos, doenças vasculares, se o indivíduo possui um hábito sedentário etc. Não será possível que este aplicativo forneça tais dados para empresas de seguros informando o hábito e questões pessoais do usuário para que elas calculem os riscos e aumentem, por exemplo, o valor do seguro de vida desta pessoa, pois estaria violando o princípio da não discriminação do usuário.

A utilização desses dados pessoais de forma indevida pode resultar em danos ao titular. Isso reforça a importância do princípio da prevenção e da proteção dos

dados pessoais. É crucial que as empresas e organizações que tratam dados pessoais estejam cientes dessas responsabilidades para evitar violação deste princípio da não discriminação, garantindo assim a privacidade dos titulares dos dados.

### 3.3.11. Princípio da Responsabilização e Prestação de Contas

Finalmente, o princípio da responsabilização e prestação de contas é definido no inciso X do artigo 6º da Lei Geral de Proteção de Dados (LGPD). Este princípio enseja a "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas"

Deste modo, (FLUMIGNAN, S.; FLUMIGNAN, W. 2020, p.137) destaca:

> Como exemplo de cumprimento a tal princípio, a comprovação de treinamentos de equipe, a contratação de consultorias especializadas, utilização de protocolos e sistemas que garantam a segurança dos dados bem como a facilitação do acesso do titular dos dados pessoais a empresa quando necessário.

É importante destacar que os princípios aqui elencados não esgotam a temática, pois, como é possível observar no artigo 64 da LGPD, menciona expressamente que os princípios contidos na lei "não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte".

Além disso, outros princípios fundamentais, como a transparência, a finalidade, a adequação, a necessidade, a obtenção de consentimento, a segurança e a responsabilidade também são importantes e devem ser levados em consideração no tratamento de dados pessoais.

# 4. O TRATAMENTO DE DADOS PESSOAIS

Neste capítulo, buscamos, inicialmente, estabelecer conceitos relacionados ao tratamento de dados pessoais. Posteriormente, serão explicadas as hipóteses que possibilitam o tratamento de dados pessoais, a definição de dados pessoais sensíveis, os dados pessoais de crianças e adolescentes e ainda será brevemente apresentada a hipótese que estipula o término da operação de tratamento de dados. Por fim, abordaremos o direito dos titulares dos dados.

É importante apresentar, antes de seguirmos aos próximos assuntos, alguns conceitos delimitados no artigo 5º da LGPD, para melhor elucidação sobre o tratamento de dados pessoais.

A LGPD, no artigo 5º, incisos I e II, aborda a diferença entre dados pessoais e dados pessoais sensíveis. No inciso III, descreve o que são dados anonimizados:

> 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;
> III - Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

O conceito de dados pessoais possui critério ampliado, pois, ao atribuir a possibilidade de o titular ser identificável por meio de seus dados, gera a identificação pela associação de outras informações, além de nome, sobrenome, CPF, endereço físico ou eletrônico, mas também pelo histórico de compras, número de IP (*Internet Protocol*) e passagens em pedágios, entre outros.

De acordo com Patrícia Peck (2020, p. 33 – 34), o conceito de dados pessoais é amplo e engloba toda informação relacionada a uma pessoa identificada ou identificável. Isso inclui, mas não se limita pois:

> Toda informação relacionada a uma pessoa identificada ou identificável, não se limitando, portanto, a nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, podendo incluir dados de localização, placas de

> automóvel, perfis de compras, número do Internet Protocol (IP), dados acadêmicos, histórico de compras, entre outros. Sempre relacionados a pessoa natural viva.

Já os dados pessoais sensíveis se referem a informações que dizem respeito à personalidade e expressão pessoal do indivíduo, como por exemplo, dados sobre orientação sexual, identidade de gênero, direcionamento político, religião, filiação sindical, origem racial e ainda sobre informações de saúde, dados genéticos, dentre outros.

Complementa Patrícia Peck (2020, p.35) que dados pessoais sensíveis são:

> [...] dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Manifesta-se a preocupação de haver discriminação em função dessas características, pois "os dados sensíveis são uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade" (BIONI, 2021, p. 83).

Por conseguinte, defendemos que o rol, expresso no inciso II do artigo 5º da LGPD, não deve ser compreendido como taxativo, pois são definidos conforme a potencialidade de causar vulnerabilidade com o tratamento destes dados, devendo assim designar a competência a Autoridade Nacional de Proteção de Dados, e a doutrina, delimitar os casos de se considerar como dados pessoais sensíveis.

Destaca-se que, em função de não haver ainda uma regulamentação bem definida, quanto ao posicionamento expresso anteriormente, a LGPD aplica normas distintas quanto ao tratamento de dados pessoais e dados pessoais sensíveis, com o intuito de repelir a utilização desses dados voltadas a práticas discriminatórias.

Em relação a dados anonimizados (inciso III, art. 5º), podemos dizer que são aqueles incapazes de produzir a identificação do titular após passar por um processamento denominado anonimização, fase na qual se desvincula o titular do dado por meio de técnicas específicas.

Evandro Eduardo Seron Ruiz (2020, p. 108) citando Carvalho Dias[12] aduz que:

> Anonimização é uma solução para a remoção de informações sensíveis de um documento. Carvalho Dias, especificamente define anonimização de dados como um processo para mascarar ou remover informações sensíveis de um documento preservando seu formato original

Nesse sentido, temos a definição legal sobre o processo de anonimização de dados no inciso XI, do artigo 5º da LGPD, que afirma ser a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

O artigo 12 da LGPD nos diz que "os dados anonimizados não serão considerados dados pessoais", portanto não se aplicando a LGPD nestes casos. Todavia, a lei coloca ressalvas dizendo que, se for possível a reversão do processo de anonimização, possibilitando assim identificar o titular, será aplicada a LGPD. Nesse sentido, Barreto, Almeida e Doneda (2020, p. 534) defendem que:

> Caso a anonimização seja revertida, os dados passam a ser considerados dados pessoais e as disposições da lei são aplicadas. Entende-se que o risco de reversão da anonimização se relaciona ao interesse e aos esforços de reidentificação das pessoas, que se configuram em contravenção.

Ao averiguar se o dado a ser tratado é considerado pessoal, faz-se necessário realizar "uma análise contextual que depende de qual tipo de informação pode ser extraída de uma base de dados", ou seja, do conglomerado de dados, estabelecido em um ou diversos locais, seja em meio físico ou digital (BIONI, 2021).

Já em relação ao banco de dados (inciso IV, art. 5º), é uma estrutura capaz de armazenar os dados pessoais de forma organizada. Essa estrutura pode ser física ou virtual, em um ou vários locais. Nesse sentido, Adalberto Simão Filho (2019, p. 172) afirma que:

> Banco de dados agrega assim, um conjunto estruturado de dados pessoais cuja proteção se assemelha aos demais direitos da personalidade, sendo formado e estruturado no âmbito de certos princípios e, por sua vez, contido em qualquer plataforma física ou digital única ou conjugada.

[12] DIAS, F. M. C. Multilingual Automated Text Anonymization. Tese de Doutorado, apresentada à Universidade Técnica de Lisboa, 2016, p.134

A Lei Geral de Proteção de Dados Pessoais assegura ainda, nos incisos V a IX, do artigo 5º, a definição de alguns tipos de pessoas que se relacionam ao processo de tratamento de dados, sendo elas:

> [...]
> V - Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX - Agentes de tratamento: o controlador e o operador;
> [...].

A titularidade dos dados pessoais é da pessoa natural à qual pertencem as informações objeto de tratamento. No que diz respeito aos agentes de tratamento (inciso IX, art. 5º), temos a figura do controlador mencionado no inciso VI, art. 5º, (órgão de decisão) conforme Cíntia Rosa Pereira de Lima (2020, p. 291):

> O controlador é a pessoa física ou jurídica, de direito público ou privado, a quem competem as decisões sobre o tratamento dos dados pessoais (art. 5º, inc. VI da LGPD). Portanto, o controlador irá determinar a finalidade e os motivos para o tratamento de dados pessoais.

A figura do controlador tem a responsabilidade sobre a finalidade e motivação do tratamento de dados, assegurando sempre aos titulares o acesso às suas informações, observado os segredos comerciais e industriais. Contudo, em caso de recusa por parte do controlador dos dados, conforme pontua Adalberto Simão Filho (2019, p. 178):

> Se houver recusa de oferecimento de informações por parte do controlador, baseado na observância do segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Já a figura do operador (inciso VII, art. 5º) possui relação de subordinação, pois enquanto o controlador é quem detém o poder decisório sobre as operações de

tratamento de dados, o operador é o responsável pela execução das rotinas de tratamento em nome do controlador. Dessa forma, depreende-se que o operador é:

> [...] a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5o, inc. VII da LGPD). Além das obrigações acima relacionadas para o controlador, o operador deve, também, realizar o tratamento conforme as instruções do controlador (art. 39 da LGPD). (LIMA, 2020, p.292)

Por sua vez, a figura do encarregado (inciso VIII, art. 5º) diz respeito à interação entre os atores, sendo a pessoa indicada pelo controlador que atua como "canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (art. 5º inciso VIII da LGPD).

Assim o encarregado possui algumas obrigações dentre elas:

> As principais obrigações do encarregado consoante a LGPD brasileira são: a) dever de sigilo ou de confidencialidade no exercício das suas funções; b) administrar as reclamações e comunicações dos titulares de dados pessoais, incluindo o dever de prestar esclarecimentos e adotar as providencias cabíveis; c) administrar as comunicações da ANPD; e d) orientar os funcionários do controlador quanto às melhores práticas para a proteção dos dados pessoais. (LIMA, 2020, p. 293):

Desta forma, sobre tratamento, é interessante trazer para reflexão a definição, contida no artigo 5º, inciso X, da LGPD:

> X - Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; [...]

Analisando o inciso retro mencionado, compreende-se que o rol apresentado é meramente exemplificativo, pois o tratamento se refere a qualquer operação realizada com dados pessoais, desde a coleta dos dados até a eventual destruição.

Na figura do consentimento apresentada no inciso XII do artigo 5º, é especificado que a "manifestação" deve ser "livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". Portanto, o consentimento não poderá ser para fins genéricos, sendo necessário a especificidade. Nesse sentido a:

> [...] manifestação específica, exige resposta específica e igualmente inequívoca com fundamento na dignidade da pessoa humana, na autonomia informativa, com particular relevo para a sua multidimensionalidade, e no livre desenvolvimento da personalidade. (SARLET, 2020, p.32)

Importante ressaltar que a figura do consentimento mencionada anteriormente, também se apresenta no inciso XVI do artigo 5º, onde a lei define o conceito de uso compartilhado de dados:

> XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, **com autorização específica**, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; (destacamos)

Com isso, a lei estabelece que há a necessidade de autorização específica para o compartilhamento de dados. A figura do consentimento é mais um requisito de legalidade. Conforme Cíntia Rosa Pereira de Lima e Lívia Froner Moreno Ramiro (2020, p. 273) afirmam:

> [...] A opção do legislador foi regular, ou seja, o compartilhamento de dados pessoais não é proibido, mas para tanto depende do consentimento específico do titular nos termos do art. 5º, inc. XVI que determina que uso compartilhado de dados é a "comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, **com autorização específica**, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados". (destaque nosso).

Além desse dispositivo, o § 5º do art. 7º da LGPD também exige o consentimento específico do titular dos dados pessoais para a finalidade que diga respeito ao compartilhamento de dados pessoais. O titular dos dados pessoais tem o direito de ser informado sobre o uso compartilhado de suas informações pessoais para que possa consentir ou não com tal prática pelo controlador do tratamento de dados pessoais.

A lei ainda nos apresenta, no inciso XVII, do artigo 5º, o sentido de relatório de impacto à proteção de dados pessoais, que é o documento a ser elaborado pelo controlador de dados:

> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> [...]

De acordo com a lei, esse relatório tem como objetivo avaliar os riscos para os direitos fundamentais dos titulares de dados pessoais decorrentes do tratamento de dados pessoais e identificar medidas para mitigar esses riscos.

Nesse sentido Adalberto Simão Filho (2019, p.190) em conformidade com a legislação pontua que:

> O relatório deverá conter, no mínimo a descrição dos tipos de dados coletados, metodologia utilizada para a coleta e para garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco.

Este relatório poderá ser objeto de solicitação da Autoridade Nacional de Proteção de Dados (ANPD), nos termos do artigo 10, § 3º, da LGPD. Caso seja o fundamento, o interesse legítimo ou conforme o artigo 38 da mesma lei, a ANPD poderá determinar, quando julgar necessário, que o controlador elabore este relatório, inclusive de dados sensíveis, resguardando os segredos comerciais e industriais.

A LGPD ainda nos apresenta, no inciso XVIII do artigo 5º, que uma das possibilidades legais de realizar o tratamento de dados é a realizada pelos órgãos de pesquisa, e a lei assim determina.:

> XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
> [...].

Portanto, são aos órgãos delimitados nessa definição que o tratamento é autorizado, para fins de desenvolvimento dos estudos a que se dedicam. Evidentemente,

o tratamento a ser feito sobre os dados deve relacionar-se com o objeto da pesquisa e com a área de estudo a que o órgão se dedica.

Quanto à Autoridade Nacional de Proteção de Dados (ANPD), apresentada no inciso XIX do artigo 5º da LGPD, trata-se de "autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal," responsável por cuidar, orientar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD, Art. 55-A).

Assim, a competência das atribuições da ANPD está fixada no artigo 55-J da LGPD, que lhe atribui um caráter regulatório, fiscalizatório e sancionatório. Uma de suas atribuições é "a fixação das diretrizes da política nacional de proteção de dados por meio de resolução de sua alçada, a partir de proposta do Conselho". (PFEIFFER, in LUCCA et al., 2019)

## 4.1. SITUAÇÕES LEGAIS PARA O TRATAMENTO DE DADOS

Enfim, após esse introito sobre os conceitos de tratamentos de dados pessoais contemplados na Lei Geral de Proteção de Dados Pessoais, importantes para elucidação do propósito desta dissertação, passaremos a analisar as situações legais que permitem o tratamento de dados pessoais, dados pessoais sensíveis, respectivamente objeto de tratamento das Instituições Particulares de Ensino Superior e, por último e não menos importante, os dados pessoais de crianças e adolescentes.

### 4.1.1. Tratamento de Dados Pessoais

Para que seja possível o tratamento de dados pessoais de forma legal, seja na fase de coleta, armazenamento, dentre outros tipos, é necessário observar os princípios já mencionados no capítulo 3, bem como os requisitos estabelecidos no rol do artigo 7º da Lei Geral de Proteção de Dados Pessoais.

A primeira situação a ensejar o tratamento de dados pessoais é a já mencionada via do consentimento, sendo esta palavra o comando geral que norteia a aplicabilidade da lei, pois, por meio do consentimento conferido pelo titular dos dados de forma manifestamente "livre, informada e inequívoca" (artigo 5º, inciso XII) "por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (artigo 8º).

Assim, não é admissível que o consentimento seja concedido de forma tácita, inviabilizando então o tratamento desses dados.

A lei ainda estabelece no artigo 8º § 1º que, em "caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais". Todavia, se não for o caso de escrito, caberá ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o texto legal. Nesse sentido:

> [...] o consentimento precisa ser, no mínimo (i) *livre*, ou seja, representa uma escolha real para o titular de dados, sem qualquer dos vícios de manifestação da vontade; (ii) *informado*, ou seja, obtido após a apresentação de informações claras, completas e objetivas para o titular a respeito das finalidades do tratamento, e (iii) *inequívoco*, ou seja, demonstrável por qualquer meio de prova lícita (e não apenas escrito). (LEONARDI, in LUCCA et al., 2019, p. 321):

Portanto, é proibido realizar qualquer tratamento de dados obtidos de forma viciada (vício de consentimento), exemplo, a obtenção de dados mediante dolo, na intenção de o controlador ludibriar o titular.

Observa-se então que só será considerado válido o consentimento se houver uma finalidade determinada e específica, não se admitindo utilizar termos genéricos para obtenção de acesso aos dados. Caso o controlador necessite compartilhar esses dados com outros controladores, será necessário a obtenção do consentimento do titular para essa finalidade especificamente. (LEONARDI, *in* LUCCA et al., 2019).

Se eventualmente ocorrer modificação na finalidade, inconciliável com a finalidade anterior sobre o tratamento dos dados, será necessário voltar-se ao titular dos dados para informá-lo sobre a mudança e a eventual obtenção ou não do consentimento.

Destaca-se que o titular possui o direito de revogar o consentimento a qualquer tempo, manifestando expressamente esse desejo, lhe sendo assegurados procedimentos gratuitos e facilitados para atingir esse objetivo. Todavia, as operações de tratamento realizadas anteriores à revogação permanecerão mantidas, salvo se o titular requisitar a eliminação dos dados pessoais.

Para os dados dos quais tenham se tornado inequivocamente públicos, é dispensada a autorização (consentimento) do titular, entretanto, tal dispensa não furta a responsabilidade do controlador em seguir em observância aos princípios do direito para realizar o tratamento desses dados.

Dentre as possibilidades que permitem realizar o tratamento de dados pessoais, o consentimento é apenas uma dessas, pois o controlador poderá, se for o caso, enquadrar o tratamento de dados em outra base legal. Entretanto, "se não houver outra base legal para enquadramento do tratamento de dados, o tratamento deverá ser interrompido imediatamente". (COTS; OLIVEIRA, 2019).

A segunda possibilidade considerada para o tratamento de dados pessoais é quando o controlador necessita cumprir obrigação legal ou regulatória.

Marcel Leonardi (2020, p. 323) aduz que:

> [...] ainda que o tratamento de dados pessoais baseado em obrigação legal ou regulatória não exija que leis ou regulamentos imponham diretamente uma atividade específica de tratamento, a finalidade do tratamento realizado nessa hipótese é justamente o cumprimento da obrigação legal ou regulatória prevista nessa norma, não podendo exceder essa finalidade.

Portanto, poderá haver o tratamento de dados pessoais nas situações que se exijam por causa da relação jurídica existente, seja por determinação legal ou regulatória. Sendo vedado ao titular impugnar o tratamento.

A exemplo, podemos utilizar o tratamento de dados pessoais dos funcionários, para assegurar as obrigações de e-Social, FGTS, INSS, operação de folha de registro, ou até mesmo dados de consumidores, para a emissão de nota fiscal. (COTS; OLIVEIRA, 2019).

A terceira possibilidade de tratamento de dados pessoais se dá pela administração pública, conforme o inciso III, do artigo 7º da LGPD. Tão somente poderá ser realizado se for "necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei".

É temerário a generalidade do termo "políticas públicas", pois é um termo utilizado em larga escala na sociedade para se referir a tudo que seja positivo de implementar na sociedade. Entretanto, as críticas a serem tecidas pelo uso dessa

terminologia se fundamentam pela possibilidade de permitir ao Estado invadir e violar os direitos dos indivíduos sob o pretexto de implemento de políticas públicas.

Conforme Augusto Tavares Rosa Marcacini (2020, p.150) comenta ao analisar o teor do inciso III:

> [...] impressiona como é amplo o seu sentido e o quão indefinidos são os seus limites. Diga-se que a expressão política pública parece ter-se tornado uma espécie de curinga para designar tudo aquilo que se supõe ser bom, belo e justo, olvidando o legislador, apenas para ficarmos no assunto central destes comentários, que o Estado é também parte do problema, e não necessariamente parte da solução. Não é demais lembrar que o extermínio de judeus, ciganos e outras categorias sociais consideradas indesejáveis foi política pública da Alemanha nazista, que com mortífera eficácia soube operar o tratamento de dados pessoais por meio da tecnologia disponível ao seu tempo: cartões perfurados.

Já na quarta situação que possibilita o tratamento de dados pessoais, destina-se a realizar estudos por órgãos de pesquisa. Assim, conforme já demonstrado há pouco ao retratar a possibilidade de tratamento contida no inciso XVIII, do artigo 5º, órgãos de pesquisa podem ser entes da administração pública direta ou indireta, ou ainda pessoas jurídicas de direito privado que não tenham como finalidade auferir lucro, a exemplo de associações ou fundações, possuindo sede e foro em território nacional.

Somente os órgãos dentro dessa limitação do artigo 5º, inciso XVIII, possuem autorização para o tratamento de dados dentro dos limites do desenvolvimento de suas atividades. Não obstante esta disposição do inciso XVIII, é preciso ainda respeitar os princípios da LGPD, em especial o da finalidade.

Ainda temos a quinta possibilidade de tratamento, que se destina para “a execução de contrato ou de procedimentos preliminares à sua constituição, a pedido do titular”. Insta salientar que esta operação deve ser realizada na fase de execução do contrato, todavia, a requerimento do titular é possível realizar o tratamento na fase pré-contratual, conforme exemplifica Marcel Leonardi (2019, p. 325):

> Imagine-se, por exemplo, o titular de dados pessoais que adquire um pacote turístico em um *website* de agência de turismo. Para poder executar os serviços contratados, essa agência de turismo precisará compartilhar os dados pessoais do titular com a companhia aérea, o hotel e eventuais prestadores de serviço complementares e, poderá utilizar como base legal de tratamento a execução de contrato.

Adentrando na sexta possibilidade, temos o "exercício regular de direitos em processo judicial, administrativo ou arbitral." Assim, a previsão contida no inciso VI da LGPD não é clara em dizer de quem seja esse direito, todavia, conjectura-se que esses direitos se refiram ao controlador, para que em eventual disputa jurídica entre controlador e titular, possam ser utilizados desse tratamento para assegurar direitos do controlador "exigíveis do titular dos dados, ou que informem ou comprovem o cumprimento das obrigações do controlador, ou simplesmente gerenciem os documentos que demonstrem os direitos e as obrigações entre as partes [...]" (MARCACINI, 2020, p. 152).

A próxima possibilidade, sendo a sétima aqui apresentada, ocorre com o tratamento "da vida ou da incolumidade física do titular ou de terceiros." Destaca-se a importância da vida, bem juridicamente tutelado pelo direito brasileiro, assim, qualquer ameaça a esse bem jurídico ou integridade física do titular ou de terceiros, permite-se extraordinariamente o tratamento de dados pessoais, nesses casos.

A oitava possibilidade de tratamento é o realizado exclusivamente em procedimentos efetuados por profissionais da área da saúde ou serviços de saúde e autoridade sanitária. Este comando se desdobra da anterior, pois aqui também tem questões que envolvem o risco de dado ao bem jurídico; "vida". Igualmente, o tratamento se dá de forma restritiva, conforme estabelecida pela lei.

Essa "tutela da saúde" é outro texto subjetivo presente no comando legal, pois a saúde em si, não pode ser sujeito de direito, sendo necessário dizer quem é o sujeito de direito tutelado pela proteção de dados. (MARCACINI, 2020, p. 152-153).

A penúltima possibilidade, sendo então a nona prevista no texto legal, é destinada a atender o legítimo interesse do controlador ou de terceiros. A despeito de o comando legal garantir o legítimo interesse do controlador, isto não é absoluto, pois os direitos e liberdades fundamentais dos titulares prevalecem, exigindo assim, a proteção dos dados pessoais.

Assim, "o tratamento de dados pessoais com base no legítimo interesse é, normalmente, a base legal mais flexível entre as dez disponíveis, já que não está atrelado a uma finalidade específica" (LEONARDI, 2019, p. 324).

Quando ocorrer o tratamento de dados fundamentado no legítimo interesse, deverá ser elaborado relatórios de impacto à proteção de dados, que estarão sujeitos à revisão e possíveis discordâncias da ANPD.

Por fim, chegamos à última possibilidade de tratamento de dados pessoais, a décima contida no artigo 7º da referida Lei Geral de Proteção de Dados Pessoais. Assim, temos a figura da "proteção do crédito".

Inovação da legislação brasileira, pois o crédito financeiro é uma ferramenta importantíssima para a economia, pois, por meio dele, é possível a movimentação de recursos no mercado brasileiro e viabiliza o desenvolvimento pessoal e empresarial, permitindo a injeção de recursos financeiros na economia local.

Marcel Leonardi (2020, p. 330) entende que a interpretação do conceito de proteção do crédito deve ser feita "extensivamente", permitindo assim o tratamento tanto para a concessão de crédito quanto para atividades de apoio, como produtos e serviços.

Destaca-se que o artigo 43 do CDC expressamente autoriza a criação de base de dados pelo serviço de proteção ao crédito, tendo em vista que a atividade de crédito é uma atividade de risco em função da "inadimplência e degradação de crédito (reclassificação para pior do nível de risco) e risco de degradação de garantias (o bem que garante o crédito deixa de existir ou perde valor)." (COTS; OLIVEIRA, 2021).

Diante dessas dez possibilidades apresentadas pelo artigo 7º da LGPD e até aqui sinteticamente explicadas, temos um vislumbre sobre as hipóteses que são permitidas, conforme a LGPD, de realizar o tratamento de dados pessoais. Todavia, deve-se sempre observar os princípios sobre a proteção de dados e os princípios gerais do direito, pois, em razão dos constantes avanços tecnológicos e da própria legislação, novas situações podem surgir.

É importante escolher a possibilidade de tratamento ou base legal de tratamento, observando as vantagens e desvantagens de cada uma. Não é uma tarefa fácil decidir corretamente. Todavia, o controlador deverá ponderar cautelosamente, conforme a sua atividade e a finalidade para a qual se destinará o tratamento dos dados.

### 4.1.2. Dados Pessoais Sensíveis

Neste tópico, abordaremos, em especial, sobre os dados pessoais sensíveis, que detêm uma atenção especial da legislação, pois o tratamento desses dados pode dar origem à discriminação ao titular dos dados, sendo uma real possibilidade de lesão

ou ameaça às liberdades individuais. De acordo com o entendimento sintetizado por Patrícia Peck Pinheiro (2021, p. 35):

> Os dados sensíveis merecem tratamento especial porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa.

A evolução tecnológica tornou o esquecimento mais difícil, expandindo assim a capacidade de memória da humanidade, pois guarda registros de localização, destinos e caminhos utilizados, dados de saúde e condição clínica, preferências sexuais, etnias, raça ou gênero e identidade de gênero, relacionamentos, preferências de consumo e peculiaridades dos indivíduos. Isto posto, denota-se que a sociedade em rede não permite o "esquecimento e, quiçá, o fim do próprio perdão" (TEPEDINO; TERRA; GUEDES, 2022, p. 270).

A possibilidade legal para a realização do tratamento de dados pessoais sensíveis está contida na LGPD, em seu artigo 11. Assim, nos é apresentado um rol, que tem sido discutido, pois conforme pontua Carlos Nelson Konder (2019, p. 263), "[...] é inviável conceber rol taxativo de dados sensíveis, já que eles são definidos pelos efeitos potencialmente lesivos do seu tratamento."

Reconhecendo essa fragilidade, o legislador, no parágrafo 1º do artigo 11, determina que o referido artigo pode ser aplicado a qualquer tratamento de dados pessoais que venham a revelar dados sensíveis.

Assim, é possível perceber no texto da lei que o legislador, na tentativa de assegurar maior proteção aos dados, estabeleceu possibilidades comuns que permitem o tratamento de dados pessoais e de dados pessoais sensíveis, como, por exemplo, o consentimento do titular (I), o cumprimento de obrigação legal ou regulatória pelo controlador (II, a), o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (II, b), a realização de estudos por órgãos de pesquisa (II, c), o exercício regular de direitos, inclusive em contratos e em processo judicial, administrativo e arbitral (II, d), a proteção da vida ou da integridade física do titular ou de terceiros (II, e), e a tutela da saúde, exclusivamente, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária (II, f).

Outras regras distintas são observadas na legislação, a exemplo disso, a questão do consentimento. Na Lei Geral de Proteção de Dados Pessoais, o artigo 7º, inciso I, diz que o tratamento pode ser realizado mediante o consentimento do titular.

Para que o tratamento de dados pessoais sensíveis seja realizado, é necessário que o consentimento seja de forma destacada e específica, para fins específicos. Assim, há uma restrição formal em relação ao consentimento.

A possibilidade de tratamento de dados pessoais sensíveis sem consentimento fica afastada quando é necessário para a execução de um contrato ou procedimentos preliminares relacionados a um contrato em que o titular seja parte, a pedido do titular dos dados, para atender a interesses legítimos do controlador ou terceiros ou para proteção do crédito. Estas situações são encontradas nos incisos V, IX e X do artigo 7º da LGPD.

Não há repetição destas possibilidades de tratamento no artigo 11 da LGPD, o que indica que as relações patrimoniais mencionadas nestes incisos não justificam os riscos envolvidos no tratamento de dados pessoais sensíveis do titular (KONDER, 2019).

A LGPD permite o tratamento de dados pessoais sensíveis sem o consentimento do titular apenas para garantir a prevenção à fraude e à segurança do titular em processos de identificação e autenticação de cadastro em sistemas eletrônicos, desde que não prevaleçam direitos e liberdades fundamentais do titular (art. 11, inciso II, alínea g).

De acordo com o artigo 11, § 2º, deverá haver publicidade sobre a dispensa de consentimento caso o tratamento seja realizado para cumprimento de obrigação legal ou regulatória pelo controlador ou para execução de políticas públicas pela administração pública.

O artigo 23, inciso I, complementa a lei, exigindo que as informações sobre a previsão legal, finalidade, procedimentos e práticas utilizadas para a execução dessas atividades sejam fornecidas de forma clara e atualizada, em veículos de fácil acesso, preferencialmente em seus sites eletrônicos.

A Lei, ao se referir ao tratamento de dados pessoais sensíveis relacionados à saúde com a finalidade de obtenção de lucro pelo controlador, aplica regras mais restritivas, sendo vedado o compartilhamento desses dados, exceto quando consentido pelo titular em caso de portabilidade ou para a prestação de serviços de saúde por operadoras, planos de saúde e assistência farmacêutica (art. 11, § 4º). A vedação ao

tratamento de dados sensíveis de saúde, prevista na lei, consiste em impedir que os planos integrantes da saúde suplementar promovam a "seleção de riscos na contratação" dos planos ou até mesmo promovam a "exclusão de descritos" vinculados (art. 11, § 5º).

Para fins de estudos direcionados à saúde pública, a LGPD permite que seja realizado o tratamento, desde que observada a finalidade específica a que se destina e que o responsável pelo tratamento desses dados seja unicamente o órgão de pesquisa, proibindo então que esses dados sejam transferidos a terceiros, efetivando assim a proteção dos dados a serem tratados.

Compreende-se que é necessário maior rigor na abordagem quanto ao tratamento de dados pessoais sensíveis, pois eles podem dar origem a violações de direitos individuais e discriminação, sendo importantíssimo a tutela desses direitos pela LGPD. No entanto, ainda é necessário aprofundar os debates sobre o tema para aprimorar a legislação.

### 4.1.3. Tratamento de Dados Pessoais de Crianças e Adolescentes

A despeito da Instituição de Ensino Superior (IES) não tratar dados de crianças, eventualmente ocorrerá o tratamento de dados pessoais de adolescentes, na concepção da lei. O legislador entendeu haver uma posição de vulnerabilidade, ao realizar o tratamento de dados de crianças e adolescentes, determinando, assim, um regulamento específico a respeito do tratamento desses dados.

Para melhor elucidação, trazemos o conceito estabelecido pelo Estatuto da Criança e do Adolescente, no artigo 2º, que conceitua criança e adolescente. Em termos legais, criança é pessoa com até doze anos de idade incompletos e adolescente é pessoa entre doze e dezoito anos.

A nova legislação brasileira de proteção de dados pessoais, ou qualquer outra que trate do tema, não poderia olvidar ou ignorar a abordagem deste assunto, pois esses indivíduos, cada vez mais precoces, possuem acesso a diversas tecnologias que eventualmente coletam seus dados, sendo necessário efetivar a proteção desses dados, seja no meio físico ou virtual. (AMARAL; PRADO, 2020, p. 164-165).

A LGPD, seguindo o modelo europeu, buscou assegurar a proteção aos dados pessoais desses indivíduos de forma mais especial, a fim de que o tratamento de dados pessoais de crianças e adolescentes seja realizado observando o melhor interesse dessas crianças e adolescentes.

O artigo 14 da seção III do capítulo II da LGPD aborda questões sobre o tratamento de dados pessoais desses indivíduos, mas a lei não menciona ou define explicitamente o princípio fundamental do direito da criança e do adolescente, que é o princípio da proteção integral.

Cláudio do Prado Amaral (2020, p. 166) pontua que "o princípio do melhor interesse decorre do princípio da proteção integral e só pode ser adequadamente interpretado à sua luz". Para atender o "melhor interesse" dessas crianças e adolescentes, ou seja, aquele que não causa danos ou prejuízos e decorre do princípio da proteção integral, a lei assegura o tratamento de dados pessoais dessas crianças e adolescentes que traga "benefícios", dos quais "a ausência de tratamento não poderia ou teria dificuldades de trazer" (COTS; OLIVEIRA, 2021).

A figura do consentimento, de forma específica, se apresenta apenas para o tratamento a ser realizado nos casos de crianças, que requerem o "consentimento específico e destacado dado por pelo menos um dos pais ou pelo responsável legal" (LGPD, art. 14, § 1º). Já na obtenção do consentimento para o tratamento dos dados pessoais dos adolescentes, ocorre da mesma forma que o tratamento de dados pessoais de adultos.

A obtenção do consentimento específico para o tratamento de dados pessoais de crianças se diferencia do consentimento inequívoco aplicado aos adolescentes e a outras pessoas, pois este último não precisa ser expresso de forma positiva pelo titular dos dados, possibilitando o consentimento tácito, observado no contexto da operação.

Já o consentimento específico é a expressão positiva da vontade do titular dos dados pessoais, relacionada ao tratamento de seus dados pessoais, e deve ser "destacado e dado por pelo menos um dos pais ou pelo responsável legal" (LGPD, artigo 14, § 1º).

Outro ponto relevante em relação ao tratamento de dados pessoais de crianças é que o controlador deverá manter a transparência sobre o tipo de dado coletado, a forma de utilização e os procedimentos para o exercício dos direitos dos

titulares. As informações devem ser transmitidas de forma clara e simples, garantindo a acessibilidade aos pais, incluindo recursos audiovisuais se necessário.

A lei prevê ainda a possibilidade de tratar os dados de crianças sem o consentimento dos pais, excepcionalmente para entrar em contato com os genitores ou responsáveis legais, mas essa possibilidade é limitada a uma única vez, sem armazenamento dos dados e proibindo a transferência a terceiros, para garantir a proteção da criança.

Nota-se que crianças dessa geração precoces entram em contato com tecnologias de jogos ou plataformas de redes sociais. Neste sentido, a lei garante que o fornecimento de informações pessoais não deve ser condicionado, exceto as estritamente necessárias, para que os titulares menores possam acessar aplicativos, jogos, entre outros.

É dever, de acordo com a lei, que o controlador promova o esforço necessário, empregando tecnologias disponíveis e formas, para garantir que houve o consentimento pelo responsável pela criança. Deste modo, aplicativos têm utilizado, juntamente à certificação do consentimento, a solução de cálculo matemático de grau de dificuldade superior à idade do participante para obter maior assertividade de se tratar de um adulto que deu o consentimento. (TEIXEIRA, 2019).

Caso ocorra conflito entre os genitores ou responsáveis legais em relação ao consentimento, qualquer um deles pode recorrer ao judiciário para solucionar o conflito, pois a lei dispõe que o consentimento deve ser dado por pelo menos um dos genitores, o que pode causar divergência.

Importa destacar que, na elaboração da LGPD, o legislador buscou construir uma proteção que pode se mostrar eventualmente ineficiente em alguns aspectos, o que só a aplicação da lei determinará. Caberá aos juristas e operadores do direito atentos a todo o sistema de proteção da infanto-juventude em paralelo à LGPD apontar pontos de inflexão ou melhorias para a legislação brasileira de proteção de dados pessoais.

## 4.2. TÉRMINO DO TRATAMENTO DE DADOS PESSOAIS

O Marco Civil da Internet (Lei 12.965/2018), no seu artigo 7º, inciso X, assegura o direito à exclusão dos dados pessoais do usuário na internet. Esta disposição tem como objetivo garantir a autodeterminação informativa, ou seja, permitir que o titular dos dados possa ter seus dados apagados definitivamente quando a relação entre as partes findar.

A Lei Geral de Proteção de Dados (LGPD) traz no seu artigo 15 hipóteses que demonstram o término do tratamento de dados pessoais. Essas possibilidades não configuram uma lista taxativa, mas servem como exemplos. A lei apresenta cinco hipóteses para o término do tratamento de dados pessoais: (I) pelo exaurimento da finalidade do tratamento dos dados; (II) ao findar o prazo estabelecido para o tratamento; (III) pelo exercício da autodeterminação do titular; e (IV) por ilegalidade no tratamento.

A primeira e segunda hipóteses se relacionam com a autodeterminação informativa, na qual a finalidade e o tempo são estabelecidos como limites. A primeira hipótese, em especial, decorre do princípio da finalidade, pois verifica-se se a finalidade para a qual o tratamento de dados foi destinado foi atingida.

Assim, é necessário encerrar a operação, pois, após alcançar a finalidade, não há justificativa para continuar o tratamento dos dados pessoais. Por exemplo, o tratamento de dados para aquisição de passagens aéreas exaurirá com a finalização do transporte aéreo, permitindo que o titular autorize o armazenamento dos dados para futuras aquisições de passagens.

A segunda hipótese ocorre quando o período estabelecido para o tratamento de dados finda, pois a operação está sujeita a um lapso temporal. Ao findar esse período, o tratamento também terminará.

A terceira hipótese se relaciona com o princípio do consentimento, que decorre da vontade íntima do titular, que pode comunicar sua vontade e, assim, exercitar seu direito de revogar o consentimento. No entanto, caso esse direito seja exercido, o interesse público ficará protegido.

Por fim, a quarta hipótese, referida na lei, ocorrerá por determinação da Autoridade Nacional de Proteção de Dados, quando houver alguma transgressão à

LGPD. Ressalta-se que, especificamente nesta situação, somente serão eliminados os dados tratados de forma irregular. (COTS; OLIVEIRA, 2021).

Resumidamente, o tratamento de dados pessoais deverá ser encerrado com o término da operação de tratamento dos dados, com o esgotamento do prazo estipulado para o tratamento, com o exercício da autodeterminação ou com a violação às disposições da Lei Geral de Proteção de Dados Pessoais. Assim, após o término do tratamento, os dados pessoais deverão ser eliminados, conforme o estabelecido no artigo 16 da LGPD.

## 4.3. DIREITOS DO TITULAR

Aqui, buscamos destacar os direitos mais relevantes ao presente estudo, principalmente porque muitos pontos da Lei Geral de Proteção de Dados Pessoais podem ser alterados pela Autoridade Nacional de Proteção de Dados em função da necessidade de regulamentação, entretanto, sua aplicação ainda é imediata.

Sendo assim, iniciamos este título com o artigo 9º da LGPD, que dispõe sobre a facilitação do acesso dos titulares dos dados às informações de tratamento. Estas informações devem ser "disponibilizadas de forma clara, adequada e ostensiva", incluindo outras características, como é possível observar nas disposições abaixo:

> [...]
> I - Finalidade específica do tratamento;
> II - Forma e duração do tratamento, observados os segredos comercial e industrial;
> III - Identificação do controlador;
> IV - Informações de contato do controlador;
> V - Informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - Responsabilidades dos agentes que realizarão o tratamento; e
> VII - Direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

O artigo 18 da LGPD aduz que o titular dos dados goza do direito de obter acesso aos dados e receber, a qualquer momento, a confirmação do controlador sobre a existência de operação de tratamento de seus dados pessoais, bastando apenas requisitá-la. Assim, o controlador deverá disponibilizar essa informação em até 15 dias, contados a partir da data do requerimento (artigo 19, inciso II da LGPD).

A requisição dever ser facilitada, conforme prevê o artigo 19, inciso I da LGPD, e deve estar disponível tanto em ambientes virtuais quanto físicos. Cintia Rosa e Livia Froner (2020, p. 257) complementam que "o acesso facilitado previsto neste artigo deve nortear a concretização de todos os demais direitos garantidos na LGPD, bem como o direito de acesso aos dados".

A lei também permite ao titular requerer a correção de seus dados caso ele constate alguma incongruência. Nesse caso, a correção deverá ser realizada imediatamente, mas não há um prazo especificado para que seja feita pelo controlador.

Além disso, o titular tem o direito à portabilidade de seus dados para outro fornecedor de produto ou serviço, como outra instituição de ensino superior, mediante requisição expressa.

No entanto, a lei não especifica o formato dos dados, cabendo à regulamentação posterior pela ANPD garantir que os dados possam ser efetivamente transferidos para outro controlador, preferencialmente em um formato legível por máquinas ou por outros sistemas.

Cintia Rosa e Livia Froner (2020, p. 272) destacam que "seria importante e muito útil que tal portabilidade se operasse diretamente entre os agentes de tratamento de dados, dada a vulnerabilidade informacional do usuário que, muitas vezes, não saberia realizar tal procedimento".

De outro modo, a Lei Geral de Proteção de Dados (LGPD) no artigo 18, inciso VI, assegura o direito à eliminação dos dados pessoais. Como já mencionamos, a regra é a eliminação dos dados ao término do tratamento. Entretanto, se não ocorrer, é assegurado ao titular a possibilidade de requerer que o controlador proceda com a eliminação dos dados de sua base.

Existem algumas ressalvas, como quando é necessário manter os dados por determinação legal ou regulatória (LGPD art. 16, inciso I), para fins de estudo por instituto de pesquisa (desde que sempre que possível sejam anonimizados; LGPD art. 16, inciso II), para transferência para terceiros nos termos e limites da lei (LGPD art. 16, inciso III), ou para uso exclusivo do controlador, desde que anonimizado e sem acesso a terceiros (LGPD art. 16, inciso IV).

Por fim, a referida legislação reconhece a irrenunciabilidade sobre a titularidade dos dados pessoais (LGPD art. 17). Desta forma, não é admissível a realização de negócio jurídico com a transferência ou cessão de dados pessoais ou a

limitação do exercício da titularidade. A lei determina que "toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade" (COTS; OLIVEIRA, 2021).

# 5. *COMPLIANCE* DE DADOS PESSOAIS

No presente capítulo, iremos abordar o assunto de *compliance* para proteção de dados pessoais. Preliminarmente, trataremos da definição de *compliance* e dos requisitos eficazes dos programas de *compliance*, bem como da atuação junto à Lei Geral de Proteção de Dados Pessoais, juntamente com as boas práticas de governança.

Preliminarmente, trataremos do conceito de *compliance* e dos requisitos mínimos para atingir a conformidade. Observa-se que a expressão "*compliance*" tem estado em grande evidência, principalmente nas notícias governamentais e empresariais, devido aos incontáveis escândalos de corrupção no Brasil e no mundo, e ao esforço em reduzir a corrupção nos sistemas políticos e econômicos.

Ela tem origem do inglês "*to comply*", que significa agir de acordo com a lei, e, portanto, *compliance* é estar em conformidade com a lei. Resumidamente, é "estar em conformidade com as regras internas da empresa, de acordo com procedimentos éticos e normas jurídicas vigentes" (CARVALHO; BERTOCCELLI; ALVIM, 2021).

Ao se referir à conformidade, podemos compreender que a sua consecução não se limita à observação da lei, mas é necessário implementar um conjunto de táticas e medidas direcionadas à organização e seus membros, com o objetivo de cumprir normas legais e regulamentares, pautadas pela ética e pela adoção de políticas e diretrizes procedimentais (ARTESE, 2021).

Para atingir a conformidade em uma Instituição de Ensino Superior (IES), é necessário conhecer as rotinas e procedimentos internos, analisando-os em paralelo com a legislação a ser observada em cada fase dos processos. É preciso, então, estabelecer uma estrutura de políticas corporativas e procedimentos que representem ações para concretizar os preceitos normativos, minimizando o risco de cometer atos ilícitos e identificando os possíveis responsáveis, aplicando as medidas sancionatórias necessárias, proporcionando o retorno à normalidade legal de imediato.

A adoção de instrumentos de governança corporativa, como os programas de *compliance* ou programas de conformidade, aplicados à proteção de dados, visa promover a harmonia entre os atores envolvidos no tratamento de dados (SIMÃO FILHO, 2020, p. 329).

A implementação de programas de *compliance* possibilita a gestão de risco de forma satisfatória, viabilizando a identificação de eventuais violações e os possíveis danos resultantes. A adoção de políticas de *compliance* serve como atenuante em eventuais sanções administrativas, pois estimula o estabelecimento de uma cultura corporativa de respeito às normas jurídicas, minimizando as possibilidades de violação.

Para que um programa de governança alcance seus objetivos, é necessário que ele contenha requisitos mínimos. Programas de fachada, sem efeitos reais na estimulação da consciência corporativa e minimização das transgressões, ou que não preencham os requisitos mínimos, podem resultar em penalidades maiores. (FRAZÃO; OLIVA; ABILIO, 2019)

A conformidade com a Lei Geral de Proteção de Dados (LGPD) é uma obrigação para as instituições privadas de ensino superior, visando garantir a proteção dos dados pessoais.

Uma forma de garantir a conformidade é estabelecer um programa de *compliance* ou conformidade de dados pessoais, que inclua a identificação e avaliação de riscos relacionados à privacidade de dados, a implementação de medidas de segurança e auditorias regulares para garantir o cumprimento das exigências da LGPD, além de desenvolver uma equipe dedicada e capacitar os funcionários para lidar com questões relacionadas à privacidade de dados.

De acordo com a Associação Brasileira de Mantenedoras de Ensino Superior (ABMES):

> "as instituições de ensino superior devem desenvolver programas de conformidade para garantir que os procedimentos de tratamento de dados pessoais sejam realizados de maneira adequada, levando em conta os princípios da privacidade e segurança da informação."

É importante que as instituições privadas de ensino superior tenham uma equipe dedicada a lidar com questões relacionadas à privacidade de dados e que os funcionários sejam capacitados para lidar com essas questões. Isso inclui a designação de um encarregado de proteção de dados (DPO), que será responsável por garantir a conformidade com a LGPD e lidar com qualquer questão relacionada à privacidade de dados.

## 5.1. REQUISITOS DOS PROGRAMAS DE *COMPLIANCE*

Noutro aspecto, temos a necessidade de pontuar alguns dos requisitos básicos necessários para a eficácia dos programas de *compliance*. A intenção aqui é apresentá-los para que seja compreendida melhor a proposta de adequação da Instituição de Ensino Superior (IES).

É importante destacar que um dos pontos para a efetividade dos programas de *compliance* em qualquer organização é a dependência fundamentalmente do comprometimento da alta direção para assegurar os meios necessários para o desenvolvimento do programa, seja através de treinamentos, divulgação e monitoramento do andamento do programa (CARVALHO; ABREU; TAKAKI, 2021).

A alta direção poderá adotar comunicação periódica para apresentar o programa de *compliance* e utilizar reuniões para externalizar a necessidade de que toda a equipe esteja engajada, entre outras possibilidades.

Outro dos requisitos mínimos consiste na "avaliação contínua de riscos e atualização do programa" de *compliance*. Resumidamente, esta consiste em avaliar os riscos no desenvolvimento da atividade, identificar pontos de melhoria e adequar o programa para torná-lo mais assertivo, evitando a transgressão de normas, com base na análise do risco (FRAZÃO; OLIVA; ABILIO, 2019).

A promoção de uma detalhada análise de riscos possibilita ao programa de *compliance* uma adequação personalizada, considerando a avaliação de riscos e atualização do programa uma das mais importantes partes do programa.

Após a identificação dos riscos, temos o segundo elemento, a "elaboração de código de ética e conduta". Este documento se fundamenta em traduzir os valores e princípios da instituição, apontando as condutas a serem adotadas no ambiente corporativo. O código de ética e conduta deve ser aplicado a todos os atores da instituição e deve ser um documento escrito e de linguagem acessível (FRAZÃO; OLIVA; ABILIO, 2019).

Além da criação do código de ética e conduta, é fundamental criar os procedimentos de controles internos em conjunto com a análise dos riscos, facilitando a mitigação de diversos problemas com a análise periódica do controle interno.

É necessário assegurar a autonomia e independência dos procedimentos de controle interno, com capacidade de executar e supervisionar as normas estabelecidas no programa de conformidade. Incentivados pela alta direção, os treinamentos periódicos aos colaboradores possibilitam maior entendimento da implantação de normas aplicáveis ou esclarecimento de questionamentos sobre o tema. Portanto, os treinamentos devem ter o propósito de esclarecer a cada setor as particularidades do risco atribuído a ele.

Os treinamentos sobre *compliance* devem ser constantes, tanto para garantir a transmissão de adaptações e alterações no programa, como para reiterar suas premissas e contribuir para minimizar o risco de esquecimentos e incompreensões pelo funcionário. (FRAZÃO; OLIVA; ABILIO, 2019).

Destacamos que, após a análise dos riscos e a implementação de medidas para mitigação, é factível que não se atinjam todos os objetivos da instituição, pois é necessário estabelecer a cultura corporativa de agir com respeito à ética e às leis.

Logo, temos a necessidade de monitoramento das ações implementadas para verificar se os colaboradores ou a alta direção estão cumprindo o propósito estabelecido no programa de conformidade. Portanto, faz-se necessário o monitoramento contínuo dos procedimentos e a atualização do programa, se necessário. (CARVALHO; ABREU; TAKAKI, 2019).

Então, esse monitoramento deve verificar se estão ocorrendo respostas adequadas às transgressões da lei ou às áreas que necessitam de intervenção por inobservância da cultura corporativa. Nesse sentido, é necessário observar e analisar as relações com os parceiros comerciais quanto à adoção de medidas que assegurem o efetivo funcionamento do programa de *compliance*.

A palavra de ordem no *compliance* é resultado. É necessário observância permanente dos resultados para promover a adequação necessária do programa, pois "o emprego dos resultados dessa vigilância na constante atualização e aprimoramento do programa de *compliance* indica o compromisso da pessoa jurídica com o cumprimento da lei - quanto mais ágil a mudança, maior o comprometimento" (FRAZÃO; OLIVA; ABILIO, 2019, p. 373).

Outro ponto importante a destacar são os canais de comunicação, que possibilitam o esclarecimento de dúvidas dos colaboradores em relação à postura desejada pela organização. Além disso, esses canais podem servir para o recebimento

de denúncias, sendo um meio seguro para o colaborador sem prejudicá-lo, já que está abarcado pelo sigilo.

A adoção de canais de comunicação contribui para a prevenção de atos ilícitos e difunde o comportamento de conformidade. Além disso, proporciona uma maior percepção da gestão sobre o que ocorre, possibilitando agir para coibir ou corrigir novas condutas.

O canal de comunicação, ao ser utilizado, deve imediatamente iniciar os procedimentos necessários para apurar o fato. Se for constatado que é infundado, arquiva-se, mas se verificada a ocorrência de infrações, encaminha-se para o responsável por aplicar as medidas sanções necessárias, garantindo a credibilidade dos canais e estimulando o uso constante deste meio, que é uma ferramenta poderosa na consecução do programa de *compliance*.

A detecção e apuração de condutas contra o programa de *compliance* é outro ponto importante para assegurar o sucesso efetivo do programa. Deve-se investigar e reprimir condutas antagônicas ao programa de conformidade. Portanto, ao identificar tal prática, a instituição deve agir rapidamente em relação ao agente perturbador para garantir a adequação às normas ou promover a aplicação da penalidade cabível, reafirmando o compromisso com o fiel cumprimento das normas.

Salientamos que é fundamental adotar um tratamento igualitário a todos os colaboradores, pois isso mantém uma postura reconhecidamente séria e viabiliza a credibilidade da instituição na adoção do programa de *compliance*, difundindo a ideia entre os colaboradores de que a instituição segue a legalidade, utilizando meios de investigação e julgamento justos.

## 5.2. *COMPLIANCE* E A LGPD

Como já demonstramos o conceito de *compliance* e os requisitos dos programas de *compliance*, será realizado aqui uma breve análise do programa de conformidade na perspectiva da Lei Geral de Proteção de Dados (LGPD) e as responsabilidades e penalidades administrativas tratadas pela lei brasileira de proteção de dados pessoais.

O *compliance* de dados pessoais não está limitado ao contato com consumidores, mas está direcionado a várias esferas da atividade empresarial, assumindo então uma transversalidade e revisando os padrões de conduta para uma adequada execução das normas.

Remetendo-se, então, à relação de tratamento de dados dos estudantes pela secretaria da Instituição de Ensino Superior (IES), as regras de conformidade devem ser adotadas nesse setor para atender os desígnios da LGPD, mitigando, por exemplo, a coleta de dados que não sejam necessários ou que possam revelar-se discriminatórios.

### 5.2.1. Da Política de Boas Práticas e de Governança

A LGPD preceitua, no artigo 50, que os controladores e operadores, dentro dos limites de suas atribuições, podem formular regras destinadas a boas práticas e 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. [...]

Estas regras, elaboradas pelos agentes que realizam o tratamento de dados pessoais, devem levar em conta elementos como a natureza, escopo, finalidade, probabilidade e gravidade dos riscos e benefícios decorrentes do tratamento de dados do titular.

O inciso I do artigo 50 da LGPD determina que os programas de governança em privacidade, ao serem implementados, devem conter requisitos mínimos:

> (...)
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

É importante identificar se o tratamento dos dados pessoais é realizado pelo operador ou controlador, pois a LGPD atribui maior responsabilidade e deveres ao controlador. A lei distribui as regras corporativas em "regras de boas práticas e governança" (LGPD, artigo 50) e "programa de governança em privacidade" (LGPD, artigo 50, § 2º), destinadas, principalmente, aos controladores.

Portanto, ocupa-se o primeiro com "os aspectos operacionais do processo de tratamento de dados", ou seja, possui caráter instrumental para executar ou definir padrões técnicos e estruturas em que o sistema irá agir. Já o segundo demonstra características mais amplas, como a estruturação de normas de governança corporativa, abordando aspectos relacionados à tutela dos direitos dos titulares de dados. Todavia, em qualquer dos casos, a gestão do risco é o ponto fundamental (FRAZÃO; OLIVA, ABILIO; 2019).

A adoção de um programa de governança em privacidade forma um agrupamento de normas e regras de boas práticas e governança que podem ser observadas pelos agentes que realizam o tratamento de dados pessoais. Além disso, proporciona a aproximação das políticas de segurança da informação para o cumprimento de preceitos legais.

Programas de *compliance*, conforme as regras de boas práticas, para serem considerados bons, devem se basear em conhecer e reavaliar os riscos, promover medidas adequadas para responder a eventuais violações e servir ainda de subsídio para a alta direção na melhor gestão da instituição.

Para que seja possível construir um programa eficiente de *compliance*, é necessário conhecer todos os processos executados pela instituição, bem como seus fluxos de dados, quais dados são tratados e com quais finalidades. Dessa forma, é necessário realizar o mapeamento de dados, desde a coleta até o armazenamento ou descarte.

Logo, deve-se preocupar em analisar quais dados são coletados, a forma de coleta, os instrumentos que asseguram a precisão da coleta e a finalidade do tratamento, o responsável pela coleta, a relação da necessidade desses dados com a atividade da instituição e o que acontece com esses dados após estarem em posse da instituição.

Posteriormente, à identificação dos riscos, é necessário elaborar a documentação corporativa (normas internas, boas práticas e códigos de ética) para especificar os mecanismos utilizados na instituição para a coleta e tratamento de dados pessoais. Essa documentação deve conter instruções claras para guiar os colaboradores e a alta direção na condução das operações com dados pessoais.

Além disso, a documentação deve abordar sobre quais dados podem ser manipulados, em quais situações de tratamento e para qual finalidade se destinam, bem como o período autorizado para realizar esse tratamento e o armazenamento ou eliminação dos dados.

É importante destacar que, se possível, é interessante estabelecer quais funcionários estão autorizados a realizar a coleta e o tratamento de dados, e segmentar quais funcionários podem acessar quais informações. (FRAZÃO; OLIVA; ABILIO, 2019).

Deve-se estabelecer na documentação corporativa os meios pelos quais os titulares dos dados poderão exercer seus direitos garantidos pela Lei Geral de Proteção de Dados (LGPD), contendo indicação clara sobre o encarregado de dados. O programa de *compliance* deve garantir que o tratamento de dados realizado pela instituição permita o efetivo exercício desses direitos pelos titulares dos dados pessoais.

As instituições que incorrerem em violações dos preceitos normativos da lei estarão sujeitas às penalidades administrativas a serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), e podem ainda responder em outras esferas, como a cível e penal. A legislação determina que as penalidades administrativas sejam aplicadas ao final do processo administrativo, respeitando sempre o contraditório e a ampla defesa.

As sanções podem ser aplicadas gradativamente, isolada ou cumulativamente, conforme as particularidades de cada situação, observando fatores como a boa-fé da instituição, a implementação de estruturas e procedimentos internos que possam mitigar o dano, a utilização de políticas de boas práticas e governança, a resposta imediata a possíveis violações e a correção pronta para minimizar ou evitar eventuais danos. Logo, possuir um programa de *compliance* de proteção de dados

pessoais ajuda sobremaneira a organização a minimizar as sanções passíveis de imposição pela ANPD, caso haja transgressão das normas de proteção de dados (BLUM; MORAES, 2021).

É necessário que um bom programa de *compliance* de dados pessoais revise e atualize imediatamente o termo de uso e a política de privacidade, promovendo a atualização das cláusulas de contrato com colaboradores, usuários dos serviços e parceiros que trabalham com dados.

O percurso da adoção de programas de *compliance* de dados pessoais, se não fornecer uma resposta definitiva a questões de tratamento de dados, oferece uma visão de solução para eventual falha de violação da lei. Isso é feito de duas maneiras: (i) alivia o titular dos direitos dos ônus excessivos e do risco desavisado; e (ii) transfere a quem tem interesse e melhores recursos a responsabilidade pelo uso ético e justo dos dados. Sobretudo, isso deve ser feito com monitoramento constante. (ARTESE, 2021, p. 501)

Diante do exposto, o *compliance*, independentemente de sua forma, se tornou uma realidade para estabelecer boas práticas e governança, especialmente no que se refere ao tratamento de dados pessoais, estabelecendo normas nas operações e estruturando a organização para cumprir a lei.

#### 5.2.1.1. Das Medidas de Segurança da Informação

Sobre as medidas de segurança da informação, trataremos brevemente no capítulo 6, direcionado às instituições privadas de ensino superior. Portanto, trataremos aspectos mais pedagógicos trazidos pela LGPD.

Iniciamos pelo estabelecido pelo artigo 46 da LGPD, sobre a segurança e sigilo de dados. Ali, fica definido que controladores e operadores, na posição de agentes de tratamento de dados pessoais, devem utilizar medidas de segurança, técnicas e administrativas, capazes de assegurar a proteção dos dados pessoais, para evitar acessos não autorizados e a ocorrência de situações de violação acidental às normas, que possam provocar "destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito."

Essas medidas, vinculadas ao princípio da segurança, mencionado no capítulo 3 deste trabalho, têm como objetivo assegurar a proteção de dados, protegendo-os de diversas ameaças, garantindo a continuidade das atividades da instituição de forma segura e minimizando riscos, assegurando a confidencialidade e a integridade dos dados pessoais.

A Autoridade Nacional de Proteção de Dados, no uso de suas atribuições, poderá determinar os padrões técnicos mínimos para a aplicação das medidas estabelecidas no caput do artigo 46 da LGPD. Para isso, será considerada a natureza das informações tratadas, as características específicas do tratamento e o estado da tecnologia, especialmente em relação ao tratamento de dados sensíveis.

A segurança deve ser considerada desde os primeiros passos do tratamento de dados. Assim, as medidas devem ser implementadas desde a primeira etapa, que é a coleta dos dados pessoais, seja para organizações que prestam serviços ou ofereçam produtos. Devem ser observados durante a execução e ao término do tratamento. Portanto, os princípios de privacidade estão presentes desde a primeira etapa, proporcionando maior proteção ao tratamento de dados pessoais.

Temos a ideia da proteção à privacidade como um princípio a ser implementado desde as fases iniciais da execução, concebido pelo "privacy by design". Assim, essa proteção continua com a criação de ferramentas tecnológicas e modelos de negócios. Deste modo, a privacidade é garantida de ponta a ponta, levando em consideração todos os interesses envolvidos, sejam do controlador ou do titular, em toda a cadeia de execução de produtos ou serviços. (COTS; Oliveira, 2021).

Não obstante, qualquer dos atores que atuem em qualquer fase do processo de tratamento tem o dever de garantir a segurança dos dados pessoais, inclusive ao término do tratamento. Entretanto, caso ocorra alguma fragilidade de segurança que comprometa a operação ou coloque em risco de dano relevante, como o vazamento de dados pessoais ou acessos por agentes não autorizados, é dever do controlador informar a Autoridade Nacional e o titular dos dados dentro do prazo definido pela ANPD, nos termos do artigo 48, § 1º da LGPD. A informação deve conter, no mínimo:

> (...)
> I - A descrição da natureza dos dados pessoais afetados;
> II - As informações sobre os titulares envolvidos;
> III - A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - Os riscos relacionados ao incidente;

> V - Os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> (...)

Após o recebimento da informação, a ANPD analisará o ocorrido e, de acordo com o grau do incidente, determinará ao controlador a veiculação do fato em meios de comunicação adequados, se necessário, para tutelar os direitos do indivíduo e determinar a adoção de meios para reverter ou mitigar os riscos.

A ANPD poderá não agir em determinados incidentes caso seja demonstrado que foram adotados mecanismos de segurança, como a criptografia, para tornar os dados ininteligíveis, tornando desnecessárias as medidas mencionadas anteriormente. Desta forma, os sistemas implementados para o tratamento de dados precisam atender aos preceitos de segurança, boas práticas e governança.

### 5.2.2. Da Responsabilidade Prevista na LGPD

A LGPD estabelece a responsabilidade civil aos agentes de tratamento de dados pessoais no artigo 42, que:

> Art. 42. 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, é obrigado a repará-lo. (...)

Nota-se que o artigo 42 é o dispositivo principal da LGPD que aborda a responsabilidade civil. Neste sentido, observa-se que tal responsabilidade é imputada apenas aos agentes de tratamento (controlador ou operador). Portanto, a responsabilidade civil não se aplica ao encarregado de dados, pois este não é definido como agente de tratamento. Assim, ele não responde civilmente, mas sim, conforme a disposição legal aplicável às suas condutas (COTS; OLIVEIRA, 2021).

Não há que se falar em responsabilidade solidária do controlador e do operador, pois cada um responderá nos limites dos atos que praticou, obrigando-se a reparar os danos causados pelas suas condutas ao violar dispositivos da LGPD.

A lei estabelece duas possibilidades de responsabilidade solidária, conforme o artigo 42, § 1º da LGPD. A primeira ocorre quando o operador viola dispositivos da LGPD, e a segunda quando o operador não cumpre as determinações legais do controlador quanto ao tratamento de dados pessoais. Nestes casos, a responsabilidade será solidária.

Quando mais de um controlador participa da operação de tratamento de dados e causam danos ao titular, ambos serão responsabilizados, sendo resguardado o direito de ação de regresso ao que não deu causa diretamente ao dano. (TEIXEIRA; ARMELIN, 2020).

De outro lado, a lei determina que o juiz, quando houver verossimilhança nas alegações dos titulares ou em situações de hipossuficiência, poderá inverter o ônus da prova. Isso porque, muitas vezes, o titular é a parte mais fraca na relação, encontrando-se em desvantagem frente ao controlador e ao operador. A verossimilhança se dá quando o juiz se convence de que a razão assiste ao titular dos dados. (COTS; Oliveira, 2021).

O artigo 44 da LGPD estabelece que o tratamento de dados pessoais que não seja realizado de acordo com a lei ou que não forneça a segurança esperada será considerado uma operação irregular. Além disso, o parágrafo único determina que o controlador ou operador que não adotar medidas de segurança "responderá pelos danos decorrentes da violação da segurança dos dados" (...).

#### 5.2.2.1. Isenção de Responsabilidade

O artigo 43 da LGPD estabeleceu um rol de situações que permitem a exclusão da responsabilidade dos agentes de tratamento (controlador e operador). Assim, na Lei Geral de Proteção de Dados, os agentes de tratamento não são sujeitos a responsabilização desde que comprovem que: "não realizaram o tratamento de dados pessoais que lhes é atribuído; não houve violação à legislação de proteção de dados; ou o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros." Vamos analisar*:*

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - Que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - Que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

São essas hipóteses que excluem a responsabilidade. Em geral, são possibilidades previstas pelo direito que resultam na extinção da responsabilidade do indivíduo, pois removem o nexo de causalidade entre a ação e o dano (TEIXEIRA; ARMELIN, 2020).

Somente haverá responsabilização se houver uma violação da LGPD que cause danos ao titular dos dados pessoais. Do contrário, não há razão para falar em responsabilização.

Se ocorrer a culpa exclusiva do titular dos dados ou a culpa exclusiva de terceiros, sem a intervenção do controlador, também haverá a isenção de responsabilidade.

Por fim TEIXEIRA e ARMELIN, (2020 p.322). aduz que:

> LGPD precisa ser compatibilizada com todo o ordenamento jurídico pátrio, sendo que o fato príncipe, o caso fortuito e a força maior (fortuito externo) são excludentes de responsabilidade aplicáveis às relações jurídicas sujeitas à LGPD, bem como à sua fonte subsidiária, o CDC

Conclui-se que o legislador previu a responsabilidade civil dos agentes de tratamento de dados na LGPD com sabedoria, pois, conhecendo a realidade brasileira, ele se preocupou em garantir que os titulares dos dados pessoais tivessem os recursos necessários para proteger sua privacidade e usar mecanismos para coibir e punir aqueles que conduzem ao tratamento ilegal de seus dados pessoais.

### 5.2.3. Das Sanções Administrativas Previstas na LGPD

Sanção é uma espécie de punição aplicada a um indivíduo por promover comportamento em desacordo com as normas. Assim, a sanção administrativa é uma punição que tem o objetivo de coibir a transgressão das regras, e não necessariamente de reparar os danos causados por essa conduta infratora.

A LGPD, no artigo 52, prevê de forma exaustiva um rol de medidas administrativas sancionadoras para a transgressão das normas da LGPD. Como podemos ver na legislação:

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

O rol apresentado acima é considerado exaustivo, pois abrange todas as possibilidades disponíveis no âmbito administrativo. No entanto, na esfera judicial, o magistrado tem a liberdade de, no exercício da tutela jurisdicional, determinar o que entender necessário para assegurar o exercício do direito do titular (COTS; OLIVEIRA, 2021).

Qualquer transgressão aos dispositivos estabelecidos na LGPD estará sujeita às medidas administrativas de sanção, que serão aplicadas pela Autoridade Nacional de

Proteção de Dados. O artigo não menciona nenhum dispositivo específico, deixando claro que qualquer transgressão à lei está sujeita às sanções administrativas, mesmo as menos evidentes, como princípios.

Observa-se que as sanções administrativas são direcionadas aos agentes de tratamento de dados pessoais, ou seja, aos operadores e controladores de dados. Desta forma, a lei não prevê medidas administrativas em relação ao encarregado de dados, pois ele atua por subordinação ao controlador ou operador e, portanto, não se enquadra como agente de tratamento.

Como mencionado anteriormente, a ANPD é o órgão competente para aplicar sanções administrativas em caso de violação das disposições da LGPD sobre tratamento de dados. O artigo 52 § 1º da LGPD fornece uma referência para a aplicação dessas sanções, que podem ser aplicadas isoladamente, cumulativamente ou gradativamente após o procedimento administrativo, observando-se o princípio do contraditório e da ampla defesa previstos no artigo 5, inciso LV, da Constituição Federal de 1988.

Os parâmetros a serem seguidos pela ANPD para a aplicação de sanções administrativas devem observar (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, em consonância com o disposto no inciso II do § 2º do art. 48 da LGPD; (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.

Para definir a sanção a ser aplicada, é necessário considerar o fato em questão, pois fixar uma medida desproporcional à realidade pode impedir o desenvolvimento da livre iniciativa. Portanto, é importante usar a razoabilidade ao equilibrar a sanção ao potencial lesivo da conduta do agente.

Na implementação do *compliance* de dados pessoais, é possível adotar boas práticas que visem minimizar os efeitos de possíveis sanções.

### 5.2.4. Efeitos dos Programas de *Compliance* de Dados Pessoais

É evidente a preocupação do legislador com a segurança da informação e a privacidade dos dados dos titulares. Assim, compreende-se que a aplicação de programas de governança ou *compliance* é um poderoso instrumento para assegurar o cumprimento da legislação de proteção de dados pessoais e mitigar os efeitos de possíveis transgressões.

Os efeitos dos programas de governança vão muito além da simples observância da lei. Eles impactam a forma como a organização desenvolve suas atividades, pois se propõem a reestruturar toda a sua forma de organização. No caso do *compliance* de dados pessoais, eles afetam a maneira como a instituição coleta, trata e descarta os dados.

Com programas efetivos de *compliance*, a relação de confiança entre o titular e o agente de tratamento é positiva, pois o programa assegura os mecanismos necessários para reduzir os riscos.

Assim, a relação se torna transparente e pode se transformar em um diferencial competitivo para os negócios da instituição. A adoção de programas de governança corporativa também pode ensejar o afastamento da responsabilidade, conforme previsto no artigo 43, inciso II.

A existência de um programa de governança robusto contribui para que as sanções aplicadas pela ANPD sejam amenizadas, pois é um mecanismo de autorregulação institucional que possui instrumentos capazes de demonstrar o comprometimento da instituição em realizar as operações de dados pessoais de acordo com a lei.

Os programas de *compliance* de dados pessoais visam instrumentalizar os agentes de tratamento para adotarem mecanismos eficazes que garantam a segurança da informação e o fiel cumprimento das disposições da LGPD.

Ter uma estrutura funcional de *compliance* alinhada à governança permite que os riscos sejam minimizados e que as operações sejam realizadas com mais segurança, propiciando uma resposta mais efetiva e ágil a eventuais incidentes de vazamento de dados.

# 6. LGPD NA INSTITUIÇÃO DE ENSINO SUPERIOR PRIVADA

No presente capítulo, iniciamos a análise da aplicação da Lei Geral de Proteção de Dados (LGPD) no interior da instituição privada de ensino superior, a partir da perspectiva observada no estudo de caso. Destacamos algumas considerações preliminares aos resultados obtidos, necessárias para a melhor compreensão do estudo realizado no Centro Universitário Unifasipe, que serão discutidos no capítulo seguinte.

O Centro Universitário Unifasipe, uma instituição de ensino superior privada, foi escolhido como local de estudo de caso devido à sua importância para o Estado de Mato Grosso, onde tem colaborado há mais de vinte anos na formação de nível superior.

O Grupo Unifasipe é um dos três maiores grupos educacionais presentes no Estado de Mato Grosso e é o único genuinamente mato-grossense. Conta com mais de vinte cursos de graduação e pós-graduação ativos.

Com sede administrativa em Sinop, no Estado de Mato Grosso, o grupo está em plena expansão, possuindo sete unidades em Mato Grosso e uma unidade em Brasília, dedicadas exclusivamente ao ensino superior, e contando com mais de quinze mil alunos ativos entre graduação e pós-graduação.

Além disso, o grupo também possui três unidades de escolas de ensino infantil, fundamental e médio, colaborando para o fortalecimento do setor educacional no Estado de Mato Grosso. Por essa relevância, o grupo foi escolhido como objeto de estudo de caso.

Para uma melhor compreensão, conceituamos alguns elementos necessários para a conformação da Instituição de Ensino Superior (IES) com a LGPD, como, por exemplo, o sistema de tecnologia da informação. Embora a instituição possua um sistema de gestão acadêmica, será necessário implementar melhorias nos processos para promover a adequação à lei.

Portanto no presente capítulo, iniciamos uma explanação sintética sobre os conceitos de gestão da segurança da informação, gestão de documentos e gestão de documentos eletrônicos (GED). A digitalização de documentos é apresentada como uma ferramenta poderosa para ajudar na gestão e na segurança das informações da Instituição de Ensino Superior (IES).

Abordamos também os agentes envolvidos no tratamento de dados na IES, fazendo uma análise da situação atual, identificando problemas e apresentando uma proposta de estrutura de gestão de risco para manter a IES em conformidade com a Lei Geral de Proteção de Dados (LGPD).

É importante destacar a relação entre a LGPD e o desenvolvimento das atividades das Instituições de Ensino Superior Privadas, que precisam tratar dados pessoais de acordo com as disposições do artigo 7º, incisos II a X da LGPD e do artigo 10, que dispensa a necessidade de autorização ou consentimento do titular em casos específicos, como o cumprimento de obrigações legais.

O artigo 62 da Lei Geral de Proteção de dados deixa claro que o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) e a Autoridade Nacional de Proteção de Dados (ANPD) editarão regulamentos conforme a sua competência sobre o tratamento de dados pela União conforme determina a Lei 9.394/1996 denominada Lei de Diretrizes e Bases da Educação Nacional (LDB) e a Lei 10.861/2004 que instituiu o Sistema Nacional de Avaliação da Educação Superior – SINAES.

> Art. 62. A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional), e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004.

A Lei 9.394/1996 LDB, prevê em seu artigo 9º uma série de encargos à União, das quais:

> Art. 9º A União incumbir-se-á de:
> (...)
> V – coletar, analisar e disseminar informações sobre a educação;
> (...)
> IX – autorizar, reconhecer, credenciar, supervisionar e avaliar, respectivamente, os cursos das instituições de educação superior e os estabelecimentos do seu sistema de ensino.

Assim conforme determina o parágrafo 2º do mesmo artigo sobre o cumprimento dos referidos encargos está previsto o seguinte:

> § 2° Para o cumprimento do disposto nos incisos V a IX, a União terá acesso a todos os dados e informações necessários de todos os estabelecimentos e órgãos educacionais.

Essa dispensa e regulamentação é necessária pois impacta no cumprimento de obrigação legal com a disponibilização de informações ao Ministério da Educação (MEC), ao Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) e ao Sistema Nacional de Avaliação da Educação Superior – SINAES.

Em ambos os casos mencionados acima a Instituição de Ensino Superior deverá disponibilizar os dados dos estudantes a União, ou seja, será compartilhado os dados pessoais com a União para o cumprimento de uma determinação legal.

As instituições de ensino superior estão sujeitas à LGPD e devem tomar medidas para garantir a proteção dos dados pessoais dos alunos, professores e funcionários. Isso inclui a implementação de medidas de segurança para evitar vazamentos de dados, a criação de políticas de privacidade e a capacitação de funcionários para lidar com questões relacionadas à privacidade de dados.

De acordo com a Associação Brasileira de Mantenedoras de Ensino Superior (ABMES):

> "As instituições de ensino superior devem se adaptar à nova regulamentação, elaborando políticas e procedimentos para garantir a privacidade e segurança dos dados pessoais de seus alunos, professores e funcionários, além de serem transparentes quanto à coleta, uso e compartilhamento desses dados."

Além disso, o Conselho Nacional de Educação (CNE) emitiu uma Resolução (nº 1, de 26 de outubro de 2020) que estabelece diretrizes para as instituições de ensino superior se adequarem à LGPD. Esta resolução recomenda que as instituições de ensino superior estabeleçam medidas para garantir a privacidade e segurança dos dados pessoais, criem políticas de privacidade e capacitem seus funcionários para lidar com questões relacionadas à privacidade de dados.

A Lei Geral de Proteção de Dados Pessoais obriga as instituições de ensino superior a garantir a proteção dos dados pessoais dos alunos, professores e funcionários, incluindo medidas de segurança, políticas de privacidade e capacitação de funcionários.

Além das medidas mencionadas anteriormente, as instituições de ensino superior (IES) também devem designar um encarregado de proteção de dados (DPO) para garantir a conformidade com a LGPD e lidar com qualquer questão relacionada à privacidade de dados. Essa pessoa será responsável por garantir que a instituição esteja

cumprindo as exigências da LGPD e deve ter conhecimentos especializados em privacidade de dados e proteção de dados.

A IES também deve se preparar para lidar com requerimentos de acesso e retificação de dados pessoais, bem como para lidar com incidentes de segurança de dados. Isso inclui a implementação de medidas de segurança para proteger os dados pessoais contra vazamentos, roubo e outras violações de segurança, bem como a capacitação dos funcionários para lidar com incidentes de segurança de dados.

É importante destacar que, uma vez que as instituições de ensino superior lidam com dados sensíveis, como informações médicas e financeiras dos estudantes, é ainda mais crucial que elas cumpram as exigências da LGPD e implementem medidas de segurança e proteção de dados adequadas.

As instituições de ensino superior devem também ser transparentes sobre como eles coletam, usam e compartilham dados pessoais. Isso inclui fornecer informações claras e precisas sobre como os dados são coletados, usados e compartilhados, bem como garantir que os indivíduos tenham o direito de acessar, corrigir ou excluir seus dados pessoais.

A IES deve se preparar para a LGPD, implementando medidas de segurança, designando um DPO, preparando-se para lidar com requerimentos de acesso e incidentes de segurança de dados, além de serem transparentes sobre como eles coletam, usam e compartilham dados pessoais.

## 6.1. SISTEMA DE TECNOLOGIA DA INFORMAÇÃO

O conceito de sistema foi inicialmente introduzido por Ludwig von Bertalanffy em 1930, tendo como base o conceito aristotélico de que "o todo é maior do que a soma das partes". Bertalanffy desenvolveu a Teoria Geral dos Sistemas, e, segundo Martinelli (2012, p. 8), consiste em:

> [...] um esqueleto, um modelo de análise do mundo empírico, um modelo de como analisar fenômenos complexos enquanto sistemas, um todo com partes interrelacionadas.

Portanto, um sistema é constituído por elementos interconectados e interdependentes com o objetivo de formar um conjunto organizado para um fim comum. A partir daí, outras áreas do conhecimento se valeram dessa teoria e a utilizaram de forma interdisciplinar para o gerenciamento de informações.

O gerenciamento da informação pode ser conceituado como processos, ou seja, é "um conjunto estruturado de atividades que inclui como as empresas obtêm, distribuem e usam a informação e o conhecimento" (DAVENPORT, 2000, p. 173).

É necessário que esses "processos" sejam constantemente aperfeiçoados e monitorados, por isso surge a figura dos sistemas de informação para viabilizar um gerenciamento mais eficaz, servindo como base de conhecimento para o constante aperfeiçoamento desses sistemas. De acordo com Laudon, K. e Laudon, J. (1999, p. 4), o gerenciamento de sistemas de informação é:

> Um conjunto de componentes inter-relacionados trabalhando juntos para coletar, recuperar, processar, armazenar e distribuir informação com a finalidade de facilitar o planejamento, o controle, a coordenação, a análise e o processo decisório em empresas e outras organizações.

Os sistemas de informação (SI) desempenham uma função primordial no tratamento de informações e dados pessoais, tendo a informação como elemento principal. Um dos fundamentos de sua existência é o armazenamento de informações em conjunto com o banco de dados e a disponibilização dessas informações para viabilizar os processos da instituição de ensino superior.

A utilização de um sistema de informação é extremamente útil para o desenvolvimento das atividades da organização, principalmente porque automatiza diversas etapas que antes eram realizadas manualmente, agregando valor à operação. Embora a informação seja algo incorpóreo, ela possui um grande valor para o desempenho das atividades da Instituição de Ensino Superior (IES).

Os sistemas de informação têm a capacidade de mudar o "fluxo de informação", permitindo que mais usuários acessem e compartilhem informações ao mesmo tempo. Assim, as tarefas que antes eram realizadas manualmente e de forma sequencial, podem ser automatizadas e feitas simultaneamente, eliminando a demora na tomada de decisão. De acordo com Laudon, K. e Laudon, J. (2010, p. 10):

> Os Sistemas de Informação automatizam muitas etapas que antes eram executadas manualmente. A tecnologia da Informação pode alterar o fluxo de informação, tornando possível que um número maior de pessoas

> acesse e compartilhe informações, substituindo as etapas sequenciais por tarefas que podem ser executadas simultaneamente e eliminado o atraso na tomada de decisão.

A Instituição de Ensino Superior (IES) produz diariamente um grande volume de informações, como dados de matrícula, listas de presença, lançamento de notas e avaliações. Para gerenciar essas informações de forma eficaz, é necessário que seja realizado, desde o início, o mapeamento de todas as informações que realmente afetam as atividades da Instituição de Ensino Superior (IES).

Dessa forma, será possível ter um controle aprimorado da segurança da informação, desde a coleta até o descarte de dados que não são objeto de tratamento pela Instituição de Ensino Superior (IES).

Esse mapeamento das informações é fundamental para conhecer o verdadeiro tamanho da operação de tratamento de dados e identificar as categorias de informações tratadas, para que a Instituição de Ensino Superior (IES) possa se adequar à Lei Geral de Proteção de Dados (LGPD) e garantir a proteção dos dados dos estudantes.

## 6.2. GERENCIAMENTO E SEGURANÇA DA INFORMAÇÃO

Observou-se na Instituição de Ensino Superior (IES) uma preocupação com a segurança da informação por parte dos gestores. Essa preocupação se comprovou por meio da atuação de diversos atores da instituição, especialmente pelo diretor de tecnologia do grupo, que demonstrou os investimentos realizados na segurança da informação.

Sobre segurança da informação, podemos conceituá-la como os meios que a instituição utiliza para garantir a proteção dos dados pessoais, sejam de terceiros, como os alunos, ou internos, como os funcionários. Portanto, a instituição deve promover ações ou instrumentos que possibilitem este objetivo.

SÊMOLA (2014, p. 41) define a segurança da informação como "uma área do conhecimento dedicada à proteção de ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade." Para uma melhor compreensão, apresentamos três princípios fundamentais da segurança da informação:

Confidencialidade, que assegura o acesso à informação somente por pessoas autorizadas, e que geralmente é encontrado sob a nomenclatura de controle de acesso, limitando o acesso dos sistemas para evitar que pessoas não autorizadas tenham conhecimento de informações que não lhes dizem respeito; disponibilidade da informação, pois ela deve estar disponível no momento da requisição; e integridade, que consiste em a informação estar em um estado perfeito, isto é, igual ao momento de armazenamento, garantindo que ela não seja modificada acidentalmente por pessoas não autorizadas.

A implementação de políticas de gestão da segurança da informação é essencial para minimizar os riscos inerentes ao tratamento de dados pessoais. Na pesquisa em questão, foi possível identificar que a Instituição de Ensino Superior (IES) está em processo de adequação à Lei Geral de Proteção de Dados (LGPD), implementando práticas eficazes de proteção, especialmente de dados pessoais, para garantir a segurança dos documentos, sejam eles físicos ou eletrônicos.

Foi observado que a IES adotou pontos de controle para identificação de possíveis ameaças, e realizou investimentos em infraestrutura de TI, como softwares e hardwares de segurança, além de redes lógicas seguras, como cabeamentos e conexões Wi-Fi.

Além disso, devido à determinação do Ministério da Educação (MEC) por meio da Portaria SESU N°1/2020, que determinou a emissão de diplomas online, houve a necessidade de adequação da infraestrutura de segurança, especialmente em relação aos dados pessoais, para garantir a integridade desse processo.

A instituição tem demonstrado preocupação em garantir a segurança da informação de forma adequada, buscando a conscientização das pessoas envolvidas na manipulação de dados pessoais e incentivando os usuários dos sistemas a utilizarem as ferramentas oferecidas pela Instituição de Ensino Superior (IES), como os termos de confidencialidade e responsabilidade jurídica.

No que se refere às informações disponibilizadas em meio eletrônico, a Instituição de Ensino Superior (IES) tem trabalhado com seus fornecedores de software e hardware para implementar mecanismos e melhorias eficazes na proteção dos documentos e dados pessoais.

## 6.3. GERENCIAMENTO DE DOCUMENTOS

A implementação de um sistema de gestão documental na Instituição de Ensino Superior (IES) é uma fase importante na busca pela organização, arquivamento e fácil localização dos arquivos, especialmente na secretaria acadêmica, que possui uma grande demanda.

A gestão de documentos consiste em um conjunto de medidas e rotinas que garantem o efetivo controle de todos os documentos, desde sua produção até sua destinação final. (BERNARDES, 1998).

Esta implementação, combinada com as medidas de segurança da informação, visa proporcionar maior segurança às informações e documentos utilizados na Instituição de Ensino Superior (IES) e é um passo importante para a adequação à LGPD. Além disso, a gestão documental ajuda na eficiência administrativa, preservando documentos que anteriormente poderiam ter sido perdidos devido à falta de gestão documental.

Entre as medidas a serem adotadas, destaca-se a implantação de programas de gestão, pois:

> A implantação de um programa de gestão documental garante aos órgãos públicos e empresas privadas o controle sobre as informações que produzem ou recebem, uma significativa economia de recursos com a redução da massa documental ao mínimo essencial, a otimização e racionalização dos espaços físicos de guarda de documentos e agilidade na recuperação das informações. (BERNARDES; DELATORRE, 2008, p.7)

A implementação de meios de gerenciamento de documentos, utilizando conceitos e bases doutrinárias sobre o assunto, oferece à Instituição de Ensino Superior (IES) maior controle sobre suas informações e uma otimização nos meios físicos de armazenamento de arquivos, agregando agilidade no desempenho das atividades.

Destaca-se que essas medidas adotadas pela Instituição de Ensino Superior (IES) são decisões estratégicas, pois proporcionam maior controle sobre o ciclo de vida dos documentos, evitando assim a permanência de arquivos desnecessários.

A Instituição de Ensino Superior (IES), na gestão de documentos, pretende adotar o modelo apresentado por Bernardes e Delatorre (2008, p.10), que consiste em

compreender o ciclo de vida dos documentos, dividido em três fases: corrente, intermediária e permanente, como demonstrado no quadro 1.

**Quadro 1: Fases do ciclo de vida documental**

| | | |
|---|---|---|
| **CORRENTE** | Documentos vigentes e frequentemente consultados | Arquivo corrente |
| **INTERMEDIÁRIA** | Final de vigilância. Aguardam prazos de prescrição e precaução, raramente são consultados e aguardam destinação final: eliminação ou guarda permanente. | Arquivo intermediário |
| **PERMANENTE** | Documentos que perderam a vigência administrativa, porém são providos de valor secundário ou histórico-cultural. Arquivo | Permanente ou histórico |

Com isso, a gestão de documentos se torna mais eficiente, uma vez que permite estabelecer a localização de cada documento em todas as fases. Nesse sentido, foi observado na equipe operacional da Secretaria Acadêmica que a gestão documental facilita as atividades cotidianas, pois encontrar um documento já posicionado e indexado acelera os trabalhos da Secretaria.

Ressalta-se que é necessário o treinamento constante para a utilização das boas práticas de governança neste ponto, pois há a definição do que pode ser eliminado ou a determinação dos locais corretos para o armazenamento dos documentos, bem como o tempo de guarda da documentação.

O Dicionário Brasileiro de Terminologia Arquivística (2005, p. 100) define a gestão de documentos como:

> Conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando sua eliminação ou recolhimento. Também chamado de administração de documentos.

Portanto, no Quadro 2, a Instituição de Ensino Superior (IES) nos apresentou algumas etapas e atividades que devem ser implementadas para assegurar a gestão eficiente de documentos.

Ressalta-se que as etapas a seguir foram apresentadas e destacadas como um modelo elaborado por Bernarde e Delatorre (2008, p. 9).

**Quadro 2: Implementação da Gestão de Documentos**

| | |
|---|---|
| Produção de documentos | Elaboração padronizada de tipos/séries documentais, implantação de sistemas de organização da informação e aplicação de novas tecnologias aos procedimentos administrativos. |
| Utilização dos documentos | Inclui todas as atividades de Protocolo (recebimento, classificação, registro, distribuição, tramitação e expedição), todas as atividades de Arquivo (organização e arquivamento, reprodução, acesso à documentação e recuperação de informações) e a gestão de sistemas de protocolo e arquivo, sejam eles manuais ou informatizados. |
| Destinação de documentos | Inclui uma das atividades mais complexas da gestão de documentos que é a avaliação. A avaliação se desenvolve a partir da classificação dos documentos produzidos, recebidos e acumulados pelos órgãos públicos ou empresas privadas, com vistas a estabelecer seus prazos de guarda e sua destinação final, garantindo a preservação de documentos de guarda permanente e a eliminação criteriosa de documentos desprovidos de valor probatório e informativo. |
| Tramitação | Estudo das instâncias de decisão, padronização e controle do fluxo documental (workflow). |
| Organização e arquivamento | De acordo com os critérios definidos no Plano de Classificação. |
| Reprodução | Duas razões para a reprodução: 1. reprodução visando a preservação do documento original de guarda permanente e, 2. reprodução visando a substituição do documento em papel pelo microfilme. O documento em papel de guarda temporária poderá ser eliminado e o microfilme deverá ser preservado pelo prazo indicado na Tabela de Temporalidade de Documentos de Arquivo. |
| Classificação | Recupera o contexto de produção dos documentos, isto é, a função e a atividade que determinou a sua produção e identifica os tipos/séries documentais. |
| Avaliação | Trabalho multidisciplinar que consiste em identificar valores para os documentos e analisar seu ciclo de vida, com vistas a estabelecer prazos para sua guarda e destinação (eliminação ou guarda permanente). |

A Instituição de Ensino Superior (IES) destaca que o modelo deve ser adaptado para garantir a proteção de dados pessoais em todas as fases da gestão de documentos, com a implementação de outras ferramentas, como sistemas informáticos dedicados à gestão de documentos e segurança da informação.

## 6.4. GERENCIAMENTO DE DOCUMENTOS ELETRÔNICOS

Uma das ferramentas encontradas na Instituição de Ensino Superior (IES) é o sistema GED, que é o sistema de gerenciamento de documentos eletrônicos, em fase de implantação paralela à digitalização, que será abordada no tópico seguinte.

O GED é uma ferramenta que permite a preservação e organização de documentos em meio digital, que, através de tecnologias de hardware e software destinadas a essa finalidade, possibilita o gerenciamento eficaz de qualquer documento da instituição, estabelecendo ferramentas de gerenciamento de permissões e níveis de permissão, e disponibilizando acesso via web e multiplataforma.

Destaca-se que, apesar da implementação do gerenciamento eletrônico de documentos, os arquivos físicos não serão eliminados por completo, pois, de acordo com as determinações legais aplicáveis, os documentos físicos devem ser mantidos. O que ocorre é a facilitação no gerenciamento e manipulação desses documentos.

Entretanto, para os arquivos que são originalmente digitais, não há necessidade de armazenamento em meio físico, pois a própria natureza do documento é digital, como, por exemplo, os novos diplomas que serão emitidos exclusivamente em meio digital.

## 6.5. A NECESSIDADE DA DIGITALIZAÇÃO DE DOCUMENTOS

Outro ponto importante encontrado na Instituição de Ensino Superior (IES) foi o implemento da digitalização de documentos para inserção no GED. Como ocorre em grande parte das empresas, diariamente são geradas ou utilizadas enormes quantidades de documentos por diversos setores, a Instituição de Ensino Superior (IES) utiliza a digitalização de documentos como componente de seu plano de adequação à LGPD e para otimização de processos. Isso confere agilidade e segurança ao processo de tratamento.

A Instituição de Ensino Superior (IES) se propôs a digitalizar gradualmente todos os documentos utilizados constantemente em suas operações e a concentrar as

informações em um banco de dados, eliminando assim o acúmulo de papéis e melhorando a organização de suas rotinas operacionais. Desta forma, o controle e acesso aos documentos se tornam mais eficientes, práticos e rápidos, pois a digitalização de processos agrega muitas vantagens às operações.

Assim pontua o diretor de tecnologia da Instituição de Ensino Superior do Grupo Unifasipe:

> "A falta de incentivo a modernização de processos, poderia ocasionar prejuízos até na atividade mais simples de uma instituição, pois a dificuldade na execução tomaria mais tempo do colaborador atrasando a execução dos processos. E com essa digitalização conseguimos organizar melhor os documentos da instituição inclusive para utilização como provas em eventuais litígios jurídicos." (informação verbal)[13]

Essa digitalização de processos tende a aumentar a produtividade da Instituição de Ensino Superior (IES). Observa-se, na IES, a constante e importante participação da direção de tecnologia do grupo e do gestor de TI, em todos os processos da unidade, sempre visando à segurança da informação. Corroborando essa observação, temos o entendimento de Patrícia Peck Pinheiro (2021, p.174) ao se referir à gestão de documentos eletrônicos, onde ela afirma que:

> (...) nada adianta guardar a prova se não for possível encontrá-la quando precisar. Por este motivo, tem crescido o uso de tecnologias para gestão eletrônica de documentos, que devem não apenas observar o armazenamento, mas principalmente a segurança do ambiente para proteção da integridade ao longo do tempo e a taxonomia e demais indicadores de localização e identificação da base de dados.

A segurança dos processos digitalizados é equacionada na Instituição de Ensino Superior (IES) por meio da adoção de sistemas de proteção de rede, como firewalls, criptografia, controles de acesso e rotinas de backup. Além disso, observa-se a adoção de redundância dos servidores de aplicação e a disponibilização de serviços em nuvem, redundância de conexões de alta velocidade à rede mundial de computadores e interligação entre as unidades do grupo por meio de uma rede privada com proteção integral, evitando assim o comprometimento da operação institucional.

Deste modo, o acúmulo de documentos originais em arquivos físicos deixa de representar riscos para a instituição, pois passa a ser administrados com maior cuidado com a segurança das informações dos estudantes e demais serviços relacionados ao

[13] Informação verbalmente repassada pelo diretor de tecnologia durante o estudo de caso no Centro Universitário Unifasipe.

negócio. Ao aplicar a gestão de documentos, essas informações passam a ser protegidas em local adequado, sem que haja exposição ao tempo ou manipulações desnecessárias ou acessos desautorizados. Dessa forma, é possível evitar danos ou perda de qualidade desses documentos.

## 6.6. AGENTES ENVOLVIDOS NO TRATAMENTO DE DADOS NA INSTITUIÇÃO DE ENSINO SUPERIOR (IES)

Como já foi demonstrado no capítulo 4, sobre o tratamento de dados pessoais, o artigo 5º da LGPD apresenta alguns termos utilizados no contexto de proteção de dados pessoais. Aqui, eles são recapitulados e direcionados à aplicação em uma Instituição de Ensino Superior (IES), objeto do presente estudo, e serão abordados como agentes envolvidos no tratamento.

Abaixo, para melhor ilustrar, apresentamos a Tabela 1, que relaciona o termo descrito na lei com a sua definição legal e o agente envolvido no tratamento na IES.

**Quadro 3 – Agentes envolvidos no tratamento na Instituição de Ensino Superior (IES) - Artigo 5º**

| Inciso | Termo Legal | Definição | Envolvidos no Tratamento na Instituição de Ensino Superior (IES) |
|---|---|---|---|
| V | Titular | Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; | Funcionários, prestadores de serviço, professores, coordenadores de curso, alunos e ex-alunos, visitantes; |
| VI | Controlador | Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; | Instituição de Ensino Superior (IES): Diretor Presidente e Superintendente Acadêmico; |
| VII | Operador | Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; | Parceiros de Negócios do Controlador: Instituição de Ensino Superior (IES), Co- |

| | | | |
|---|---|---|---|
| | | | Operador, Diretores de Unidades; |
| VIII | Encarregado | Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); | Ainda em definição pela direção da Instituição de Ensino Superior (IES); |

O número de operadores necessários para o tratamento de dados pode oscilar de acordo com a quantidade de parceiros que possuem o Controlador. Eles devem agir de forma a garantir a proteção e privacidade dos dados pessoais tratados ou em tratamento, sem prejudicar a responsabilização solidária em caso de infrações legais, conforme previsto no artigo 42 da LGPD.

A Lei Geral de Proteção de Dados (LGPD) não aborda a figura do Co-Operador, mas é importante levar em consideração essa ideia, pois é comum que o Controlador terceirize o tratamento de dados para outro operador, que por sua vez pode terceirizá-lo novamente. Por exemplo, a terceirização do sistema de gestão acadêmica de uma Instituição de Ensino Superior (IES) para uma empresa, que por sua vez terceiriza o serviço de armazenamento do banco de dados em nuvem.

## 6.7. DIAGNÓSTICO SITUACIONAL - ANÁLISE DO AMBIENTE

É importante mencionar que, para a elaboração do estudo proposto, na perspectiva das instituições particulares de ensino superior, foi buscado o contato com as principais instituições privadas do Estado de Mato Grosso.

No entanto, o relato preliminar é preocupante, pois a Lei Geral de Proteção de Dados (LGPD) está em vigor desde 18 de setembro de 2020 e, até o momento, as instituições privadas de ensino superior fizeram pouco ou nada para se adequar a essa legislação.

Diante disso, procurou-se analisar o ambiente do Grupo Educacional Fasipe, especificamente na unidade do Centro Acadêmico Unifasipe, a fim de compreender o que é necessário para se adequar à LGPD e garantir a proteção de dados estudantis no

Centro Acadêmico Unifasipe. Posteriormente, será observada a possibilidade de replicação em outras unidades do grupo.

Inicialmente, foi abordado, no primeiro contato com a Instituição de Ensino Superior (IES), a necessidade de conhecer o nível de compreensão sobre a implantação da LGPD e em que estágio de conformidade ou quais iniciativas estão sendo tomadas para se adequar à lei.

O contato principal para coleta de dados nesta pesquisa foi o diretor geral de tecnologia da informação do grupo Unifasipe, indicado pelo diretor presidente do grupo, que forneceu as informações e acompanhou o estudo de caso. Assim, o diretor de tecnologia é a pessoa responsável por liderar o processo de conformidade na Instituição de Ensino Superior (IES), em colaboração com o departamento jurídico.

O diretor de TI informou que a Instituição de Ensino Superior (IES) está em um processo de Roadmap para conformidade, pois estão em um processo de digitalização de documentos para uma gestão mais eficiente, como já mencionado anteriormente.

## 6.8. PROPOSTA DE ESTRUTURA DE ADEQUAÇÃO

De acordo com as observações realizadas na Instituição de Ensino Superior (IES), os resultados preliminares indicam a necessidade de idealizamos, em conjunto com a instituição, um modelo inicial para adequação à legislação brasileira de proteção de dados pessoais, de acordo com a fase atual de conformidade da Instituição de Ensino Superior (IES) e as políticas de governança de TI.

Sugerimos uma estrutura preliminar de adequação e gestão de risco, na qual apresentamos aqui, e na fase de discussão dos resultados, apresentaremos o modelo delineado com a Instituição de Ensino Superior (IES) para o processo de conformidade.

Baseado em gerenciamento de processos e governança de TI, construímos o modelo preliminar, estruturando um controle interno das operações com dados pessoais, gerenciamento de risco e a LGPD, com o objetivo de colaborar com o processo de proteção dos dados estudantis e adequação da Instituição de Ensino Superior (IES) à LGPD.

### 6.8.1. Proposta de adequação

Aqui, apresentaremos o modelo elaborado inicialmente com base na literatura aplicada ao caso da Instituição de Ensino Superior (IES). Esse modelo foi proposto com o objetivo de ajudar a Instituição de Ensino Superior (IES) a se adequar à legislação brasileira de proteção de dados pessoais, de acordo com o estágio atual de conformidade.

A elaboração desse modelo levou em conta a análise inicial do ambiente da Instituição de Ensino Superior (IES) e foi construído com base no gerenciamento de processos e governança de TI. O objetivo é contribuir para a proteção dos dados estudantis e a adequação da Instituição de Ensino Superior (IES) à LGPD.

Este modelo é estruturado em sete fases e é apresentado no quadro a seguir.

**Quadro 4: Proposta inicial para conformação da Instituição de Ensino Superior (IES)**

| FASE | DESCRIÇÃO | ESTÁGIO DA IES |
|---|---|---|
| **1ª Fase** | Inventário de dados, mapeamento de dados destinado ao conhecimento dos dados que a Instituição de Ensino Superior (IES) realiza o tratamento, se sensíveis ou não, triagem e conscientização da necessidade de adequação. | Em curso |
| **2ª Fase** | Verificação, adequação e implementação de medidas de segurança e gestão de riscos, e governança de TI, para assegurar a proteção aos dados pessoais e planejamento de *compliance*.<br>Fase destinada a adoção de medidas técnicas ou administrativas de segurança de dados pessoais, a ocorrer desde a fase de o primeiro contato com o titular até o término do tratamento e armazenamento, ou seja, todo e qualquer serviço da instituição deve estar destinado a assegurar a privacidade de dados. | Em análise |
| **3ª Fase** | Criação e adequação de estruturas destinadas ao atendimento aos titulares de dados, e mecanismos de comunicação interna e externa. | Processo existente, mas aguardando análise de adequação para conformidade |
| **4ª Fase** | Verificação do programa de *compliance* e promover as adequações e estabelecer após o mapeamento e implementar estruturas de resposta a incidentes, | Aguardando conclusão da fase 2 |

| | | |
|---|---|---|
| | proporcionando a redução de danos em eventuais violações as disposições da LGPD. | |
| **5ª Fase** | Realização de gestão de terceiros ou parceiros de negócios para adequar as ferramentas desenvolvidas por estes e utilizadas pela Instituição de Ensino Superior (IES) | Em análise de conformidade e adequações preliminares |
| **6ª Fase** | Documentação e registro das adequações já realizadas, em curso ou a ser realizadas, elaboração ou adequação de documentos institucional para conformidade elaboração de relatório relacionado aos processos de tratamento de dados pessoais, riscos do tratamento aos titulares, desenvolvido sobre o resultado das fases anteriores, o relatório possibilita conhecer medidas e situações cabíveis e possíveis para cada risco de dados levantado; | Pendente |
| **7ª Fase** | Monitoramento controle, treinamento e revisão de conformidade destinado manter a continuidade do programa de *compliance* na instituição. | Em processo de implementação |

Deve-se observar na implementação das fases, além da descrição no quadro 4, as disposições subsequentes. Na primeira fase, deve ocorrer um inventário de dados ou mapeamento de dados pessoais, que são frequentemente coletados na Instituição de Ensino Superior (IES). Portanto, é importante pontuar que o primeiro passo para iniciar o projeto de adequação na IES é conhecer os dados que são coletados, o fluxo desses dados, bem como o ciclo de vida desses dados na IES, e promover a conscientização de todos os envolvidos da necessidade de adequação e modificação de processos.

Destaca-se que este mapeamento não é uma imposição legal, mas, se não observado, tornará muito difícil o processo de adequação, pois existem uma série de obrigações que não poderão ser cumpridas sem esse mapeamento disponível.

Posteriormente, na fase 2, iniciar-se-á o levantamento de medidas de segurança e dos riscos inerentes na operação de tratamento de dados. Nesta fase, em especial, o trabalho deve ser interdisciplinar para alcançar a conformidade na proteção de dados pessoais, sendo uma obrigação implementar medidas de segurança físicas ou digitais capazes de proteger os dados pessoais dos titulares, conforme o artigo 6.º, inciso VII.

Apesar da Instituição de Ensino Superior (IES) ainda não estar nesta segunda fase, foi verificado o nível de implementação das práticas de Governança de TI, e constatou-se um grande investimento por parte da direção geral do grupo nesse setor.

Na fase 3, verifica-se a capacidade da Instituição de Ensino Superior (IES) em garantir o atendimento aos titulares dos dados, pois a Lei Geral de Proteção de Dados (LGPD) determina, nos artigos 17, 18 e seguintes, a necessidade de garantir o exercício dos direitos previstos na lei pelo titular dos dados processados.

Na fase 4, será necessário adotar medidas efetivas para responder a incidentes, sendo estas medidas obrigações de meio, como, por exemplo, o implemento de controles de gerenciamento e nível de acesso, atribuindo níveis específicos de controles de acesso aos sistemas informáticos de acordo com o grau de permissão de cada usuário na execução de suas atividades. Nestes aspectos, será necessário aplicar as boas práticas de governança, desde a alta gestão até os prestadores de serviço na ponta da operação.

Essa implementação é importante para gerenciar os riscos, identificando e adotando os meios adequados para garantir a segurança dos dados tratados e criar estruturas de mitigação de danos ou soluções adequadas para reduzir os efeitos de eventuais transgressões à LGPD.

Na fase 5, será necessário trabalhar em conjunto com os parceiros de negócio para promover a implementação das adequações em sistemas e ferramentas utilizadas na Instituição de Ensino Superior (IES), desenvolvidas por terceiros.

Na fase 6, serão registradas todas as medidas efetivamente desenvolvidas, implementadas ou a serem implementadas na instituição, criando e adequando a documentação institucional para atender à legislação e às boas práticas de governança corporativa.

Na fase 7, que é permanente e transversal às outras fases do processo de adequação, consiste em monitoramento, treinamento, controle e revisão da conformidade com a LGPD, desde a primeira fase, realizando as intervenções necessárias para adequar o processo de adequação à realidade da instituição e à lei constantemente.

O modelo proposto foi concebido com base na adequação à lei, tendo como base a implementação de um programa de *compliance* que poderá produzir impactos financeiros e operacionais para a instituição. É necessário destinar orçamento para que a adequação seja efetivada. Contudo, com base nas particularidades da presente pesquisa, em que as questões de gestão financeira são objeto de estudo, decidimos não detalhar este tema.

Todo programa de *compliance* importa em modificações, quanto maior o escopo do programa de conformidade, maior o número de mudanças em processos. Dessa forma, toda modificação consiste em transformar atitudes humanas, maneiras de executar rotinas operacionais, procedimentos, entre outros.

A adesão a programas de *compliance* pode resultar em resistência às medidas de conformidade, pois pode forçar as pessoas a saírem de sua zona de conforto e opor-se, em alguns casos, às mudanças institucionais, motivadas pela incapacidade de mudar ou pela falta de compreensão sobre as razões da transformação.

## 6.9. COLETA DE DADOS - ESTUDO DE CASO

Na pesquisa, buscou-se analisar as partes interessadas no processo de tratamento de dados estudantis, diretamente envolvidas com a gestão de uma Instituição de Ensino Superior (IES), especialmente na graduação, por meio da coleta de informações *in loco*. Paralelamente, foram selecionadas literaturas que abordavam o tema da proteção de dados nas instituições de ensino, especialmente aquelas que tratavam de medidas de conformidade, governança em TI, melhores práticas, processos de controle, como já mencionado anteriormente sobre a gestão de documentos, e principalmente a Lei Geral de Proteção de Dados (LGPD), para verificar a adequação da instituição.

Para o desenvolvimento desta pesquisa, buscou-se compreender a adequação da Instituição de Ensino Superior (IES) aos princípios de privacidade e proteção de dados pessoais e dados pessoais sensíveis no tratamento de informações dos estudantes.

Além disso, buscou-se avaliar a possibilidade de replicação desta adequação em outras instituições de ensino e verificar a relação com a hipótese de que as Instituições Privadas de Ensino Superior deverão observar esses princípios, diante das inovações tecnológicas. Para isso, é necessário que a IES empregue meios adequados, como técnicas de *compliance*, governança de TI ou outras formas de gestão, a fim de cumprir a legislação de proteção de dados.

Para o desenvolvimento desta pesquisa, foi realizada a coleta de dados por meio de um estudo de caso com a própria Instituição de Ensino Superior (IES). A IES colaborou fornecendo informações sobre a percepção da instituição e da Lei Geral de Proteção de Dados (LGPD) com os principais envolvidos no processo de tratamento de dados pessoais.

O estudo de caso foi escolhido como procedimento para conduzir a percepção da realidade da organização e obter resultados com maior qualidade. As informações foram coletadas com base nas informações disponibilizadas pela IES objeto de estudo. Esse momento é considerado um dos mais importantes do trabalho, pois direciona a discussão para o ambiente da vida real (MICHEL, Maria H. 2015).

A presente pesquisa apresenta em alguns momentos uma perspectiva teórica sobre os temas em função do nível embrionário de adequação percebido na instituição.

## 6.10. ANÁLISE DOS PROBLEMAS

Neste ponto, buscou-se observar o ambiente institucional e sua conformidade com a lei. Para isso, elaborou-se o Quadro 4, apresentado anteriormente, que permitiu identificar e qualificar o estágio atual da instituição em relação às fases definidas para adequação à lei.

A discussão dos resultados melhor elucidará essas informações, elencando os pontos mais relevantes e as dificuldades percebidas, como, por exemplo, a ausência de um plano oficial de *compliance* para conformidade com a lei e o conhecimento superficial da legislação de proteção de dados pessoais.

## 6.11. PROFISSIONAIS ENVOLVIDOS NO ESTUDO DE CASO

No processo de coleta de dados para a realização da pesquisa, primeiramente foi estabelecido o contato com o presidente do grupo e mantenedor da Instituição de

Ensino Superior (IES), na oportunidade em que foram especificados a intenção, as eventuais contribuições e os objetivos da pesquisa.

Em seguida, houve o direcionamento ao diretor de tecnologia do grupo, pois ele é a pessoa responsável pelo projeto de adequação, em conjunto com o departamento jurídico do grupo.

Após conversas preliminares com o diretor de TI, foi disponibilizado acesso às informações necessárias para a realização do estudo de caso sobre os atores que lidam com dados pessoais estudantis na Instituição de Ensino Superior (IES).

Foi realizado o estudo de caso no Centro Universitário Unifasipe, coletando dados disponibilizados pelos gestores acadêmicos e administrativos: Diretor-Presidente, Superintendente Geral, Diretor Acadêmico, Diretor Comercial, Diretor Administrativo e Financeiro, Diretor de Tecnologia da Informação, Secretária Acadêmica Geral, Assessoria Jurídica, Direção de Contabilidade, Coordenador de TI - Sistemas e Supervisor de TI - Infraestrutura.

Já do corpo discente, tivemos a participação do representante da pós-graduação (Lato Sensu) e do representante da graduação.

Destaca-se que todas as informações foram disponibilizadas pela instituição, a qual já havia realizado uma pesquisa interna sobre questões relacionadas ao entendimento dos colaboradores em relação à nova Lei Geral de Proteção de Dados.

Portanto a presente pesquisa é baseada em dados secundários já coletados para fins diferentes e em material de publicação, como livros, artigos ou relatórios. Não há acesso a informações pessoais identificáveis, os dados coletados foram disponibilizados anonimizados, portanto, a submissão ao comitê de ética não é necessária. Além disso, essa pesquisa não envolve a coleta de dados sensíveis ou informações que possam prejudicar os participantes ou a sociedade de alguma forma. Acreditamos que essa pesquisa está de acordo com os padrões éticos apropriados e garantirá resultados valiosos e úteis para a comunidade científica

Desta forma o estudo de caso se deu pela observação do ambiente, em paralelo com as informações disponibilizadas pela Instituição de Ensino Superior Privada (IES) e a literatura pesquisada.

# 7. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Com base na bibliografia utilizada para o desenvolvimento deste trabalho e na análise do ambiente, propomos um modelo teórico de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). Isso é motivado pelo fato de que a Instituição de Ensino Superior Privada ainda está em uma fase inicial de adequação à lei, que está em vigência desde 2020.

Consubstanciado pelo estudo de caso, observou-se que a gestão da Instituição de Ensino Superior (IES) tem conhecimento sobre a LGPD. No entanto, o entendimento sobre a importância da adequação a lei ainda é escasso ou ausente.

Foi possível identificar um nível maior de compreensão apenas com a direção de tecnologia e a assessoria jurídica, que mostraram consciência da importância de se adequar à lei e difundir sobre o assunto na IES, atribuindo-lhe a devida importância.

De forma geral, os dados fornecidos pela IES indicam que todos compreendem, em algum grau, que haverá impacto nas operações da instituição se não forem implementadas as adequações necessárias.

Essas adequações devem ser realizadas por meio de programas de *compliance* para alcançar os benefícios e evitar os prejuízos decorrentes da lei pois são vários os pontos que a operação da IES toca em relação a lei.

Durante o estudo de caso não foi possível identificar, na gerência acadêmica ou administrativa, a existência de algum projeto ou plano oficial de adequação da Instituição de Ensino Superior (IES) às normas da LGPD.

No resultado, com base nas informações recebidas pela Instituição de Ensino Superior (IES), observou-se que a consciência entre os *stakeholders* sobre a importância da Tecnologia da Informação (TI) como sustentáculo das atividades da instituição é unânime. Eles reconhecem que a TI é fundamental para o sucesso e a sustentabilidade de um programa de *compliance* de dados na IES.

Apesar de o grupo educacional contar com vinte anos de existência, verificou-se que há um estágio inicial de Governança de TI. Embora tenham sido feitos alguns investimentos em segurança, o estudo de caso destaca a necessidade de implementar mais ferramentas de gestão de TI na rede corporativa, para que as unidades do grupo e

o Centro Universitário possam se integrar sempre resguardando o acesso aos titulares dos dados e a segurança da informação.

Na compilação dos resultados, foram utilizadas, em alguns casos, a escala Likert com níveis de alta, razoável, baixa e nenhuma importância. Constatou-se que, entre as informações disponibilizadas pela IES, 70% dos dados indicam que os *stakeholders* possuem conhecimento razoável sobre a Lei Geral de Proteção de Dados Pessoais (LGPD) e, na mesma proporção, afirmam conhecer os impactos dessa lei.

Todavia, 90% dos stakeholders demonstrou conhecimento insuficiente e avaliado como baixo sobre a relevância, vantagens e desvantagens da legislação na Instituição de Ensino Superior (IES).

De outro lado, 100% dos envolvidos na operação da IES afirmaram, conforme os dados disponibilizados, que a instituição trata, em algum nível, dados pessoais dos estudantes, o que a coloca sujeita aos desígnios da lei. Entretanto, 60% desconheciam iniciativas oficiais de adequação à lei.

Quanto à gestão de governança de TI, as peculiaridades são evidentes. 100% dos envolvidos na operação da IES reconhecem a importância das estratégias de TI para as atividades da instituição e afirmam que a gestão de TI instrumentaliza a implementação de programas de *compliance* em geral na instituição.

Os dados coletados revelam que, se a TI não estiver bem estruturada e sem investimentos no setor, pode vulnerabilizar a instituição, e mostram que o ramo educacional é naturalmente exposto a riscos.

Portanto, os dados revelam que a TI representa 100% de importância para a estratégia de negócios da instituição, uma vez que é o subsídio para o bom funcionamento de todos os demais setores da IES. No entanto, no estudo de caso, não foi percebida a presença de programas de *compliance* e governança de TI na IES o que representou 70% de desconhecimento sobre a divulgação de Governança de TI.

Por tudo isto, destacamos um panorama muito aproximado do encontrado na literatura visitada e elaboramos então um quadro abaixo que relaciona os resultados obtidos nos dados disponibilizados pela Instituição de Ensino Superior (IES) através da pesquisa interna entre os *stakeholders* com a literatura visitada, demonstrando os fundamentos que são considerados, variáveis literárias, os resultados e a literatura visitada.

Tabela 1: Resumo dos resultados do estudo de caso

| Fundamento | Variáveis - Literatura | | Dados | Literatura visitada |
|---|---|---|---|---|
| Lei Geral de Proteção de Dados Pessoais Lei. 13.709/2018 | Conhecimento | Conhecimento | 70% Razoável | Lei n. 13.709, (2018); BIONI, (2021); DONEDA, (2020); PINHEIRO, (2021); ARTESE, (2021); CARVALHO, (2021); BARRETO, (2020); LIMA (2020); BERNARDES e DELATORRE (2008); BLUM (2021); CARVALHO, BERTOCCELLI, ALVIM, (2021); FLUMIGNAN S. e FLUMIGNAN W. (2020) SIMÃO FILHO (2019) PINHEIRO, (2021) MARINHO, (2020) |
| | | Compreensão dos Impactos | 70% Razoável | |
| | Importância | Relevância Vantagens e Desvantagens da LGPD na Instituição de Ensino Superior (IES). | 90% baixo | |
| | Conformidade | Instituição de Ensino Superior (IES) Manipula Dados | 100% sim | |
| | | Instituição de Ensino Superior (IES) Possui Plano de *Compliance* | 60% não | |
| Governança de TI | Relevância | Gestão de TI Importa | 100% sim | |
| | | TI vulnerabiliza a Instituição de Ensino Superior (IES) | 100% sim | |
| | Presença | Instituição de Ensino Superior (IES) Mais Exposta | 100% sim | |
| | | Instituição de Ensino Superior (IES) Possui Governança de TI | 70% não | |
| | Presença *Compliance* | Instituição de Ensino Superior (IES) apoia TI como estratégia de negócios | 100% sim | |
| | | Governança de TI dá suporte ao *Compliance* | 100% sim | |

Destacamos nos resultados alguns problemas encontrados que requerem atenção durante o processo de adequação à Lei Geral de Proteção de Dados (LGPD). Assim, observamos que a Instituição de Ensino Superior (IES) devido ao seu modelo de

negócio "B2C" (*Business to Consumer*), na qual a atividade envolve a coleta e tratamento de dados pessoais de seus clientes e potenciais clientes (titulares de dados pessoais).

Constatamos no estudo de caso que o setor comercial da instituição realiza campanhas publicitárias que arrecadam "*leads*" para prospectar fechamento de matrículas. Esses *leads*, geralmente, possuem dados pessoais como nome, telefone, endereço, entre outros, o que requer uma atenção especial para adequar a forma de coleta à lei, obtendo o consentimento explícito dos titulares de dados.

Outro ponto observado é a baixa compreensão da lei, apesar de ela estar em vigência desde 2020 e as adequações já deveriam estar implementadas ou em processo de implementação. Observamos que alguns gestores compreendem razoavelmente os impactos da LGPD.

Além disso, constatamos a inexistência oficial de programas de *compliance* para adequação à lei, a falta de práticas, rotinas e políticas de governança de TI na Instituição de Ensino Superior (IES) e a necessidade de divulgar essas políticas, apresentando os planos de investimentos e melhorias no setor.

Outro dado observado foi o potencial de riscos da operação da Instituição de Ensino Superior (IES), o que é provavelmente um dos pontos mais importantes para o desenvolvimento da atividade institucional. De acordo com os artigos 3º e 4º da LGPD, a lei se aplica a qualquer operação de tratamento realizada por pessoas naturais ou jurídicas, públicas ou privadas, independentemente do país de sua sede ou localização dos dados, desde que a operação ocorra no território nacional e tenha um objetivo econômico de lucro, oferecendo produtos ou serviços não artísticos, não acadêmicos, e/ou para fins de segurança pública, defesa nacional ou investigação.

Assim, a Instituição de Ensino Superior (IES) está exposta à lei, pois o tratamento de dados resulta da execução de sua atividade principal, que é a prestação de serviços educacionais enquanto o titular dos dados mantiver vínculo com a instituição e posteriormente, com a guarda de documentos pelo período legal. Os dados dos estudantes de graduação são os mais expostos, devido ao grande número de titulares envolvidos.

Importante destacar que outro fator de risco identificado pelos diagnósticos é a baixa compreensão da legislação de proteção de dados pessoais, e que a Instituição de Ensino Superior (IES) precisa se adequar.

Uma das nossas recomendações diante das observações é que seja implementada a realização de treinamentos direcionados a todas as partes envolvidas, desde a alta gestão até a ponta, para que sejam apresentados o conceito de privacidade de dados pessoais, os titulares de dados pessoais e seus direitos, de acordo com a Lei Geral de Proteção de Dados (LGPD), incluindo os impactos positivos e negativos de sua aplicação.

Os riscos percebidos na Instituição de Ensino Superior (IES) são resultantes da insuficiência de informações devido ao seu estágio embrionário de adequação. Por isso, foi elaborado um modelo conceitual preliminar antes de concluir o estudo de caso. Neste sentido, realizamos uma adequação ao modelo proposto anteriormente, para que a Instituição de Ensino Superior (IES) possa se adequar de forma mais realista à LGPD.

Após análise do ambiente na Instituição de Ensino Superior (IES), concluímos que é necessário realizar doze adequações baseadas na lei para alcançar a conformidade em proteção de dados pessoais.

O Quadro 4 representa a análise dos principais pontos de adequação à lei, com base nos resultados encontrados e na literatura de referência, para a construção do atual modelo.

**Quadro 5: Novo modelo de adequação da Instituição de Ensino Superior (IES)**

| **Adequações** | | | **Lei nº 13.709** |
|---|---|---|---|
| 1ª Fase | Inventário de Dados | Identificação do tipo de dados que a Instituição de Ensino Superior (IES) trata se é (pessoal, sensível, adolescente, público, anonimizado), em quais meios físico ou digital, operadores de dados internos e externos exibição de métricas de exposição da Instituição de Ensino Superior (IES) à LGPD | Art. 1°<br>Art. 2°<br>Art. 7° |
| 2ª Fase | Gerenciamento do Consentimento e Anonimização de dados pessoais | Instaurar mecanismos de adesão e controle do consentimento e assegurar se for o caso a anonimização em atendimento a requisição do titular e da ANPD. | Art. 5°<br>Art. 7° |
| 3ª Fase | Auditoria do Tratamento | Observância das atividades de tratamento de dados do art. 5º, inciso X aos princípios dispostos no Art. 6º da LGPD, por meio de controles rigorosos e instituição de controle interno para realização das auditorias implementado a revisão e criação de documentos necessários para adequação. | Art. 20<br>Art. 55 |

| | | | |
|---|---|---|---|
| 4ª Fase | Gerenciamento de Requisições dos Titulares | Criação e adequação de estruturas destinadas ao atendimento aos titulares de dados, e mecanismos de comunicação interna e externa, assim como promover a adequação do banco de dados de “leads” para controle de eventuais requisições dos titulares dos dados como o acesso aos dados, confirmação, anonimização, consentimento, portabilidade, entre outros | Art. 7° |
| 5ª Fase | Segurança dos Dados | Verificação, adequação e implementação de medidas de segurança e gestão de riscos, e governança de TI, para assegurar a proteção aos dados pessoais e planejamento de *compliance*.<br>Fase destinada a adoção de medidas técnicas ou administrativas de segurança de dados pessoais, a ocorrer desde a fase de o primeiro contato com o titular até o término do tratamento e armazenamento, ou seja, todo e qualquer serviço da instituição deve estar destinado a assegurar a privacidade de dados, realização de gestão de terceiros ou parceiros de negócios para adequar as ferramentas desenvolvidas por estes e utilizadas pela Instituição de Ensino Superior (IES) | Art. 11<br>Art. 47 |
| 6ª Fase | Relatório de Impacto à Proteção de Dados Pessoais | A Instituição de Ensino Superior (IES) deverá elaborar para atender as exigências da ANPD e outros órgãos, conforme disposição legal, que eventualmente requisite ao controlador o relatório | Art. 5°<br>Art. 9°<br>Art. 38 |
| 7ª Fase | Governança do Tratamento de Dados Pessoais | Implementação de regras de boas práticas e de governança que estabeleçam procedimentos, documentação e registro das adequações já realizadas, em curso ou a ser realizadas, elaboração ou adequação de documentos institucional para conformidade elaboração de relatório relacionado aos processos de tratamento de dados pessoais, riscos do tratamento aos titulares, desenvolvido sobre o resultado das fases anteriores, o relatório possibilita conhecer medidas e situações cabíveis e possíveis para cada risco de dados levantado possibilitando a mitigação de riscos no tratamento de dados pessoais | Capítulo IV<br>Seção I<br>Art. 43<br>Art. 45 |
| 8ª Fase | Comunicação de Incidente de Segurança | Elaboração de um plano de comunicação aos órgãos fiscalizatórios e à imprensa se for o caso sobre incidente de segurança que importe risco ou danos aos titulares dos dados | Art. 48 |

| | | | |
|---|---|---|---|
| 9ª Fase | Término do Tratamento | Adoção das medidas necessárias à eliminação de dados tratados, se for o caso aplicável, adequação para eventual conservação dos dados por necessidade legal com a elaboração de documentos que evidenciem a eliminação conforme determinação da lei | Art. 5° Art. 18 |
| 10ª Fase | Definição de um encarregado de dados (*Data Protection Officer*) | Implementar a figura do encarregado de dados seja pessoa física ou jurídica, com capacitação para exercer as atividades conforme a previsão legal | Art. 23 Capítulo VI Seção II |
| 11ª Fase | Certificação | Obter a certificação por entidade especializada nas práticas relacionadas à LGPD, para comprovar a garantia de observância aos princípios e direitos dos titulares. | Art. 33 Art. 35 |
| 12ª Fase | Perenidade e mediação de Conflitos | Monitoramento controle, treinamento e revisão de conformidade destinado manter a continuidade do programa de *compliance* na instituição com a comunicação dos contratos que envolvam o tratamento de dados de alunos de convênios Federais (Fies, Prouni) | Art. 26 |

Em resumo, os resultados apresentados são baseados em um estudo de caso desenvolvido por meio da observação das ações que foram implementadas ou que ainda serão implementadas, como no caso dos processos da secretaria acadêmica, para se adequarem às normas da Lei Geral de Proteção de Dados (LGPD), nos contratos de prestação de serviços educacionais, na captação de novos clientes, entre outros.

Ressalta-se que até a conclusão desta pesquisa, não foi identificada nenhuma ação substancial de adequação, exceto as já mencionadas, pois a Instituição de Ensino Superior (IES) ainda se encontra em estruturação da primeira fase do modelo proposto.

No entanto, após a realização da pesquisa, observou-se uma mudança comportamental da IES em relação aos resultados encontrados, resultando em uma mobilização para se organizar e implementar medidas para a adequação.

Diante desse estudo de caso, concluímos que a hipótese sugerida ao problema: “a Instituição Privada de Ensino Superior deverá observar os princípios de privacidade e proteção de dados pessoais e dados pessoais sensíveis no tratamento de dados dos estudantes, diante as inovações tecnológicas, empregando os meios necessários para efetivar a proteção dos dados dos pessoais sensíveis ou não dos estudantes, implementando técnicas de *compliance*, governança de TI ou outras formas adequadas de gestão para cumprir a legislação de proteção de dados.”, é verdadeira e

deve ser implementada de forma gradual, com monitoramento contínuo dos resultados e realinhamento das propostas, sempre buscando assegurar a privacidade dos dados estudantis.

Além disso, identificamos que os processos de matrícula e conclusão são possivelmente impactados pela adequação à lei, pois só devem ser utilizadas as informações indispensáveis para a prestação dos serviços, o que resultará em uma redução no número de documentos obrigatórios para a conclusão desses procedimentos.

Isso terá um impacto positivo, pois a redução de documentos pode resultar em uma redução no tempo de emissão dos diplomas, otimizando a execução dos trabalhos da secretaria.

O estudo de caso indica a necessidade de uma gestão adequada dos dados pessoais dos estudantes, para assegurar a privacidade dos mesmos e cumprir a legislação de proteção de dados comprovando a hipótese elaborada.

# 8. CONSIDERAÇÕES FINAIS

A relação entre as tecnologias computacionais e o mundo em que vivemos tem sido transformadora, mudando a forma como nos relacionamos e desempenhamos as atividades cotidianas. A evolução tecnológica impulsiona as organizações a procurarem constantemente novos métodos para aumentar a eficiência de seus processos, mas também aumenta a exposição aos riscos de violação e transgressão de direitos fundamentais.

Diversas nações estabeleceram regulamentações para equilibrar a evolução tecnológica, os meios de produção atuais e os direitos fundamentais dos indivíduos, como a privacidade e a proteção de dados pessoais, o exercício da autodeterminação informacional, entre outros.

Este trabalho teve como objetivo principal da pesquisa conhecer os esforços da Instituição de Ensino Superior Privada para se adequar à Lei Geral de Proteção de Dados (LGPD), com base em um estudo de caso, fundado na hipótese sugerida ao problema de: O que é necessário para a adequação da Instituição Privada de Ensino Superior para assegurar a proteção dos dados estudantis de acordo com o regramento da Lei Geral de Proteção de Dados? Com o objetivo de responder a esta questão, apresentamos uma proposta de um modelo conceitual, dividido em fases, para auxiliar neste processo de adequação.

A despeito da relativamente nova temática, sem um respaldo doutrinário tão robusto quanto outros temas, especialmente pela restritiva delimitação abordada e pela multidisciplinaridade, buscou-se uma revisão bibliográfica que abrangesse temas como os desafios de implementação da LGPD nas organizações, programas de *compliance*, *compliance* de dados pessoais, controle interno, governança de TI e a LGPD, gestão de documentos, entre outros.

Isso permitiu a idealização de algo que possibilitasse, pelo menos, direcionar a Instituição de Ensino Superior (IES) para um modelo de conformidade com a lei.

Os objetivos gerais e específicos propostos para este estudo foram atingidos. O objetivo geral era demonstrar que a LGPD impactará a gestão da Instituição de Ensino Superior (IES), que deverá estabelecer um plano de adequação, verificando as necessidades e os principais pontos de adequação. Além disso, o estudo buscou

demonstrar a necessidade de implementar modelos de governança de dados e designar um responsável pela fiscalização e processamento dos dados estudantis.

Os objetivos específicos propostos eram realizar uma pesquisa, usando como etapa inicial o processo de evolução da sociedade da informação, acompanhando a evolução tecnológica, o uso da internet e os dados pessoais. Abordar os conceitos e características dos direitos da personalidade, especificamente os direitos de privacidade.

Posteriormente, discorrer sobre a mudança na coleta e tratamento massivo de dados, conforme a evolução das legislações que serviram de base para a Lei Geral de Proteção de Dados (LGPD). Finalizando com a identificação dos desafios na adequação da LGPD nas Instituições de Ensino Superior (IES), com o objetivo de proteger os dados estudantis e destacar as opções para adequação.

Como contribuição, a pesquisa apresenta um modelo conceitual de adequação à LGPD que pode ser revisado, ampliado ou reduzido, sempre com o objetivo de efetivar a proteção de dados pessoais e manter o caráter de perenidade do programa de *compliance*.

Destacam-se benefícios da implementação desse modelo, como a perenidade do programa de *compliance*, o monitoramento contínuo dos resultados e a possibilidade de replicação em outras unidades do grupo educacional, com os ajustes necessários.

A presente pesquisa pretende contribuir para o meio científico, dada a escassa bibliografia sobre o tema, fornecendo uma compreensão mais aprofundada sobre o uso de dados pessoais e a proteção desses dados para os indivíduos. Além disso, a pesquisa busca ampliar a conscientização sobre a inviolabilidade da privacidade em qualquer meio, seja físico ou digital. Isso ajudará a direcionar as Instituições de Ensino Superior (IES) para a adequação no tratamento de dados estudantis, de acordo com a lei.

A pesquisa também tem suas limitações, já que se concentra apenas na compreensão da adequação dos dados estudantis. No entanto, o modelo proposto pode ser replicado em diversos setores de uma IES, desde que sejam feitas as adequações necessárias.

Ao avaliar a perspectiva da proteção de dados estudantis, foi possível identificar a necessidade de explorar dados com maior profundidade em outros setores relacionados às atividades empresariais. Isso abre a possibilidade de continuar a

pesquisa no futuro, desenvolvendo outros temas relacionados à proteção de dados em uma Instituição de Ensino Superior (IES) privada.

É importante destacar que há uma falta de pesquisas científicas sobre o tema no Brasil, o que torna a pesquisa ainda mais relevante.

Recomenda-se, assim, em uma futura pesquisa de maior amplitude, o implemento da metodologia de pesquisa intervencionista, possibilitando a concretização de contribuições práticas e teóricas ainda mais relevantes para o meio científico. Ao final do presente estudo, realizado com embasamento teórico e estudo de caso por meio de observação dos dados fornecidos pela instituição de ensino superior, pudemos concluir que a hipótese sugerida para investigação, de que a instituição privada de ensino superior deverá observar os princípios de privacidade, proteção de dados pessoais e dados pessoais sensíveis no tratamento de dados dos estudantes, diante às inovações tecnológicas, empregando os meios necessários para efetivar a proteção dos dados pessoais sensíveis ou não dos estudantes, implementar técnicas de *compliance*, governança da Tecnologia da Informação (TI) ou outras formas adequadas de gestão para cumprir a legislação de proteção de dados, como já demonstrado na discussão dos resultados, é verdadeira e os procedimentos atuais necessitam de revisão e adequação às normas da Lei Geral de Proteção de Dados (LGPD).

# REFERÊNCIAS


ABBOUD, Georges; CARNIO, Henrique Garbellini; OLIVEIRA, Rafael Tomaz de. **Introdução ao Direito:** teoria, filosofia e sociologia do direito. 5. ed. São Paulo: Thomson Reuters Brasil, 2020.

ABREU, Jacqueline de Souza; **Tratamento de Dados Pessoais Para Segurança Pública:** Contornos do Regime Jurídico Pós-LGPD *in* BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Grupo GEN, 2020. 9788530992200. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 12 jan. 2022.

Associação Brasileira de Mantenedoras de Ensino Superior - ABMES, **SEMINÁRIO ABMES | ENTENDENDO A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): COMO PREPARAR SUA IES** disponível em https://abmes.org.br/audios/detalhe/532. Acesso em 17 dez. 2022.

ALEMANHHA. Tribunal Constitucional Federal. **Resumo da sentença do Tribunal Constitucional Federal Alemão de 15 de dezembro de 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CÓDIGOS]**. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html;jsessionid=CFBE0153659904890C268B9052A502A7.2_cid386. Acesso em: 07 set. 2021.

AMARAL, Claudio de Prado; **Proteção de Dados Pessoais de Crianças e de Adolescentes** *in* LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados. Grupo Almedina (Portugal), 2020. E-book. 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 17 mai. 2022.

ARTESE, Gustavo. ***Compliance* digital e privacidade.** *In*: CARVALHO, André C.; BERTOCCELLI, Rodrigo de P.; ALVIM, Tiago C.; AL, et**.** Manual de *Compliance*. Grupo GEN, 2021. E-book. 9786559640898. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559640898/. Acesso em: 1 ago. 2022.

ARQUIVO NACIONAL (Brasil). **Dicionário Brasileiro de Terminologia Arquivística**. Rio de Janeiro, 2005. E-book. Disponível em: https://simagestao.com.br/wp-content/uploads/2016/01/Dicionario-de-terminologia-arquivistica.pdf. Acesso em: 10 ago. 2022.

BARRETO, Mauricio L.; ALMEIDA, Bethânia; DONEDA, Danilo; **Uso e Proteção de Dados Pessoais na Pesquisa Científica** *in* BIONI, Bruno. Tratado de Proteção de Dados Pessoais; Grupo GEN, 2020. 9788530992200. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 14 jan. 2022.

BENACCHIO, Marcelo; MACIEL, Renata Mota**; A LGPD sob a Perspectiva da Regulação do Poder Econômico** *in* LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados. Grupo Almedina (Portugal), 2020. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 22 jan. 2022.

BERNARDES, Ieda Pimenta. **Como avaliar documento de arquivo**. São Paulo: Arquivo do Estado Imprensa Oficial, 1998. E-book. Disponível em: https://www.arqsp.org.br/arquivos/oficinas_colecao_como_fazer/cf1.pdf. Acesso em: 12 ago. 2022.

BERNARDES, Ieda Pimenta; DELATORRE, Hilda. **Gestão Documental Aplicada**. São Paulo: Arquivo Público do Estado de São Paulo, 2008. E-book. Disponível em: http://www.arquivoestado.sp.gov.br/site/assets/publicacao/anexo/gestao_documental_aplicada.pdf. Acesso em: 15 ago. 2022.

BIONI, Bruno R. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. Grupo GEN, 2021. 9788530994105. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994105/. Acesso em: 25 jan 2022.

_____. **Tratado de Proteção de Dados Pessoais**. Grupo GEN, 2020. 9788530992200. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 20 mar. 2022

BLUM, Rita Peixoto Ferreira; MORAES, Hélio Ferreira. **Lei Geral de Proteção de Dados Pessoais** in CARVALHO, André C.; BERTOCCELLI, Rodrigo de P.; ALVIM, Tiago C.; et al. Manual de *Compliance*. Grupo GEN, 2021. E-book. 9786559640898. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559640898/. Acesso em: 22 ago. 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituiçãocompilado.htm. Acesso em: 01 jul. 2021.

_____. Lei nº 8.078, de 11 de setembro de 1990. **Código de defesa do consumidor.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 nov. 2021.

_____. Lei nº 10.406, de 10 de janeiro de 2002. **Código civil**. Diário Oficial da União, seção 1, Brasília, DF, a. 139, n. 8, p. 1-74, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/CCivil_03/leis/2002/L10406.htm. Acesso em: 01 jul. 2021.

_____. Lei nº 12.414, de 09 de junho de 2011. **Lei do cadastro positivo.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm. Acesso em: 10 nov. 2021.

_____. Lei nº 12.965, de 23 de abril de 2014. **Marco civil da internet.** Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 nov. 2020.

_____. Lei nº 13.709, de 14 de agosto de 2018. **Lei geral de proteção de dados pessoais (LGPD).** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 jul. 2021.

_____. **Lei nº 13.853**, de 08 de julho de 2019. Brasília, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 02 jul. 2021

_____. Senado Federal. **Proposta de emenda à constituição n° 17, de 2019**. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. De autoria do Senador Eduardo Gomes (MDB/TO) (1º signatário) et al. Parte integrante do Avulso da PEC nº 17 de 2019. 2019a. Disponível em: https://legis.senado.leg.br/sdleggetter/documento?dm=7925004&ts=1606766520897&disposition=inline. Acesso em: 15 set. 2021.

CARVALHO, André C.; BERTOCCELLI, Rodrigo de P.; ALVIM, Tiago C.; et al**. Manual de *Compliance***. Grupo GEN, 2021. E-book. 9786559640898. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559640898/. Acesso em: 1 ago. 2022.

CASTELLS, Manuel. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. Tradução, Maria Luiza X. de A. Borges; revisão técnica, Paulo Vaz.

_____. **A Sociedade em Rede: a era da informação:** economia, sociedade e cultura. 20. ed. revisada e ampliada São Paulo: Paz e Terra, 2019: Jussara Simões - Tradução Roneide Venancio Majer.

CONSELHO DA EUROPA (DdE). **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.** European Treaty Series. n. 108, Strasbourg, 28.I. 1981. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37. Acesso em 10 set. 2021.

COSTA, R. S.; OLIVEIRA, S. R. **Os direitos da personalidade frente à sociedade de vigilância:** privacidade, proteção de dados pessoais e consentimento nas redes sociais. Revista Brasileira de Direito Civil em Perspectiva | e-ISSN: 2526-0243 | Belém | v. 5 | n. 2 |p. 22 - 41| Jul/dez. 2019.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada.** [livro eletrônico] 4. ed. rev. atual. E ampl. São Paulo: Thomson Reuters Brasil, 2021.

DAVENPORT, Thomas H. **Ecologia da informação:** por que só a tecnologia não basta para sucesso na era da informação. São Paulo: Futura, 2000.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental.** Espaço Jurídico de Direito. Joaçaba, v.12, n.2, p.91-108, jul.-dez. 2011. Disponível em: https://dialnet.unirioja.es/revista/12418/A/2011. Acesso em: 01 jul. 2020.

DONEDA, Danilo; MENDES, Laura Schertel. **Reflexões iniciais sobre a nova lei de proteção de dados.** Revista de Direito do Consumidor, São Paulo, v. 120, p. 472, nov./dez. 2018. Disponível em: https://www.academia.edu/42741127/Reflex%C3%B5es_iniciais_sobre_a_nova_lei_geral_de_prote%C3%A7%C3%A3o_de_dados?auto=download. Acesso em 12 jan. 2022.

_____. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters Brasil, 2019.

_____. **Privacidade e transparência no acesso à informação pública**. In: Democracia eletrônica. MEZZAROBA, Oribes; GALINDO, Fernando. Espanha (Zaragoza): Prenzas Universitarias de Zaragoza, 2010.

FRAZÃO, Ana. **Objetivos e alcance da lei geral de proteção de dados**. *in*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil. 2019. p. 47

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. ***Compliance* de dados pessoais.** *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. p. 372.

FLUMIGNAN, Silvano José Gomes; FLUMIGNAN, Wévertton Gabriel Gomes; **Princípios que Regem o Tratamento de Dados no Brasil** *in*: LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados. Grupo Almedina (Portugal), 2020. 9788584935796. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em

GUIDI, Guilherme Berti de Campos. **O papel do consentimento para a proteção de dados pessoais**: União Europeia, Estados Unidos e Brasil. Direito internacional em expansão. v. XVI. Belo Horizonte: Arraes Editores, 2019. ISBN: 978-858238-642-2.

GROSSI, Bernardo Menicucci (Org.) **Lei Geral de Proteção de Dados:** Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial. Porto Alegre: Fi, 2020.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

HESSE, Konrad. **Temas fundamentais do direito constitucional**. São Paulo: Saraiva, 2009.

HORNUNG, Gerrit; SCHNABEL, Christoph. **Data protection in Germany I:** The population census decision and the right to informational self-determination. Computer

Law & Security Report. v. 25, n. 1, 2009. Disponível em: https://www.uni-kassel.de/fb07/fileadmin/datas/fb07/5nstitute/IWR/Hornung/Hornung___Schnabel__Data_protection_in_Germany_I__CLSR_2009__84.pdf. Acesso em: 08 set. 2021.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA – IBGE. **PNAD contínua**. 2020. Disponível em: https://www.ibge.gov.br/estatisticas/sociais/trabalho/17270-pnadcontinua.html?=&t=o-que-e. Acesso em: 01 jun. 2021.

KAISER, Brittany. **Manipulados:** como a cambridge analytica e o facebook invadiram a privacidade de milhões e botaram a democracia em xeque. Tradução Roberta Clapp, Bruno Fiuza. Rio de Janeiro: Harper Collins, 2020.

KONDER, Carlos Nelson. **O tratamento de dados sensíveis à luz da lei nº 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.

LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de informação**. 4. ed. Rio de Janeiro: LTC, 1999.

LEONARDI, Marcel. **Principais Bases Legais de Tratamento de Dados Pessoais no Setor Privado** *in* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (org.). Direito e Internet IV: sistema de proteção de dados pessoais (de acordo com a lei nº 13.709, de 14 de agosto de 2018, e a lei 13.853, de 08 de julho de 2019, que converteu em lei a medida provisória nº 869, de 27 de dezembro de 2018). São Paulo: Quartier Latin, 2019.

LIMA, Cíntia Rosa Pereira D. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados.** Grupo Almedina (Portugal), 2020. 9788584936397. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 10 jan. 2022.

_____. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. 9788584935796. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 11 jan. 2022.

_____. **Sistemas de informação Gerenciais**. 9. ed. Rio de Janeiro: LTC, 2011.
LIMA, Ana Paula Moraes Canto D. LGPD Aplicada. Grupo GEN, 2021. 9788597026931. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026931/. Acesso em: 11 jan. 2022.

LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (org.). **Direito e Internet IV:** sistema de proteção de dados pessoais (de acordo com a lei nº 13.709, de 14 de agosto de 2018, e a lei 13.853, de 08 de julho de 2019, que converteu em lei a medida provisória nº 869, de 27 de dezembro de 2018). São Paulo: Quartier Latin, 2019.

MARCACINI, Augusto Tavares Rosa. Regras Aplicadas ao Tratamento de Dados Pessoais. *in* LIMA, Cíntia Rosa Pereira D. **Comentários à Lei Geral de Proteção de Dados**. Grupo Almedina (Portugal), 2020. 9788584935796. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 15 mai. 2022.

MARINHO, Fernando. **Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos**. Grupo GEN, 2020. E-book. 9788597026009. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026009/. Acesso em: 14 ago. 2022.

MARTINELLI, Dante P. **Teoria Geral dos Sistemas**. Editora Saraiva, 2012. 9788502180390. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502180390/. Acesso em: 10 mai. 2022.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. **Quando a lei geral de proteção de dados não se aplica.** 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.

MENDES, Gilmar F.; BRANCO, Paulo Gustavo G. **SÉRIE IDP - CURSO DE DIREITO CONSTITUCIONAL**. Editora Saraiva, 2021. 9786555593952. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555593952/. Acesso em: 14 abr. 2021.

_____. **Direitos fundamentais:** eficácia das garantias constitucionais nas relações privadas. In: GRUNDMANN, Stefan et al. Direito privado, constituição e fronteiras, 2. ed. São Paulo: Revista dos Tribunais, 2014.

MENDES, Laura Schertel. **Habeas data e autodeterminação informativa: os dois lados da mesma moeda**. Revista Direitos Fundamentais & Justiça. Belo Horizonte, ano 12, n. 39. 2018.

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

MICHEL, Maria H**. Metodologia e Pesquisa Científica em Ciências Sociais**, 3ª edição. Grupo GEN, 2015. E-book. 978-85-970-0359-8. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/978-85-970-0359-8/. Acesso em: 10 jan. 2022.

NAVARRO, Ana Maria Neves de Paiva. **O direito fundamental à autodeterminação informativa**. Laboratório de Estudos Teóricos e Analíticos sobre o Comportamento das Instituições (LETACI), vinculado à Faculdade Nacional e ao Programa de Pós-Graduação em Direito da Universidade Federal do Rio de Janeiro, com financiamento da Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) pela concorrência do Edital nº 9 de 2011 (Processo nº E26/111.832/2011), e do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pela

concorrência do Edital Universal de 14/2011 (Processo n° 480729/2011-5) Disponível em: http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c. Acesso em 11 nov. 2021.

OLIVEIRA, Ana Paula de; ZANETTI, Dânton. **A lei geral de proteção de dados brasileira na prática empresarial.** Revista Jurídica da Escola Superior de Advocacia da OAB-PR. ano 4,n. 1. mai. 2019. Disponível em: http://revistajuridica.esa.oabpr.org.br/wpcontent/uploads/2019/05/revista-esa-cap-08.pdf. Acesso em: 01 jun. 2020.

ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf . Acesso em: 9 jun. 2021.

OECD **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.** Elaboração: André-Pascal. França: OECD Publications Service, 2011. p. 3 2 . The OECD Privacy Framework 2013. p. 3-5 (prefácio). Disponível em: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. Acesso em: 18 julho. 2021

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil. 6. ed. São Paulo: Atlas, 2013.

PARLAMENTO EUROPEU. **Carta dos Direitos Fundamentais da União Europeia**. Jornal Oficial das Comunidades Europeias. 18.02.200. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 20 set. 2021.

_____. **Directiva 95/46/CE do Parlamento Europeu e do Conselho**, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial nº L 281 de 23/11/1995 p. 0031 –0050, 1995.

_____ **Directiva 2002/58/CE do Parlamento Europeu e do Conselho**, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas). Jornal Oficial nº L 201 de 31/07/2002, p. 0037 – 0047, 2002.

_____. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.** de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 15 set. 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). Editora Saraiva, 2021. 9786555595123. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 09 março. 2022.

PINHEIRO, Patrícia Peck. **Direito Digital.** Editora Saraiva, 2021. E-book. 9786555598438. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 10 ago. 2022.

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese. **A proteção de dados pessoais na internet no brasil: análise de decisões proferidas pelo Supremo Tribunal Federal**. Revista Cadernos do Programa de Pós-Graduação em Direito PPGDir./UFRGS. v.11, n.2, 2016. Disponível em: http://seer.ufrgs.br/ppgdir/article/view/61960/39936. Acesso em 01 jun. 2021.

RAMIRO, Mônica Arenas. **El derecho fundamental a la protección de datos personales em Europa.** Valencia: Tirant la blanch, 2006.

REINHARDT. Jörn. **Conflitos de direitos fundamentais entre atores privados**: "efeitos horizontais indiretos" e pressupostos de proteção de direitos fundamentais. Belo Horizonte, ano 13, n. 41, p. 59-91, jul.-dez. 2019. Disponível em: http://dfj.emnuvens.com.br/dfj/article/view/819. Acesso em 01 out. 2021.

RUARO Regina Linden; RODRIGUEZ Daniel Piñeiro; FINGER Brunize**. O direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de Direito-UFPR, Curitiba, n. 53, 2011. Disponível em: https://revistas.ufpr.br/direito/article/view/30768/19876. Acesso em: 01 jul. 2021.

SARLET, Gabrielle Bezerra Sales. **Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro** *in* LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados. Grupo Almedina (Portugal), 2020. 9788584935796. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 14 jan. 2022.

SARLET, Ingo Wolfgang. **A Eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. rev. e atual. Porto Alegre: Livraria do Advogado Editora, 2018.

_____. **Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Revista Direitos Fundamentais & Justiça. Belo Horizonte, ano 14, n. 42, 2020.

SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. 2. ed. Rio de Janeiro: Lumen Juris, 2006.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** uma visão executiva. 2ª ed. Rio de Janeiro: Campus, 2014.

SCHWABE, Jürgen *et al* (org.). **Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad-Adenauer-Stiftung, 2005. 993 p. Tradução de: Beatriz Hennig; Leonardo Martins (Org.); Mariana Bigelli de Carvalho; Tereza Maria de Castro; Vivianne Geraldes Ferreira.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 25. ed. rev. e atual. São Paulo: Malheiros Editores, 2005.

SIMÃO FILHO, Adalberto; **A Governança Corporativa Aplicada às Boas Práticas e *Compliance* na Segurança dos Dados** *in* LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados. Grupo Almedina (Portugal), 2020. E-book. 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 22 ago. 2022.

SIMÃO FILHO, Adalberto; **Regime Jurídico do Banco de Dados – Função Econômica e Reflexos na Monetização**; *in* LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (org.). Direito e Internet IV: sistema de proteção de dados pessoais (de acordo com a lei nº 13.709, de 14 de agosto de 2018, e a lei 13.853, de 08 de julho de 2019, que converteu em lei a medida provisória nº 869, de 27 de dezembro de 2018). São Paulo: Quartier Latin, 2019.

TEPEDINO, Gustavo; TERRA, Aline de Miranda V.; GUEDES, Gisela Sampaio da C. **Fundamentos do Direito Civil: Responsabilidade** Civil. v.4. Grupo GEN, 2022. E-book. 9786559643967. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559643967/. Acesso em: 1 mai. 2022.

TEPEDINO, Gustavo; FRAZÃO, A.; OLIVA, M. D. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

TEIXEIRA, Tarcísio; ARMELIN, Ruth Maria G. F. **Responsabilidade e Ressarcimento de Danos por Violação às Regras Previstas na LGPD**: um Cotejamento com o CDC *in* LIMA, Cíntia Rosa Pereira D. Comentários à Lei Geral de Proteção de Dados: Grupo Almedina (Portugal), 2020. E-book. 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 22 ago. 2022.

VERGILI. Gabriela Machado. **Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados**. Dataprivacy. Artigos 18.09.2019, 2019. Disponível em: https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-aprotecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geralde-protecao-de-dados/. Acesso em: 05 jan. 2021.

VILELA, C. M. M *in* LIMA, Ana Paula Moraes Canto D. **LGPD Aplicada**. Grupo GEN, 2021. 9788597026931. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026931/. Acesso em: 11 jan. 2022.

# APÊNDICES

**APÊNDICE A - Termo de Anuência para pesquisa**

GRUPO FASIPE EDUCACIONAL

**TERMO DE ANUÊNCIA PARA PESQUISA E ESTUDO DE CASO**

Eu, Deivison Benedito Campos Pinto, diretor presidente, responsável pelo Grupo Unifasipe, tenho ciência e **AUTORIZO** a realização da pesquisa intitulada "**SISTEMA PROTETIVO DOS DADOS ESTUDANTIS - A (IN)APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NAS INSTITUIÇÕES PRIVADAS DE ENSINO SUPERIOR**" a ser realizada pelo mestrando José Jander Dias Ferreira Junior, sob a orientação do Prof. Dr. Adalberto Simão Filho, vinculada à Universidade de Ribeirão Preto (UNAERP), com o seguinte objetivo geral: Demonstrar que a LGPD impactará a Gestão da IES que deverá estabelecer um plano de adequação, verificando as necessidades e os principais pontos de atenção e adequação.

Estou Ciente que os dados coletados serão mantidos em absoluto sigilo e anonimizados de acordo com a lei 13.709/2018, (Lei Geral de Proteção de Dados) e que tais dados serão utilizados exclusivamente para realização deste estudo com a consequente publicação da dissertação final.

Por fim, compreendo que este projeto não implicará em qualquer tipo de ônus para os participantes da pesquisa e para o Centro Universitário Unifasipe.

Rondonópolis, 08 de setembro de 2020.

**Deivison Benedito Campos Pinto**

**Diretor Presidente**

## APÊNDICE B – Tabulação dos Dados Encontrados

| DIREÇÃO ÓRGÃOS DE APOIO ACADÊMICO E ÓRGÃOS SUPLEMENTARES | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Váriaveis Observáveis – LGPD (13.709/2018) | | | | | | Váriaveis Observáveis – Governança de TI | | | | | |
| Dados Setorizados Disponibilizados | Conhece | IES opera dados pessoais | Compreende os Impactos da Lei | Entende os beneficios e prejuizos | Compliance ou Iniciativas para adequar | Valor da TI na operação | TI Vulnerabiliza a IES | IES mais exposta a risco | IES detém Gov. TI IES divulga Gov. TI | Importância das Estratégias de TI | Gov. TI apoia Compliance |
| DO1 | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim |
| DO2 | Parcial[4] | Sim | Não | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO3 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO4 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO5 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO6 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO7 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO8 | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim | Sim |
| DO9 | Parcial[4] | Sim | Não | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO10 | Parcial[4] | Sim | Parcial[3] | Parcial[4] | Não sabe | Sim | Sim | Sim | Sim | Sim | Sim |
| DO11 | Parcial[4] | Sim | Parcial[3] | Parcial[4] | Não sabe | Sim | Sim | Parcial[3] | Parcial[4] | Sim | Sim |
| DO12 | Sim | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO13 | Parcial[4] | Sim | Parcial[3] | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO14 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO15 | Não | Sim | Não | Não | Não sabe | Sim | Sim | Parcial[3] | Parcial[4] | Sim | Sim |
| DO16 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO17 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[4] | Sim | Sim |
| DO18 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[3] | Sim | Sim |
| DO19 | Parcial[3] | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[3] | Sim | Sim |
| DO20 | Sim | Sim | Sim | Parcial[4] | Não sabe | Sim | Sim | Sim | Parcial[3] | Sim | Sim |
| | 70% | 100% | 70% | 90% | 60% | 100% | 100% | 100% | 70% | 100% | 100% |

Nota: 1. Parcial[3] ≥ (maior ou igual a sim); 2. Parcial[4] ≤ (menor ou igual a não)

**APÊNDICE C – PDI Centro Universitário pesquisado**

**Mantida pela FASIPE CENTRO EDUCACIONAL LTDA.**
Credenciada pela Portaria MEC nº1.175 de 05/12/2007, publicada no DOU de06/12/2007. Recredenciada pela Portaria MEC nº 1.972, de 8 de novembro de 2019, publicada no Diário Oficial da União, de 11 de novembro de 2019, fica credenciado o Centro Universitário Fasipe, por transformação da Faculdade Fasipe.

**FASIPE CENTRO EDUCACIONAL LTDA.**
**Mantenedora**

**CENTRO UNIVERSITÁRIO FASIPE**
**Mantida**

# PLANO DE DESENVOLVIMENTO INSTITUCIONAL

**PERÍODO DE VIGÊNCIA 2020/2024**

**SINOP / MATO GROSSO**

**REITORIA**

**Deivison Benedito Campos Pinto**
Reitor

**Adriano Marcos Rodrigues**
Vice-Reitor

**Alan Murilo da Silva**
Pró-Reitoria de Ensino, Iniciação Científica, Extensão e Pós-Graduação

**Francisco Fabio Soares**
Pró-Reitoria Financeira

**Claudia Wohnrath**
Pró-Reitoria Administrativa

**Bruno Rodrigues dos Santos**
Diretor Acadêmico – Unidade Aquarela das Artes

**SINOP / MATO GROSSO**

PLANO DE DESENVOLVIMENTO INSTITUCIONAL – PDI

CENTRO UNIFASITÁRIO FASIPE
2020/2024

SUMÁRIO