e-ISSN: 2177-8183

# MARCO CIVIL DA INTERNET E LEI GERAL DE PROTEÇÃO DE DADOS NO ENSINO SUPERIOR

# CIVIL RIGHTS FRAMEWORK FOR THE INTERNET AND GENERAL DATA PROTECTION LAW IN HIGHER EDUCATION

# MARCO CIVIL DE INTERNET Y LEY GENERAL DE PROTECCIÓN DE DATOS EN LA EDUCACIÓN SUPERIOR

*João Marcos Heggler*
joaoheggler@utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Doutorando - PPGECTD-PG

*Romeu Miqueias Szmoski*
rmszmoski@utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Professor Dr. - PPGECTD-PG

*Awdry Feiser Miquelin*
awdry@utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Professor Dr. - PPGECTD-PG

*Sani de Carvalho Rutz da Silva*
sani@utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Professora Dra. - PPGECTD-PG

Alessandra Dutra
alessandradutra@utfpr.edu.br
Universidade Tecnológica Federal do Paraná
Professora Dra. - PPGECTD-PG

## RESUMO

O presente artigo tem como objetivo discutir a respeito do cumprimento do Marco Civil da *Internet* (MCI) e da Lei Geral de Proteção de Dados (LGPD) em ambientes acadêmicos. A pesquisa se caracteriza como exploratória, qualitativa e interpretativa, com apoio bibliométrico. Para a análise e interpretação do *corpus* da pesquisa, fizemos a utilização da análise de conteúdo, com a apresentação dos principais aspectos legais do MCI e da LGPD, no âmbito da educação que orientam a busca de artigos e que compõem o panorama de pesquisas, obtido nas bases *Scopus e Web of Science* com a seleção final para a análise de 10 artigos relativos à proteção e à segurança de dados pessoais no contexto educacional. Destaca-se a responsabilidade das instituições de ensino em relação ao adequado tratamento de dados pessoais digitais e físicos dos usuários. A investigação revelou uma escassez de publicações a respeito do cumprimento do MCI e da LGPD nos ambientes educacionais, principalmente em relação ao MCI. Os resultados apontam que, embora o

e-ISSN: 2177-8183

MCI e a LGPD estabeleçam dispositivos específicos e abrangentes para a proteção das informações e dos dados, a sua aplicação prática ainda enfrenta desafios; além da necessidade de conscientização, treinamento dos profissionais e implementação de protocolos de segurança robustos e abrangentes. Conclui-se que a efetivação dessas leis, de políticas de segurança e de privacidade, é fundamental para vislumbrar a proteção de dados dos estudantes e demais usuários, possibilitando um ambiente acadêmico mais seguro e confiável.

**Palavras-chave**: MCI. LGPD. Segurança Digital. Ensino Superior.

## ABSTRACT

Thisarticleaimstodiscuss compliance withthe Civil Rights Framework for the Internet (MCI) andthe General Data Protection Law (LGPD) in academicenvironments. The researchisexploratory, qualitative, interpretative, andbibliometric. Content analysis wasusedtoanalyzeandinterpretthe research corpus. The main legal aspects of the MCI and LGPD in thefield of education are presented, whichguidethesearch for articlesthat make upthestudies overview obtainedfromthe Scopus and Web of Science databases, with a final selection of 10 articlesrelatingtotheprotectionandsecurity of personal data in theeducationalcontext. The responsibility of educationalinstitutions in relationtothepropertreatment of users' digital andphysical personal data ishighlighted. The investigationrevealed a scarcity of publicationsregarding compliance withthe MCI and LGPD in educationalenvironments, especially in relationtothe MCI. The resultsindicatethat, althoughthe MCI and LGPD establishspecificand comprehensive provisions for theprotection of informationand data, theirpracticalapplication still faces challenges, in additiontotheneed for awareness, training of professionals, andimplementation of robustand comprehensive securityprotocols. It isconcludedthattheenforcement of theselaws, security policies, andprivacy policies isessentialtoensuretheprotection of studentandotheruser data, enabling a saferand more reliableacademicenvironment.

**Keywords:**MCI. LGPD. Digital Security. Higher Education.

## RESUMEN

El presente artículo tiene como objetivo discutir elcumplimientodel Marco Civil de Internet (MCI) y laLey General de Protección de Datos (LGPD) en entornos académicos. La investigación se caracteriza por ser exploratoria, cualitativa, interpretativa y conapoyo bibliométrico. Para elanálisis y lainterpretacióndel corpus de lainvestigación se utiliza elanálisis de contenido. Se presentanlosprincipales aspectos legalesdel MCI y la LGPD enelámbito de laeducación que orientanlabúsqueda de artículos que conformanel panorama bibliográfico obtenido de las bases de datos Scopus y Web of Science, conlaselección final para elanálisis de 10 artículos relativo a la protección y seguridad de los datos personales en el contexto educativo. Cabe destacar laresponsabilidad de lasinstituciones educativas enrelaciónconeltratamientoadecuado de losdatospersonalesdigitales y físicos de losusuarios. La investigaciónreveló una escasez de publicaciones sobre elcumplimientodel MCI y la LGPD enlos entornos educativos, especialmente enrelaciónconel MCI. Los resultados indican que, aunqueel MCI y la LGPD establecendisposiciones específicas y exhaustivas para laprotección de lainformación y losdatos,

e-ISSN: 2177-8183

suaplicaciónprácticasigueenfrentando retos, además de lanecesidad de sensibilización, formación de losprofesionales e implementación de protocolos de seguridad sólidos y exhaustivos. Se concluye que laaplicaciónefectiva de estas leyes y de las políticas de seguridad y privacidad es fundamental para garantizarlaprotección de losdatos de losestudiantes y demásusuarios, lo que permite un entorno académico más seguro y confiable.

**Palabras clave:** MCI. LGPD. Seguridad Digital. Educación Superior.

## INTRODUÇÃO

A *internet* é um mundo de possibilidades, encurtando virtualmente as distâncias, aproximando as pessoas e intensificando as inter-relações; se tornando indispensável para o cotidiano das atividades da sociedade, para o desenvolvimento tecnológico e o consequente tráfego de arquivos e informações. Por isso, é inevitável o compartilhamento constante de dados dos usuários e uma dependência tecnológica, até mesmo, para as tarefas mais simples. Neste sentido, a sua utilização precisa ser monitorada e regulamentada.

Além disso, o uso crescente da *web* faz com que o volume de acessos às redes seja intenso e os dados pessoais acabem expostos e eventualmente invadidos e subtraídos. Os cuidados, a precaução com a segurança e a privacidade desses dados podem ser desprezadas ou não receberem a devida importância e valoração, podendo acarretar em condutas e práticas inadequadas, descuidadas, danosas ou criminosas por parte de terceiros em relação à invasão desses dados, impactando negativamente o cotidiano pessoal, social, profissional e educacional das pessoas.

Juntamente com os avanços das tecnologias digitais, também surgem algumas preocupações dos legisladores, desenvolvedores, pesquisadores e gestores educacionais em relação à necessidade de investigar, criar estratégias e buscar soluções para tentar garantir a segurança e a proteção aos dados, pois a privacidade desses dados é um bem pessoal extremamente valioso, que precisa ser preservado. No Brasil, essa preocupação está bastante presente em razão da

massiva utilização da *internet*, refletindo-se na urgência de criação e na efetivação de regulamentações para o acesso, tratamento, armazenamento, compartilhamento e uso das informações privadas e pessoais. De acordo com a LGPD, tratamento de dados significa:

> 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 (Brasil, 2018).

Nesta perspectiva, embora a Constituição da República Federativa do Brasil de 1988 (CF/1988) tenha estabelecido determinados direitos, deveres e garantias fundamentais visando à proteção, a inviolabilidade da intimidade e da vida privada, sigilo das correspondências e das comunicações dos indivíduos (Brasil, 1988), o país não dispunha em seu ordenamento jurídico de um rol de regulamentos específicos e detalhados para a proteção de dados pessoais físicos e digitais (Cardoso; Régis, 2024).

Visando suprir essa lacuna legal foi promulgada, em 2014, a Lei 12.965, também conhecida como MCI, estabelecendo: princípios; garantias; direitos e deveres sobre o uso da *internet* no Brasil, assim como a Lei n° 13.709/2018, popularmente chamada de LGPD,compreendida como um instrumento legal extremamente importante e necessário para as instituições, organizações e pessoas, visando à proteção dos dados pessoais e a regulamentação da garantia dos direitos de privacidade, liberdade e desenvolvimento da personalidade dos indivíduos (Brasil, 2014; 2018).

A relevância do MCI e da LGPD no contexto da proteção e da segurança de dados não significa apenas a evolução das regulamentações dessas matérias legais, mas uma realidade frente às incertezas surgidas em torno dos riscos e desafios que ameaçam a proteção de dados dos usuários. Surge, então, a necessidade de adaptação dos indivíduos, das organizações e das instituições de ensino a esse novo cenário de proteção em âmbito nacional e de constatação da importância do respeito às determinações legais no sentido de se evitar certas penalizações (Lugati; Almeida, 2022).

e-ISSN: 2177-8183

No âmbito educacional, a segurança digital é fundamental para proteger os dados pessoais dos alunos, dos professores, dos profissionais da educação e demais usuários; envolvendo a coleta de dados pessoais, dados cadastrais, registros escolares e acadêmicos, além das consultas públicas. As instituições públicas e privadas de ensino têm a incumbência de garantir que esses dados sejam tratados com transparência e segurança de acordo com as regras estabelecidas. As leis em vigor, mais as possibilidades de responsabilização de terceiros, tanto na esfera pública como na esfera privada permitem vislumbrar certa confiança no ambiente educacional no que tange à coleta, tratamento, processamento, armazenamento e compartilhamento de dados.

Apesar do MCI e da LGPG serem duas leis relativamente conhecidas considerando as suas datas de publicações, esta pesquisa se justifica em razão da escassez de pesquisas discutindo a respeito de sua efetiva implementação nos ambientes educacionais. Diante disso, esta investigação tem como objetivo discutir a respeito do cumprimento do MCI e da LGPD em ambientes acadêmicos.

O objeto deste estudo são os aspectos relativos à adequação das determinações do MCI e da LGPD à rotina de tratamento de dados pessoais digitais, envolvendo as Instituições de Ensino Superior (IES). Para isso, o artigo apresenta uma análise documental para e na fundamentação teórica,envolvendo os principais aspectos legais do MCI e da LGPD, no âmbito na educação,dialogando com artigos científicos, que representam estudos que estruturam um *corpus* de pesquisa relevante para a análise e discussões das questões relativas à proteção e à segurança digital no contexto do Ensino Superior.

## METODOLOGIA

A presente pesquisa é exploratória, documental e bibliográfica, caracterizada como uma pesquisa qualitativa (Gil, 2008). Para a análise de conteúdo dos materiais selecionados, foi utilizada a proposta de Bardin (2016), seguindo as três etapas dessa metodologia: 1) pré-análise para sistematizar as ideias iniciais; 2) exploração do material para selecionar os artigos pertinentes à pesquisa, juntamente com a

bibliometria descrita no quadro 1; e 3) tratamento e interpretação dos dados coletados. Como auxílio para organizar as referências bibliográficas, foi utilizado o *software*/pacoteBibliometrix (Aria; Cuccurullo, 2017), conforme detalhamento no Quadro 1:

**Quadro 1 – Etapas da utilização do Bibliometrix**

| n° | Etapas | Procedimentos |
|---|---|---|
| 1 | Estabelecendo a pesquisa | Para responder à pergunta: Quais as possibilidades, desafios e ações a respeito do efetivo cumprimento do MCI e da LGPD em ambientes acadêmicos? |
| 2 | Pesquisa exploratória | A pesquisa exploratória seguiu as combinações dos descritores de busca: "*General Data Protection Law*" OR "*Lei Geral de Proteção de Dados*" AND "*Marco Civil da Internet*". |
| | | Na busca foi utilizado o termo "Marco Civil da Internet" apenas em português, pois em inglês não se obtiveram resultados. A inclusão/pesquisa da combinação AND *Education* não retornou publicações de artigos sobre o MCI e a LGPD na educação, por isso foram utilizados apenas os descritores relacionados a essas duas leis. |
| 3 | Pesquisa nas bases de dados | Bases escolhidas: *Scopus e Web of Science* com a utilização do Portal de Periódicos da CAPES no sítio de periódicos, com o acesso por meio da Comunidade Acadêmica Federada (CAFe). |
| 4 | Filtragem/ critérios de inclusão | - Período das publicações entre janeiro de 2020 e julho de 2024;<br>- somente artigos científicos;<br>- em português, inglês e espanhol;<br>- acesso aberto. |
| 5 | Organização dos artigos (Bibliometrix) | A pesquisa resultou em 22 artigos, sendo: *Scopus* = 17; *Web of Science* = 5. Foram utilizados: o *software* RStudio e o pacote Bibliometrix para a junção das duas bases e retirada de 2 duplicatas. |
| 6 | Critérios de exclusão | - Artigos duplicados;<br>- fuga do tema;<br>- não apresentar elementos úteis para a pesquisa. |
| 7 | Seleção dos artigos completos para leitura prévia | Foram pré-selecionados 20 artigos completos para a leitura prévia. Após a aplicação dos critérios de exclusão restaram 10 artigos para a análise e interpretação do conteúdo conforme a etapa 8. |
| 8 | Leitura, análise e interpretação | Nesta etapa foram realizadas: uma análise documental dos aspectos legais do MCI e da LGPD e uma análise interpretativa dos 10 artigos científico-acadêmicos, em consonância com essas leis na busca de respostas para esta pesquisa. |

Fonte: Autoria própria (2024)

Os aspectos legais do MCI e da LGPD, bem como as fontes de leituras que serviram como fundamentos para amparar as discussões da pesquisa, os recortes da realidade e as situações, apresentados através da análise dos artigos, baseada nas legislações demonstradas por algumas possibilidades de ocorrências e

sugestões de correções para os problemas relacionados às eventuais violações de segurança e proteção de dados no âmbito acadêmico.

## FUNDAMENTAÇÃO TEÓRICA

### Aspectos legais sobre o MCI e a LGPD no Brasil

A proteção de dados e a segurança digital no Brasil se alicerçam em um arcabouço legal consistente em termos de regramentos à disposição da sociedade e da justiça, tanto no âmbito administrativo, como civil e, ou penal. Desta forma, esses dispositivos legais recomendam, estabelecem e determinam princípios, objetivos, competências, diretrizes e regulamentos, ao desenvolverem disciplina em determinadas matérias e, ou sancionarem violações de direitos no setor público e privado. Neste sentido, tanto o MCI como a LGPD abrangem os eventos e os fatos relacionados às esferas civil e administrativa, com atribuições para solucionar determinadas desavenças legais envolvendo certos usuários e controladores de dados, além das especificidades relacionadas à atuação dos órgãos e instituições de acordo com as suas competências e poderes de atuação, fiscalização e aplicação de sanções (Brasil, 2014; 2018).

O MCI regulamenta o uso da *internet* no Brasil, estabelecendo direitos, garantias e deveres aos usuários, amparada pelos seus princípios: a liberdade de expressão, de comunicação e de pensamento; a proteção dos dados pessoais e da privacidade; a estabilidade e funcionalidade da rede. Outros aspectos e garantias podem ser considerados importantes em seu texto como a neutralidade da rede; a proteção de seus registros de acesso e de comunicações privadas; da responsabilização por danos ocasionados pelos provedores de *internet*; a possibilidade de intervenção judicial para a apresentação dos registros de conexão; questões relativas ao acesso e diretrizes para a atuação do poder público (Brasil, 20l4; Zanon, 2022).

e-ISSN: 2177-8183

Essa regulamentação digital se fundamenta no respeito aos Direitos Humanos;na consideração do desenvolvimento da personalidade; e no reconhecimento da importância da garantia do essencial exercício da cidadania, o incentivo à colaboração, à pluralidade e à diversidade; o uso da rede como um objetivo social, a proteção do consumidor e a livre concorrência (Brasil, 20l4).

A respeito da proteção dos registros o MCI, estabelece em seu artigo 11:

> Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de *internet* em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (Brasil, 2014, p. 6).

Todos têm direito ao acesso à *internet*, sem nenhuma distinção ou pretensa desigualdade. O MCI destaca a importância de promover e estimular a participação na vida cultural; o fomento à inovação tecnológica e "adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados" (Brasil, 2014, p. 2).

Além disso, como garantias dessa lei, os usuários não poderão ter a sua conexão suspensa ou cortada, salvo por inadimplência de pagamento. A capacidade e a qualidade da *internet* devem ser mantidas de acordo com o que foi pactuado no contrato de fornecimento; os dados cadastrais, pessoais e de conexão dos usuários, somente poderão ser disponibilizados a terceiros com o devido consentimento espontâneo do titular, com todos os esclarecimentos sobre as finalidades desse compartilhamento de dados e com o devido respeito às hipóteses e determinações previstas em lei (Brasil, 2014).

Essa lei garante que os usuários não podem ter a sua vida privada, sigilo de informações, comunicações e intimidade violadas. As eventuais violações estarão sujeitas à indenização da vítima por dano material e moral. As liberações de acesso por terceiros a esses dados e informações pessoais somente poderão ocorrer por ordem judicial e de acordo com os preceitos legais. A operacionalização dos dados pessoais por terceiros, em regra, deve ter informações esclarecedoras sobre a sua coleta, utilização e armazenamento; a finalidade de utilização deles deve ser

plenamente justificada pelos motivos dessa coleta. Os contratos de fornecimento e uso da *internet* devem ser claros e conter todas as suas cláusulas transparentes e passíveis de interpretação e entendimento pelos contratantes, principalmente sobre os detalhes relacionados à operacionalização de dados pessoais (Brasil, 2014).

Em relação à neutralidade da rede, o estabelecimento dos responsáveis e das condições e das cláusulas comerciais são características fundamentais nas rotinas do tráfego de pacotes de dados, uma vez que eles não podem sofrer nenhum tipo de discriminação em relação ao seu tratamento, comunicação e operacionalização. Esse tráfego deve ter suporte técnico e tecnológico adequado para evitar a degradação de seu conteúdo e de sua qualidade e prevenir os riscos potenciais à segurança digital dos dados de seus titulares (Brasil, 2014).

Com relação aos arquivos e registros de conexão de *internet* sobre os dados pessoais e de conteúdos privados guardados em ambiente controlado, a sua guarda e disponibilização devem atender aos preceitos dessa lei, inclusive nas situações relacionadas à preservação da honra e da intimidade, bem como da privacidade e da imagem dos titulares dessas informações. O acesso ao fluxo de comunicações da *internet* e às comunicações privadas arquivadas poderá ocorrer somente através de ordem judicial (Brasil, 2014).

Os provedores de *internet* que disponibilizem conteúdos não poderão ser responsabilizados por material criado por terceiros, salvo aqueles que não cumprirem ordem judicial a respeito ou quando descumprirem o pedido de providências para a exclusão da publicação do conteúdo danoso. No entanto, eles serão responsabilizados subsidiariamente (se o devedor/responsável principal não cumprir com a obrigação) quando notificados e descumprirem com as diligências técnicas necessárias para a exclusão de conteúdos explícitos e de caráter privado, que violem ou divulguem a intimidade pessoal sem a devida vontade e autorização dos titulares (Brasil, 2014).

Além disso, para o desenvolvimento e o uso da *internet* no Brasil, é necessário o envolvimento do Poder Público, através da União, Estados, Distrito Federal e Municípios para o cumprimento das diretrizes propostas pelo MCI, a saber: a criação de uma governança multiparticipativa e democrática; promoção de uma

gestão racional da *internet* com a participação do Comitê Gestor no Brasil e a interoperabilidade entre sistemas e terminais diversos, no âmbito nacional e social; promoçãoda qualidade técnica; a inovação e a divulgação das aplicações de uso; e estímuloà criação de programas voltados à capacitação dos usuários. Ademais, há um incentivo para a adoção de tecnologias de acessos livres; a divulgação de dados públicos de forma acessível, transparente e organizada; a melhoria da infraestrutura de redes com o estímulo a centros de armazenamento, gerenciamento e divulgação de dados no país (Brasil, 2014).

As iniciativas públicas devem estimular a cultura digital e a *internet* como uma ferramenta social, promovendo a inclusão digital, ao passo em que reduz as desigualdades regionais no que tange o acesso às tecnologias e o fomento à produção de conteúdo nacional. Portanto, o Estado deve, continuamente, formular e promover estudos, metas, estratégias e planos para o uso e desenvolvimento dessa tecnologia no país (Brasil, 2014). O MCI representa um avanço significativo na proteção de direitos, garantias e deveres dos usuários, em especial, em relação ao respeito aos Direitos Humanos e à garantia do exercício da cidadania; à proteção dos dados pessoais e da privacidade e à inviolabilidade da intimidade e da vida privada dos usuários, à possibilidade de responsabilização de terceiros por danos sofridos e à necessidade de consentimento livre e expresso para a coleta, uso, armazenamento e tratamento desses dados.

Portanto, ao assegurar essas garantias de forma ampla, podendo atingir todos os setores da sociedade, inclusive a educação, essa legislação permite vislumbrar maior transparência e controle por parte dos usuários sobre suas informações pessoais, além de estabelecer mecanismos de reparação em casos de violações. Dessa maneira, o MCI, juntamente com a LGPD, pode contribuir para um ambiente digital mais seguro e controlado.

Nesse sentido, a LGPD foi criada em 2018 para regulamentar o tratamento de dados pessoais coletados por qualquer meio dentro do território brasileiro; independente do país, sede ou localidade em que estejam localizados os dados, abrangendo inclusive os meios físicos e digitais (Nascimento; Silva, 2023). Esse regramento visa proteger os dados manipulados por pessoas físicas e jurídicas de

direito público e privado, buscando proteger os direitos fundamentais como a liberdade, a privacidade e a personalidade dos indivíduos (Brasil, 2018).

De acordo com essa lei, um dado pode ser considerado como pessoal quando a informação da pessoa puder ser identificada ou identificável. Dado anonimizado é quando os dados não podem ser identificados através da tecnologia disponível na ocasião do tratamento. A elaboração da LGPD se fundamentou no regulamento internacional *GDPR*, em português: Regulamento Geral sobre a Proteção de Dados e que entrou em vigor em 2017 e normatiza a proteção e a privacidade de dados pessoais nos países participantes da União Europeia com reflexos dessa matéria e desse regulamento nas relações envolvendo a proteção de dados em diversos países (GDPR, 2016; Andrade; Barreto, 2020).

Controlador a quem compete às decisões e operador é aquele que realiza o tratamento seguindo as diretrizes do controlador (Brasil, 2018).Como propostas de mitigação do uso indiscriminado de dados, Gomes, Cunha Filho e Luccas (2023) apresentam a ideia de valorização dos princípios da finalidade, transparência e necessidade contidos na GDPR. No primeiro, os dados somente poderão ser tratados de acordo com a explicitação de sua finalidade, excetuando-se uma segunda opção de uso não autorizado; no segundo princípio, o controlador deve informar ao titular de forma transparente sobre a real finalidade de utilização e como as informações serão tratadas; e no terceiro, o controlador poderá usar apenas a quantidade necessária de dados disponíveis.

Esses princípios também podem ser encontrados em alguns trechos da LGPD com o objetivo de subsidiar a proteção de dados no Brasil, juntamente com as seguintes garantias: a liberdade de expressão, de comunicação, de opinião, a autodeterminação informativa, a proibição de violação da intimidade, da imagem e da honra. Estende-se a outros aspectos, envolvendo a proteção da liberdade, da concorrência, da livre iniciativa, do consumidor, o desenvolvimento e a inovação tecnológica e o crescimento econômico, e, ainda, protege a dignidade, o exercício da cidadania e os Direitos Humanos (GDPR, 2016; Brasil, 2018).

Em relação ao rol de princípios, Nascimento e Silva (2023) preferiram enfatizar em sua pesquisa os princípios da finalidade, da adequação e da

necessidade. O primeiro está relacionado à atividade específica a ser desenvolvida pela instituição de acordo com a real finalidade e a consequente informação ao titular dos dados; o segundo destaca a importância da adequação entre os dados a serem tratados e a informação repassada ao titular sobre o tratamento; e o terceiro se refere à quantidade mínima necessária de dados para atender às finalidades planejadas.

Apesar de a LGPD ser abrangente, adaptativa e interpretativa, essa lei não se aplica integralmente a todas as situações. O Artigo 4 da LGPD elenca os casos em que essa lei não é aplicada: quando o tratamento de dados é realizado por pessoa natural com a finalidade exclusiva envolvendo aspectos particulares e não econômicos; realizado para fins exclusivamente jornalístico, artístico e acadêmico (aplicando-se, neste último caso, os Artigos 7 e 11 desta lei); segurança pública; defesa nacional; segurança do Estado e atividades de investigação e repressão de infrações penais (Brasil, 2018).

Em especial, no caso desta pesquisa, os Artigos 7 e 11 são destinados para regular algumas situações específicas sobre o tratamento dos dados pessoais acadêmicos. De acordo com o Artigo 7, entre outras determinações, esses dados somente poderão ser tratados mediante o consentimento por escrito do titular ou outro meio que demonstre a manifestação de sua vontade, proibindo-se qualquer vício dessa autorização (Brasil, 2018).

No artigo 11, a respeito dos dados sensíveis do titular e artigo 14, que trata dos dados pessoais de crianças e adolescentes, eles somente poderão ser tratados para atender aos seus interesses específicos e com o respectivo consentimento de pelo menos um dos pais ou responsável legal. Quando estritamente necessário, o consentimento poderá ser dispensado no caso de exigência de lei específica ou para atender obrigação regulatória do controlador (Brasil, 2018).

Em razão dos artigos 7 e 11, a possibilidade de acesso aos dados sensíveis dos alunos ficou bastante restrita, hipóteses de mitigação dos riscos e utilizações indevidas e fraudulentas, além de buscar evitar danos irreparáveis às pessoas (Andrade; Barreto, 2020). De acordo com o GDPR, se a violação dos dados não for tratada de forma rápida, adequada e oportuna, o titular poderá sofrer sérios abalos

psicológicos e danos físicos e materiais, podendo até limitar indevidamente os seus direitos (GDPR, 2016).

O titular dos dados pode solicitar aos seus controladores a revisão de decisões tomadas envolvendo o tratamento automatizado de seus dados pessoais que impactem ou prejudiquem os seus interesses e caso necessário, a solicitação de eliminação de seus dados ou a revogação de seu consentimento. Pode-se obter, também, informações claras e transparentes abrangendo os registros, critérios e procedimentos de armazenamento e divulgação automatizados de seu perfil pessoal e de personalidade, profissional, de consumo, de crédito; salvo quando essa transparência ofender os segredos comerciais e industriais (Brasil, 2018).

O tratamento e compartilhamento de dados pessoais pelo Poder Público seguirão as suas especificidades atendendo aos requisitos e atribuições legais, obedecendo às respectivas regras para o exercício de sua competência, atribuições e o devido estabelecimento da finalidade desse tratamento. Na hipótese de transferência de dados deve-se atentar para os riscos e a prevenção de irregularidades e fraudes, cuidados relacionados à proteção, à segurança e à integridade do titular desses dados (Brasil, 2018).

As seguranças administrativa e técnica desses dados pessoais devem ser garantidas para a prevenção dos acessos não autorizados ou problemas relacionados ao perigo de alteração ou destruição e uso inadequado ou ilícito. Além da preocupação com a salvaguarda dos dados pessoais do titular, qualquer medida que contrarie a proteção dessas informações deve receber medidas para a mitigação dos danos, proporcionais a sua gravidade (Brasil, 2018).

O tratamento de dados está sujeito à fiscalização e eventuais sanções administrativas aplicadas pela autoridade nacional no caso de infrações cometidas pelos agentes administrativos, com a sujeição de advertência, multa simples, multa diária e, ao final a publicação da infração, entre outras penalidades, possibilitando-se o contraditório e a ampla defesa, além da gradação das penalidades de acordo com os danos sofridos pelo titular dos dados ou pela eventual reincidência e aspectos benéficos relacionados à cooperação e à boa fé do infrator (Brasil, 2018).

e-ISSN: 2177-8183

Nessa perspectiva de fiscalização, de acordo com a LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD) com sede no Distrito Federal possuindo autonomia técnica e decisória. Essa autarquia tem a competência de zelar pela proteção dos dados pessoais conforme estabelecido em legislação; elaborar as regras para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções; bem como, analisar as alegações de defesa; possibilitar a divulgação das normas e políticas públicas sobre o tema; elaborar estudos e adoção de padrões de controle; estimular a cooperação de autoridades nacionais e internacionais; elaborar relatórios técnicos periódicos, editar regulamentos e realizar auditorias (Brasil, 2018).

Enfim, devido à promulgação da LGPD foi possível ter contato com uma legislação específica a ser considerada na operacionalização digital de dados pessoais, tanto no setor público como no privado. Juntamente com o MCI, essa lei posiciona o Brasil no rol dos países preocupados com a proteção de dados de seus cidadãos; pois proteger os brasileiros de ataques pessoais e aos seus direitos fundamentais é garantir a proteção de sua personalidade e dignidade da pessoa humana (Andrade; Barreto, 2020).

## Estudo sobre proteção e segurança de dados na perspectiva do MCI e da LGPD

Em relação ao contexto da proteção e da segurança digital dos dados na educação, é possível inferir e compreender como as legislações, a exemplo do MCI e da LGPD, pode fornecer subsídios legais para resguardar os direitos e deveres dos usuários e das instituições, refletindo-se em toda a sociedade. Por isso, buscaram-se nos estudos da atualidade os dados esclarecedores relacionados às determinadas situações envolvendo a proteção e a segurança de dados pessoais e no Ensino Superior, servindo de amparo às discussões juntamente com a seção já apresentada que trata sobre os aspectos legais relacionados ao MCI e a LGPD.

Perceberam-se, através dessas leis e da análise destas pesquisas, que as instituições de ensino podem enfrentar certas dificuldades em se adequarem às normas vigentes sobre a proteção de dados digitais, especialmente devido ao atual cenário global de rápida expansão do uso da *internet* e das tecnologias digitais. As informações suscitam a necessidade de elaboração e implementação de estratégias e protocolos eficazes de segurança e de privacidade de dados dos usuários no ambiente educacional.

Nessa perspectiva, a apresentação dos estudos já desenvolvidos se inicia com alguns aspectos apontados por Gomes, Cunha Filho e Luccas (2023) ao mencionarem a necessidade da Fundação Getúlio Vargas (FGV) se adequar ao tratamento de dados de seus alunos seguindo LGPD, destacando-se a complexidade relacionada à movimentação de uma grande quantidade de dados por essa Instituição. Como proposta de adequação, os dados dos alunos foram divididos em quatro categorias visando à elaboração de estratégias para a gestão e proteção de dados, são elas: interessados, inscritos, matriculados e ex-alunos visando à proteção de cada categoria em razão da finalidade de uso das informações coletadas.

Sobre os impactos da LGPD no âmbito das IES, Almeida e Soares (2022) destacam que, de acordo com o artigo 11, o tratamento de dados sensíveis na educação deve seguir alguns cuidados especiais e criteriosos. Segundo essa lei, dado pessoal sensível se refere 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; [...]” (Brasil, 2018, p. 2).

Na perspectiva da LGPD, Almeida e Soares (2022) apontam as IES como controladoras de dados e a necessidade de adotar medidas para garantir a transparência dos procedimentos relacionados ao tratamento, utilização e aplicação, desde que não contrariem o consentimento dos alunos reconhecidos como titulares desses dados. Os controladores devem possibilitar treinamento aos membros responsáveis pelo tratamento visando à capacitação para interpretação e atualização das regras dessa lei.

e-ISSN: 2177-8183

A respeito dos riscos de incidentes relacionados ao vazamento de dados pessoais, Andrade e Barreto (2020) discutem sobre a ocorrência de vazamento de dados pessoais que remetam a algumas informações contidas em publicações e fotos de milhões de usuários cadastrados em determinadas redes sociais. Essa pesquisa reforça a ideia de que a reincidência dessas violações corrobora a importância das legislações sobre o tema. Por isso, esses autores se propuseram a avaliar a eficácia da LGPD.

Em outra análise, na pesquisa de Cardoso e Régis (2024), há uma proposta metodológica para uma análise comparativa entre o MCI e a LGPD com o objetivo de apontar eventuais semelhanças, diferenças e lacunas entre elas e, também, como esse conjunto de normas e diretrizes foram absorvidas pelo ordenamento jurídico brasileiro, considerando como estas estão sendo utilizadas para garantir a proteção de dados pessoais digitais/*online*. Esses autores mencionam que, enquanto o MCI estabelece garantias, princípios, direitos e deveres em relação ao uso da *internet*, a LGPD é mais abrangente em matéria de proteção de dados pessoais por tratar especificamente sobre essa matéria e estabelecer uma proteção dos usuários envolvendo o setor público e privado.

Ademais, na investigação de Lugati e Almeida (2022), essas autoras analisaram como as determinações estabelecidas pela LGPD estão influenciando as instituições e empresas em relação à adaptação a uma nova cultura de proteção de dados com a preocupação de se manter um pensamento voltado à inovação, a criação de modelos de proteção e à identificação das responsabilidades envolvidas, além das iniciativas técnicas referentes à segurança dos dados e à importância de transparência no repasse de informações.

Nesse sentido, na pesquisa de Canedo *et al*. (2020), os autores buscaram identificar os modelos e técnicas para a implementação de requisitos de privacidade de *software* e, consequentemente, como os profissionais de Tecnologia da Informação e Comunicação (TIC) conhecem e aplicam no seu cotidiano os requisitos legais determinados pela LGPD. Ao final, em especial, esses autores constataram que os profissionais e desenvolvedores não se consideram totalmente conhecedores dos princípios e texto dessa lei e, por isso, aptos para a aplicação em suas

atividades e projetos atinentes às diretrizes de segurança de dados, recomendadas pela LGPD.

Ao corroborar com essas situações, cabe às IES, através de suas bibliotecas e repositórios, que hospedam as publicações acadêmicas e científicas, auxiliar na tarefa de aplicação dessa lei. Nessa perspectiva, Nascimento e Silva (2023) investigaram as adequações necessárias à LGPD no âmbito dos repositórios institucionais no contexto do ensino superior, da privacidade e da proteção de dados. Esses autores perceberam, através de sua pesquisa, a amplitude dessa lei em estabelecer diretrizes e sanções para que essas instituições possam se adequar ao texto desse regulamento. O estudo propõe determinadas recomendações em relação aos fluxos e processos internos, a operacionalização de documentos institucionais, a capacitação dos envolvidos no tratamento de dados e a importância de transparência nas ações dos controladores e operadores de dados.

Em contrapartida, em sua investigação envolvendo 15 docentes de uma instituição pública de ensino tecnológico, Souza, Belda e Arima (2022) enfatizam a existência de uma diversidade de tecnologias digitais ligadas ao processo de ensino e aprendizagem devido ao consequente volume expressivo de dados utilizados por essa instituição. Por isso, estudaram a conformidade e a necessidade de ajustes entre os procedimentos adotados e o que estabelece o texto da LGPD em relação à proteção de dados pessoais. A necessidade de adequações à LGPD está relacionada ao contexto administrativo e educacional e às dimensões de proteção de dados pessoais estabelecidas nessa lei. E mais, essa investigação evidenciou a importância de criação e de implementação de um programa de governança e conscientização institucional visando à segurança e a proteção de dados, com transparência e se utilizando de métodos de controle e correção; a criação de programas de capacitação e de canais de comunicação e de informação.

Essas ações, ou seja, a criação de um programa de governança e conscientização institucional, adoção de transparência, métodos, programas e canais almejam consolidar um compromisso na busca de soluções para a mitigação de problemas relacionados às eventuais violações de privacidade e de dados pessoais, abrindo espaço para uma relação de confiança entre os titulares de dados

e a instituição devido à possibilidade de integração entre as determinações da LGPD e os objetivos de proteção e segurança institucionais, com propostas viáveis, aplicáveis e adaptáveis à realidade atual tecnológica e da sociedade (Souza; Belda; Arima, 2022).

Por fim, a investigação se deparou com uma escassez de publicações a respeito do MCI e da LGPD na perspectiva da proteção e da segurança de dados pessoais relacionando-as à educação, principalmente em relação ao MCI. Dos dez artigos selecionados para análise, apenas quatro deles trataram especificamente da LGPD no âmbito educacional: Gomes, Cunha Filho e Luccas (2023) buscaram compreender como as IES do Brasil podem adequar as suas rotinas e os seus procedimentos internos de tratamento de dados de alunos à LGPD. Nascimento e Silva (2023) discutem a LGPD no contexto dos dados recebidos, armazenados e compartilhados pelos repositórios institucionais. Os autores Souza, Belda e Arima (2022) verificaram por meio de um estudo de caso, a conformidade entre instrumentos normativos de proteção de dados pessoais adotados por uma instituição pública de ensino tecnológico e o estabelecido pela LGPD. Almeida e Soares (2022) refletiram sobre os impactos advindos da LGPD no contexto nacional com reflexos nas IES.

Apesar dos seis trabalhos restantes discutirem a implementação do MCI e da LGPD de uma forma conceitual e genérica, com outras abordagens, eles fornecem conceitos, discussões e subsídios para a análise da possibilidade de implementação e efetividade dessas leis nos meios digitais e controle de fluxos de dados das organizações e das instituições, com questões relacionadas à necessidade de tratamento de dados pessoais numa perspectiva de segurança e inovação tecnológica; análise pormenorizada dos dispositivos dessas leis; comparação entre elas; impactos dessas leis nas organizações; desenvolvimento de *softwares* e tecnologias em conformidade com essas leis e requisitos de privacidade e efeitos na inovação local decorrentes da replicação do *General Data Protection Regulation (GDPR)* na LGPD.

e-ISSN: 2177-8183

## ANÁLISE E DISCUSSÃO DOS RESULTADOS

Com base no MCI, na LGPD e nos artigos analisados identificaram-se alguns dispositivos legais, recomendações e recortes de pesquisas que podem auxiliar na compreensão dos fenômenos e situações relacionadas ao objeto de estudo. Observa-se que, apesar da diversidade de abordagens dos trabalhos revisados, as propostas para a mitigação dos problemas decorrentes de práticas indevidas convergem em sugerir a implementação de protocolos de segurança robustos e estratégias integradas, que possam efetivamente prevenir e controlar tais práticas.

Nessa perspectiva, a proteção de dados, os riscos de vazamento, a criação e o *design* de sistemas e de *softwares* podem enfrentar certas dificuldades e entraves em razão de vários aspectos, tais como:adequação às regulamentações legais nacionais e internacionais; criação de metodologias para o desenvolvimento dessas tecnologias e programas; obtenção de recursos e acesso às tecnologias disponíveis e adequadas; restrições e características estruturais das organizações e instituições; capacitação dos interessados, planejamento para mitigação de danos e transparência nas informações (Canedo *et al*., 2020).

O vazamento de dados pessoais pelos meios físicos ou digitais pode ocorrer de maneira intencional através de invasão ou furto de dados, bem como, por mero descuido ou desatenção dos usuários ao compartilharem inadvertidamente os seus dados e informações, além de consentimentos indevidos para acesso de terceiros ao seu cadastro, quando contém os seus dados e aos aceites, sem a devida precaução aos termos de uso e de privacidade solicitados, ao realizarem o *login* e, ou o cadastro em determinados *sites* e, ou redes sociais (Andrade; Barreto, 2020).

Os desafios enfrentados em razão desses vazamentos e da busca de segurança e proteção dos dados pessoais à luz da LGPD são potencializados pelo uso intenso da *internet*, dos *softwares* e dos dispositivos digitais. Por isso, os agentes de tratamentos de dados devem estar atentos aos métodos de coleta, processamento, armazenamento e compartilhamento de informações. Caso ocorra algum vazamento indevido de dados, especialmente dos dados sensíveis por falta de consentimento, devem ser apuradas as responsabilidades e concomitantemente,

buscar a criação e efetivação de protocolos de segurança mais eficientes e analisar todo o fluxo de pacotes de dados para tentar identificar as falhas de procedimentos. Isso “coloca a gestão de toda e qualquer Instituição de Ensino Superior (IES), sob o prisma da vulnerabilidade, obrigando, assim, a instituição a se submeter à avaliação e, por consequência, rever sua segurança cibernética” (Almeida; Soares, 2022, p. 42).

Considerando a ideia de Canaan (2023) para uma perspectiva de criação de protocolos de controle e de segurança cibernética, a GDPR, em seu artigo 25, introduziu implicitamente um novo princípio: a Proteção de dados desde a concepção (proteção de dados por *design* e por padrão), ou seja, desde o início do tratamento, do processamento e do desenvolvimento tecnológico, para que os responsáveis pelo tratamento e pela inovação considerem medidas técnicas e organizacionais adequadas e necessárias para a proteção de dados.

Questão essa, corroborada pelo artigo 6, inciso VII da LGPD, sobre a necessidade de se observar nas atividades relacionadas ao tratamento de dados a boa fé e o seguinte princípio: “segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; [...]” (Brasil, 2018, p. 4).

Ao normatizar o tratamento dos dados pessoais, a LGPD se consolida como um regulamento especial para a matéria e, juntamente com o MCI, oferecem diretrizes de segurança e proteção abrangentes de acordo com cada conteúdo legal. Caberá às IES e demais agentes identificarem a finalidade, a natureza, os benefícios e os desafios da operacionalização dos dados e corrigirem previamente eventuais lacunas e falhas nos processos envolvendo a segurança e a privacidade dos dados pessoais.

Em relação às IES como órgãos responsáveis e à ocorrência de desafios institucionais devido a um grande volume de acessos à *web*, elevada movimentação e armazenamento de dados nos repositórios, a pesquisa de Nascimento e Silva (2023) discorreu sobre esses repositórios institucionais, possibilitando-se identificar a importância da LGPD nas atividades de guarda, disponibilização e recuperação de

diversas informações acadêmicas, científicas, artísticas e da própria administração, pois, para o depósito, os envolvidos necessitam fornecer diversos dados, inclusive os dados personalizados, necessários para a operacionalização das produções, das pesquisas e dos documentos depositados.

E os setores e demais departamentos das IES, a exemplo das suas bibliotecas e seus repositórios, possuem fluxos e estratégias de trabalhos definidos, visando alcançar a rapidez e a eficiência nos serviços oferecidos à comunidade. Nesse sentido, são extremamente importantes os planejamentos de ações, debates e estratégias necessárias para o gerenciamento e o tratamento seguro das informações contidas nesses serviços para evitar o vazamento inapropriado de dados.

Entendendo melhor o que diz a lei no caso das responsabilidades desses repositórios das instituições,quando classificadas como pessoa jurídica de direito público, as IES têm a incumbência de exercer o seu papel como controladoras e possuem a competência em relação às decisões sobre o tratamento de dados pessoais, ou seja, têm o poder decisório das ações e das atividades envolvendo os respectivos processos à luz dos artigos 7 e 11 da LGPD, em conjunto com os demais excertos aplicáveis dessa lei, estabelecendo-se ainda: quais, como, quando e o volume de dados que serão operacionalizados de acordo com as finalidades e necessidades propostas (o porquê). São responsáveis, também, de acordo com a lei e com o interesse público, em prestar contas sobre a aplicação dos respectivos dispositivos dessa lei e sujeitos a sofrerem determinadas sanções aplicadas pela ANPD (Nascimento; Silva, 2023; Brasil, 2018).

Logo, Nascimento e Silva (2023) apresentam algumas sugestões para adequação desses repositórios institucionais aos preceitos da LGPD: cadastramento dos usuários; mapeamento dos dados pessoais e, ou sensíveis solicitados no cadastro seguindo os princípios da finalidade, necessidade e adequação; capacitação, treinamento de toda a equipe institucional sobre o fluxo de trabalho envolvendo o tratamento de dados; gestão de risco, identificação e consequente definição de estratégias de prevenção e mitigação de riscos; gestão documental, incluindo análise dos documentos e de arquivos, destinando-os de acordo com o seu

ciclo de vida; gestão institucional, estabelecimento de política institucional de privacidade e se necessário, coparticipação de equipe multidisciplinar para discussões e acompanhamento dos processos e fluxos do tratamento de dados; mapeamento dos padrões de cada documento e políticas de informação, buscando a revisão dessas políticas e manutenção de sua transparência, efetuando-se os ajustes necessários.

Além disso, Nascimento e Silva (2023) sugerem algumas possibilidades para o aperfeiçoamento da gestão desses repositórios. Acredita-se que a continuidade dos debates, a criação e a melhoria das políticas públicas a respeito dessa temática poderão contribuir para encontrar um equilíbrio entre a necessidade de depósito de documentos e de dados nos repositórios e a efetiva proteção e segurança dos dados pessoais e da salvaguarda da privacidade e da intimidade dos alunos e demais usuários.

Corroborando com a ideia anterior, Souza, Belda e Arima (2022) mencionam a respeito da adequação dos objetivos de proteção e segurança de dados pessoais envolvendo o fluxo de dados pessoais do *campus* de uma instituição pública tecnológica às determinações da LGPD. A proposta desses autores se fundamenta em elementos obrigatórios constantes na LGPD, em especial, nos direitos fundamentais de privacidade, liberdade e livre desenvolvimento da personalidade da pessoa natural; se alicerçando ainda nos princípios da necessidade, finalidade, adequação, transparência, livre acesso, qualidade, prevenção, segurança, responsabilização e não discriminação.

Outras questões também são destacadas por esses autores relacionadas à proteção de dados pessoais: a importância do consentimento expresso e inequívoco do titular em relação ao tratamento desses dados, bem como, a possibilidade de revogação, alteração e bloqueio desse consentimento e até mesmo, a eliminação total das informações armazenadas. Enfatizam a necessidade de assegurar os resultados em razão das finalidades propostas, à adequação aos objetivos e aos cuidados relacionados à utilização do mínimo necessário em relação ao volume de dados tratados (Souza; Belda; Arima, 2022).

e-ISSN: 2177-8183

Portanto, a presente pesquisa que investigou o cumprimento do MCI e da LGPD buscou apresentar subsídios e respostas do seu papel como instrumentos legais efetivos para a proteção e segurança dos dados pessoais dos usuários numa perspectiva educacional. O estudo apontou a inter-relação de diversos elementos, aspectos legais e conceitos extremamente importantes para a mitigação de riscos; necessidade de elaboração de estratégias de proteção, segurança e privacidade de dados pessoais dos usuários numa perspectiva de aplicação no ensino Superior.

Foi discutida a necessidade de adequação das determinações do MCI e da LGPD na rotina de tratamento desses dados envolvendo as IES; a importância de criação e adoção de ações mitigadoras dos riscos de vazamento e de violação de informações pessoais e/ou sigilosas; a estruturação organizacional e administrativa das instituições de ensino; o mapeamento de fluxos de dados e de trabalhos; a criação de programas de gestão de riscos dessas instituições; o desenvolvimento e implementação de tecnologias eficientes na garantia de segurança e filtros de proteção dos dados digitais; a redução das desigualdades regionais e a democratização de acesso às tecnologias; a capacitação dos responsáveis pelos tratamentos de dados; a transparência nas informações e sigilos necessários na forma da lei; a coparticipação dos setores envolvidos, da sociedade e do Poder Público de acordo com cada competência na busca de soluções e o respeito aos princípios estabelecidos, direitos e garantias fundamentais individuais e coletivas.

Enfim, a proteção de dados é uma questão complexa, exigindo-se leis detalhadas, abrangentes e aplicáveis. Além de estratégias, ações e metodologias com potencial em garantir a segurança e privacidade dos usuários. Os vazamentos de dados acidentais ou intencionais sinalizam para medidas urgentes de segurança e transparência na forma da lei, o MCI e a LGPD fornecem caminhos para isso, atribuindo responsabilidades e estabelecendo diretrizes claras para afastar os riscos, além de possibilidades legais para a solução de determinados impasses e conflitos.

## CONSIDERAÇÕES FINAIS

A pesquisa enfatiza a importância de leis capazes de prevenir, minimizar, combater e punir os abusos de direitos, a exemplo do MCI e da LGPD, induzindo a ideia de que a *internet* não é um ambiente sem lei, pois apesar dos usuários, muitas vezes, não possuírem capacidade de autoproteção e serem afetados subjetivamente por determinadas situações envolvendo riscos potenciais, vazamentos e violações de seus dados pessoais digitais e físicos; as legislações pertinentes devem ser acionadas para garantir os seus direitos, buscando evitar que não sofram abalos e danos pessoais irreparáveis ou permanentes. "Assim, a fim de colocar em cena a ideia de internet como um lugar, uma instituição que produz sujeitos e tem efeitos sobre estes [...]" (Polizel; Mendes; Carvalho, 2017, p. 313).

Além disso, em relação às IES e demais agentes responsáveis pelo tratamento de dados pessoais, eles precisam discutir e buscar implementar políticas e ações de segurança e proteção eficazes, capacitar as suas equipes e conscientizá-las sobre a importância dessas leis. Assim, a compatibilização e aplicação das normas, o avanço técnico e tecnológico, a coparticipação e a colaboração entre os envolvidos são fundamentais para proteger os direitos dos cidadãos e proporcionar um ambiente cada vez mais conectado e seguro.

Somado à necessidade de incorporação de boas práticas relacionadas à proteção e segurança da privacidade das pessoas, à garantia do respeito aos direitos individuais e coletivos em todos os processos relacionados ao tratamento dos dados pessoais, também se justifica a importância de atuação constante das instituições públicas e privadas, em parceria com órgãos responsáveis do poder público, no sentido de implementação e respeito às leis; no apoio à criação de políticas e programas de governança em privacidade e gestão da informação que estejam em harmonia com o direito à proteção de dados.

Portanto, diante de todo o exposto, entendemos que, para que aconteçam a efetivação dessas leis, de políticas de segurança e de privacidade é fundamental para vislumbrar a proteção de dados dos estudantes e demais usuários, possibilitando-se um ambiente acadêmico mais seguro e confiável. É importante ressaltar que esta investigação se limitou ao MCI e à LGPD, e estudos elencados

sobre a problemática em análise.Contudo, outros dispositivos legais poderão ser pesquisados e analisados futuramente no sentido de se aprofundar e complementar os aspectos relacionados ao tratamento, segurança e proteção de dados pessoais no âmbito da educação, afinal a ciência e o conhecimento se fazem constantemente, em diálogo com as descobertas de outrora.

## REFERÊNCIAS


ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. The impacts of the General Law of Data Protection-LGPD in the digital scenario. **Perspectivas em Ciência da Informação**, v. 27, p. 26-45, 2022. Disponível em: DOI: http://dx.doi.org/10.1590/1981-5344/25905. Acesso em: 5 jul. 2024.

ANDRADE, Diogo de Calasans Melo; BARRETO, Roberta Hora Arcieri. A ausência da atividade fiscalizadora na Lei Geral de Proteção de Dados Pessoais e sua ineficácia. **Rev. Eletronica Direito Sociedade** , v. 8, p. 61, 2020. Disponível em: DOI: https://doi.org/10.18316/redes.v8i2.5407. Acesso em: 6 jul. 2024.

ARIA, Massimo; CUCCURULLO, Corrado. Bibliometrix: An R-tool for comprehensive science mapping analysis. **Revista de Informetrics**, v. 11, n. 4, p. 959-975, 2017. Disponível em: DOI: https://doi.org/10.1016/j.joi.2017.08.007. Acesso em: 30 jul. 2024.

BARDIN, Laurence. **Análise de Conteúdo**. Tradução: Luís Antero Reto, Augusto Pinheiro. São Paulo: Edições 70, 2016. 279 p.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jun. 2024.

BRASIL. Lei 10.406 de 10 de Janeiro de 2002. Código Civil. Brasília, DF. 2002. **Diário Oficial da União**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 7 jul. 2024.

BRASIL. Lei 12.965 de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. 2014. **Diário Oficial da União**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 3 jul. 2024.

BRASIL. Lei 13.709 de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF. 2018. **Diário Oficial da União**. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 jun. 2024.

CANAAN, Renan Gadoni. The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law. **Internet Policy Review**, v. 12, n. 1, 2023. Disponível em: DOI: https://doi.org/10.14763/2023.1.1686. Acesso em: 24 jul. 2024.

CANEDO, Edna Dias; CALAZANS, Angélica Toffano Seidel; MASSON, Eloisa Toffano Seidel; COSTA, Pedro Henrique Teixeira; LIMA, Fernanda. Perceptions of ICT practitioners regarding software privacy. **Entropy**, v. 22, n. 4, p. 429, 2020. Disponível em: DOI: https://doi.org/10.3390/e22040429. Acesso em: 24 jul. 2024.

CARDOSO, Caroline de Melo; RÉGIS, Jonathan Cardoso. Direito Comparado: LGPD e o Marco Civil da Internet. **Revista de Direito**, v. 16, n. 01, p. 1-23, 2024. Disponível em: DOI: https://doi.org/10.32361/2024160116495. Acesso em: 6 jul. 2024.

GDPR, General Data Protection Regulation. Regulation (EU) 2016/679 of the European Parliament and of the Council**,** on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC . **EUR-Lex**, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679. Acesso em: 6 jul. 2024.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008. 200 p.

GOMES, Fabrício Vasconcelos; CUNHA FILHO, Marcelo de Castro; LUCCAS, Victor Nóbrega. Proteção de dados e instituições de ensino: o que fazer com dados de alunos?. **Revista Brasileira de Políticas Públicas**, v. 13, n. 1, 2023. Disponível em: DOI: https://doi.org/10.5102/rbpp.v13i1.7996. Acesso em: 4 jul. 2024.

LEONARDI, Marcel. Capítulo 8: Aspectos Controvertidos Entre a Lei Geral de Proteção de Dados e o Marco Civil da Internet. In: PALHARES, F. **Temas Atuais de Proteção de Dados**. São Paulo: Editora Revista dos Tribunais, 2020. Disponível em: https://www.jusbrasil.com.br/doutrina/secao/capitulo-8-aspectos-controvertidos-entre-a-lei-geral-de-protecao-de-dados-e-o-marco-civil-da-internet-temas-atuais-de-protecao-de-dados/120754851. Acesso em: 7 jul. 2024.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. A LGPD e a construção de uma cultura de proteção de dados. **Revista de Direito**, v. 14, n. 1, p. 1-20, 2022. Disponível em: DOI: https://doi.org/10.32361/2022140113764. Acesso em: 23 jul. 2024.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. General Data Protection Law and institutional repository: reflections and compliance. **Em Questão**, v. 29, p. 1-27, 2023. Disponível em: DOI: https://doi.org/10.1590/1808-5245.29.127314. Acesso em: 26 jul. 2024.

POLIZEL, Alexandre Luiz; MENDES, Nara Alves; CARVALHO, Fabiana Aparecida de. Discursos, violências e sensibilizações anti-cyberbullying: nós, os outros e as virtualidades reais. **Revista Brasileira de Ensino de Ciência e Tecnologia**, v. 10, n. 3, 2017. Disponível em: DOI: http://dx.doi.org/10.3895/rbect.v10n3.5145. Acesso: 10 ago. 2024.

SOUZA, Jackson Gomes; BELDA, Francisco Rolfsen; ARIMA, Carlos Hideo. GDPR application Analysis in a Public Educational Institution: a Case Study. **RIAEE - Revista Ibero-Americana de Estudos em Educação**, p. 1855-1871, 2022. Disponível em: DOI: https://doi.org/10.21723/riaee.v17i3.16789**.** Acesso em: 26 jul. 2024.

ZANON, Sandra Buth. Arquivos públicos: proteção de dados frente o acesso à informação. **Revista Ibero-Americana de Ciência da Informação**, v. 15, n. 2, p. 416-435, 2022. Disponível em: DOI: https://doi.org/10.26512/rici.v15.n2.2022.40678. Acesso em: 25 jul. 2024.

*Submetido em outubro 2025*
*Avaliado em novembro 2025*
*Publicado em abril 2026*

Agradecemos ao CNPQ pelo financiamento parcial do trabalho.