Artigo

em questão
E-ISSN 1808-5245

Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações

Bruna Laís Campos do Nascimento
Universidade Federal de Pernambuco, Recife, PE, Brasil;
Instituto Federal do Rio Grande do Norte, Lajes, RN, Brasil;
bruna.campos@ifrn.edu.br; ORCID https://orcid.org/0000-0001-6612-2076

Edilene Maria da Silva
Universidade Federal de Pernambuco, Recife, PE, Brasil;
edilene.msilva@ufpe.br; ORCID https://orcid.org/0000-0002-7840-3198

Resumo: Este artigo discute a Lei Geral de Proteção de Dados no contexto dos repositórios institucionais, enfocando as adequações necessárias a serem realizadas. Apresenta um breve panorama da legislação brasileira que trata sobre a privacidade e a proteção de dados. O presente trabalho caracteriza-se quanto aos fins como uma pesquisa de natureza exploratória, e quanto aos meios como bibliográfica e documental, com abordagem qualitativa. A partir das análises, foi identificado que a Lei Geral de Proteção de Dados apresenta consistentes diretrizes e sanções para que as instituições possam garantir adequados tratamento e segurança dos dados pessoais. Quanto aos repositórios, foi percebido que adaptações são necessárias e o estudo propõe algumas recomendações, principalmente no que concerne aos processos e fluxos de trabalho, à revisão de documentos institucionais, capacitação e às ações de transparência. Conclui que as discussões sobre a privacidade e a proteção dos dados pessoais precisam ser fomentadas na sociedade, incluindo os repositórios nesse cenário de aplicação.

Palavras-chave: Lei Geral de Proteção de Dados; privacidade; repositório institucional

1 Introdução

O avanço das tecnologias de informação e comunicação aliado ao uso da internet tem possibilitado ampliar o acesso aos mais variados recursos informacionais. Dentre as ferramentas tecnológicas disponíveis estão os repositórios institucionais (RIs), que possibilitam armazenar, disponibilizar, acessar e recuperar as produções científicas, acadêmicas, artísticas e/ou administrativas de uma determinada organização (COSTA; LEITE, 2017).

Neste contexto, para que se possa disponibilizar as produções em um RI se faz necessário realizar o depósito, o qual pode ser feito por meio do auto-

arquivamento ou do depósito mediado. Para isso, os usuários vinculados à instituição (discentes, servidores e contratados) precisam fornecer um conjunto de dados, sendo alguns referentes à publicação e outros, pessoais. Ademais, alguns repositórios, com o intuito de ofertar serviços de informação personalizados, solicitam aos usuários a realização de cadastro, sendo preciso para isso registrar também mais alguns dados, como exemplo, aqueles relativos à preferência de temáticas de pesquisa.

Em ambas as ocasiões apresentadas se faz necessário o fornecimento de dados, os quais precisam ter fluxos bem definidos, especialmente para a realização do tratamento dos dados pessoais e/ou sensíveis. É neste sentido que se torna imprescindível discutir sobre as formas de gerenciamento e armazenamento dessas informações, com vistas a evitar possíveis violações do direito à privacidade, a partir de invasões, vazamentos ou perda de dados que possam ocasionar danos aos usuários.

Diversas investigações vêm sendo realizadas sobre a proteção de dados pessoais, principalmente direcionada ao âmbito das bibliotecas. O estudo de Bourke (2022) discute as novas funções das bibliotecas na gestão de dados de pesquisa e o depósito desses nos repositórios digitais. Dentre os aspectos identificados por este autor, é mencionada a orientação junto aos usuários sobre a proteção de dados pessoais e o uso de técnicas como anonimização e pseudonimização. A pesquisa de Varela-Orol e Ameneiros Rodríguez (2018) analisa a proteção de dados pessoais nos serviços digitais oferecidos pelas bibliotecas das universidades públicas da Espanha, e tem como base o que dispõe o Regulamento Geral sobre a Proteção de Dados (RGPD). Dentre os aspectos observados, os autores focaram na informação disponibilizada aos usuários sobre o uso dos seus dados, a segurança da conexão nas páginas web dos serviços e as ações de formação oferecidas aos usuários.

Neste sentido, verifica-se que o hodierno contexto é orientado pelo intenso uso de dados na denominada sociedade da informação, o que leva a refletir e a discutir sobre o uso indiscriminado dos dados e o direito à privacidade, enquanto direito fundamental garantido pela Constituição Federal (BRASIL, 1988). Outrossim, a questão se apresenta como temática de interesse

da Ciência da Informação (CI) por discutir um fenômeno informacional que necessita lidar com os processos que envolvem o tratamento de dados.

Em âmbito nacional, documentos legislativos como a Constituição Federal, o Marco Civil da Internet e a Lei de Acesso à Informação, apresentam diretrizes mais gerais relativas à privacidade e aos dados pessoais. Contudo, a sanção da Lei Geral de Proteção de Dados (LGPD) vem regulamentar, de forma mais precisa, o tratamento dos dados pessoais em ambientes físico ou digital, tanto por órgãos públicos quanto privados. Considerando sua vigência em meados de 2020, observa-se um cenário de ajustes e adequações que precisam se efetivar no âmbito das organizações, estando sujeitas a sanções e multas, as que não se adaptarem.

Tendo em vista que os RIs são vinculados às instituições públicas ou privadas de ensino superior e que se encontram inseridos nesse contexto, foram estabelecidas as seguintes questões de partida: Como se apresenta o cenário nacional dos marcos regulatórios sobre a privacidade e a proteção de dados? No âmbito dos repositórios institucionais, que adequações se fazem necessárias com a implementação da LGPD?

Diante disso, estabeleceu-se como objetivo geral da pesquisa discutir o cenário dos repositórios institucionais frente à Lei Geral de Proteção de Dados, com enfoque nas adequações que necessitam ser realizadas. Mais precisamente, busca-se apontar parte da legislação brasileira que trate sobre a privacidade e a proteção de dados, analisá-la e pontuar os aspectos da LGPD, que se relacionam com os repositórios institucionais.

Vale salientar que, nas propostas de adequações apresentadas neste trabalho, mais precisamente naquelas relacionadas ao ordenamento jurídico e às hipóteses legais da LGPD, orienta-se a base argumentativa ao contexto das instituições públicas de ensino superior, visto que há particularidades relativas ao tratamento pelo poder público. Contudo, compreende-se que todas as demais orientações podem ser aplicadas tanto nas instituições públicas como nas privadas de ensino superior.

Considerando que o cenário apresentado pode levar os profissionais da informação envolvidos com a gestão dos RIs a repensar os fluxos para o

tratamento dos dados, bem como levantar dúvidas quanto aos ajustes necessários, apresenta-se os aspectos teóricos e práticos que envolvem as adequações à LGPD, contribuindo com as discussões no âmbito da CI.

2 Procedimentos metodológicos

A presente pesquisa se classifica quanto aos objetivos propostos como exploratória, por buscar um aprofundamento em torno de determinado problema (TRIVIÑOS, 1987), o qual se centra nas discussões acerca da privacidade e proteção de dados a partir da aplicação dos princípios e aspectos dispostos na LGPD, no âmbito dos repositórios institucionais.

Quanto aos meios para o seu desenvolvimento, foram utilizadas a pesquisa bibliográfica e a documental, com abordagem qualitativa. A pesquisa bibliográfica foi realizada a partir de consulta às bases de dados Web of Science (WoS), Scopus, Base de Dados Referenciais de Artigos de Periódicos em Ciência da Informação (BRAPCI) e Google Acadêmico. As buscas foram feitas com os termos ‘privacidade’ e ‘proteção de dados’ associados a 'repositório institucional’, em português e em inglês, por meio do uso do operador booleano AND. Na primeira busca os resultados recuperados foram pouco expressivos, sendo 1 artigo na WoS e Scopus, a BRAPCI não retornou documentos e o Google Acadêmico apresentou alguns resultados, porém após analisar os títulos das 5 primeiras páginas, verificou-se que os assuntos privacidade e proteção de dados não se relacionavam com o contexto dos RIs.

Neste sentido, tendo em vista a baixa quantidade de resultados recuperados, foi que se optou por realizar uma segunda busca e ampliá-la a partir do uso do termo mais geral ‘repositório’ nas três primeiras bases. Desta forma, obteve-se um quantitativo maior no retorno de documentos, sendo 68 na WoS e Scopus, após eliminação dos títulos duplicados. Como a BRAPCI continuou sem retornar documentos, optou-se pela eliminação do termo ‘repositório’ buscando situar a temática na CI, assim, foram recuperados 24 artigos. Em seguida, procedeu-se a leitura dos títulos e resumos para verificar se estariam relacionados aos objetivos desta pesquisa. De modo geral, para além

dos artigos científicos também foram consultados na pesquisa bibliográfica livros, cartilhas e feitas consultas aos sites institucionais.

Em relação à pesquisa documental, foi realizada a análise dos seguintes documentos legislativos: Lei nº 12.527/2011 - Lei de Acesso à Informação (BRASIL, 2011); Lei nº 12.965/2014 - Marco Civil da Internet (BRASIL, 2014); Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (BRASIL, 2018); e o Guia Orientativo de tratamento de dados pessoais pelo poder público (BRASIL, 2022a), publicado em 2022. Vale ressaltar que o intuito de consultar esses documentos centrou-se na necessidade de buscar compreender como se situa o panorama normativo brasileiro que trata sobre a privacidade e a proteção de dados.

No que se refere à análise realizada na LGPD, objeto de estudo desta pesquisa junto aos RIs, foram feitas correlações com o disposto na Lei e o cenário dos repositórios. Desta forma, buscando sistematizar as orientações que são propostas neste estudo, procedeu-se ao estabelecimento das seguintes categorias: cadastramento, capacitação, gestão de riscos, gestão documental, gestão institucional, metadados, políticas de informação e site do RI.

3 Marcos regulatórios sobre privacidade e proteção de dados: análise do cenário nacional

As discussões em torno da privacidade e da proteção de dados pessoais têm sido ampliadas, especialmente pelo contexto tecnológico ora vivenciado, bem como pelo uso indiscriminado desses dados, para os mais diversos fins, sejam comerciais, políticos e/ou econômicos. Por outro lado, observa-se um cenário em que notícias sobre roubos ou vazamentos de dados pelas empresas vêm sendo recorrente nas mídias, como exemplos, há o caso do Mercado Livre e o vazamento de dados de cerca de 300 mil usuários, ocorrendo a mesma situação em instituições financeiras como o Bradesco (CNN BRASIL, 2022; BARROS, 2022).

Tais situações podem resultar no uso indevido dos dados pessoais e gerar problemas como "[...] fraudes e roubo de identidade (quando um terceiro se faz

passar pelo indivíduo fazendo uso de dados roubados) " ou ainda levar a pessoa a ser alvo de "[...] publicidades indesejadas ou passe a integrar (sem sua autorização) listas de e-mails ou de telemarketing de empresas" (SIEBRA; XAVIER, 2020, p. 72).

Diante disso, preocupações quanto ao uso seguro e adequado dos dados se fazem necessárias. Ademais, compreendendo que a sua disponibilidade indevida pode favorecer a identificação de um indivíduo, é que Luz e Loreiro (2018, p. 74) destacam que "Proteger a privacidade, nessa perspectiva, tornou-se um mecanismo imprescindível na garantia da liberdade e da autonomia privada frente às intervenções do Estado e da sociedade como um todo".

O direito à vida privada e à intimidade são considerados direitos fundamentais garantidos pela Declaração Universal dos Direitos Humanos e reforçados, em âmbito nacional, pela Constituição Federal de 1988, sendo invioláveis e tendo o cidadão assegurado o direito à indenização material ou moral, quando houver seu descumprimento (BRASIL, 1988; BEZERRA; WALTZ, 2014; OLIVEIRA *et al.*, 2020). Para melhor compreender do que trata a privacidade e a intimidade, apresenta-se a seguir a definição apontada por Bezerra e Waltz (2014, p. 162), em que:

> A privacidade refere-se a tudo o que o indivíduo não pretende que seja de conhecimento público, reservado apenas aos integrantes de seu círculo de convivência particular, enquanto a intimidade diz respeito única e exclusivamente ao indivíduo. Esses direitos se estendem ao domicílio, à correspondência, às comunicações e aos dados pessoais. (BEZERRA; WALTZ, 2014, p. 162).

A popularização da internet junto aos mais diversos artefatos e meios tecnológicos facilitou os processos de comunicação e uso da informação. Conforme ressaltam Martins, Jorgetto e Sutti (2019, p. 711), "o advento da Sociedade da Informação, principalmente a partir das últimas duas décadas, acabou por mitigar, em certos aspectos, o que se concebe por vida privada".

Neste sentido, dentre alguns fatores, pode-se ressaltar a praticidade e a ampla oferta de serviços digitais oferecidos, que vão desde a solicitação de benefícios ao governo, emissão de documentos pessoais, até a realização de transações bancárias, compras on-line, consulta a produtos, dentre outros. A

utilização desses vários serviços ofertados pelas empresas coloca o cidadão em um cenário de exposição de dados pessoais e de informações da sua vida privada, os quais se intensificam à medida em que ele passa a fazer mais uso.

Ainda de acordo com Martins, Jorgetto e Sutti (2019), a fase de geração de dados consiste naquela em que o usuário está no controle e pode alimentar o sistema de duas maneiras: ativa ou passiva. Para estes autores, na maneira ativa, o fornecimento dos dados pelo indivíduo ocorre de modo consciente a um terceiro; já na forma passiva, ao contrário, isso ocorre inconscientemente, como é o caso de um rastreio do comportamento do usuário em determinado site, por exemplo. Buscando garantir certa segurança e viabilizar autonomia ao usuário quanto ao uso dos seus dados pessoais, é que leis vêm sendo sancionadas para regulamentar e evitar violações à privacidade.

No cenário nacional, algumas leis tratam sobre aspectos pontuais quanto ao direito à privacidade e a proteção dos dados pessoais. A Lei nº 12.527/2011, popularmente chamada de Lei de Acesso à Informação (LAI), regula os procedimentos relativos à promoção da transparência e do acesso às informações pelos órgãos públicos vinculados à União, Estados e Municípios (BRASIL, 2011). As principais características da LAI centram-se na publicização das informações de interesse público, como regra geral, além de evidenciar a transparência como cultura necessária à administração pública. Busca por meio da sua efetivação prestar contas à sociedade dos recursos públicos que são geridos pelo Estado.

Nesta Lei, observa-se que não é apresentada a expressão "dado pessoal", mas sim "informação pessoal", sendo definida no Art. 4º, inciso IV, como "aquela relacionada à pessoa natural identificada ou identificável" (BRASIL, 2011). Outrossim, estabelece que o "tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" (BRASIL, 2011). De forma geral, percebe-se que a LAI prioriza a promoção do acesso à informação pública, enquanto mantém os princípios dos direitos fundamentais relativos às informações pessoais.

Outra lei que também reforça tais princípios é a Lei nº 12.965/2014, mais

conhecida como o Marco Civil da Internet, que regulamenta as diretrizes para o uso da internet no Brasil e, dentre os princípios estabelecidos, aponta a proteção da privacidade e dos dados pessoais (BRASIL, 2014). Partindo do pressuposto de que no hodierno contexto o acesso à internet se apresenta como recurso necessário para o exercício da cidadania, pois as pessoas precisam dela para realizar diversas atividades, é que se torna fundamental garantir que o pleno direito de acesso à internet seja compatível com o direito à intimidade e à privacidade.

Teffé e Moraes (2017) consideram que a Lei nº 12.965/2014 está alicerçada no tripé axiológico constituído pelos princípios da neutralidade da rede, da privacidade e da liberdade de expressão, os quais estão intimamente relacionados. Estabelecer o equilíbrio entre eles torna-se necessário, tendo em vista que "Enquanto a neutralidade da rede reforça a liberdade de expressão, a privacidade representa seu limite" (TEFFÉ; MORAES, 2017, p. 112).

Desta forma, o Marco Civil da Internet assegura, quanto aos dados pessoais, em seu Art. 7º, os seguintes direitos e garantias: "I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação"; "VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei"; e no inciso "IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais" (BRASIL, 2014). Conforme visto, aponta-se a necessidade do usuário em consentir o uso dos seus dados pessoais tendo melhor controle sobre eles, evitando o uso indiscriminado pelas empresas, além de ter garantida a indenização em caso de danos resultantes da violação.

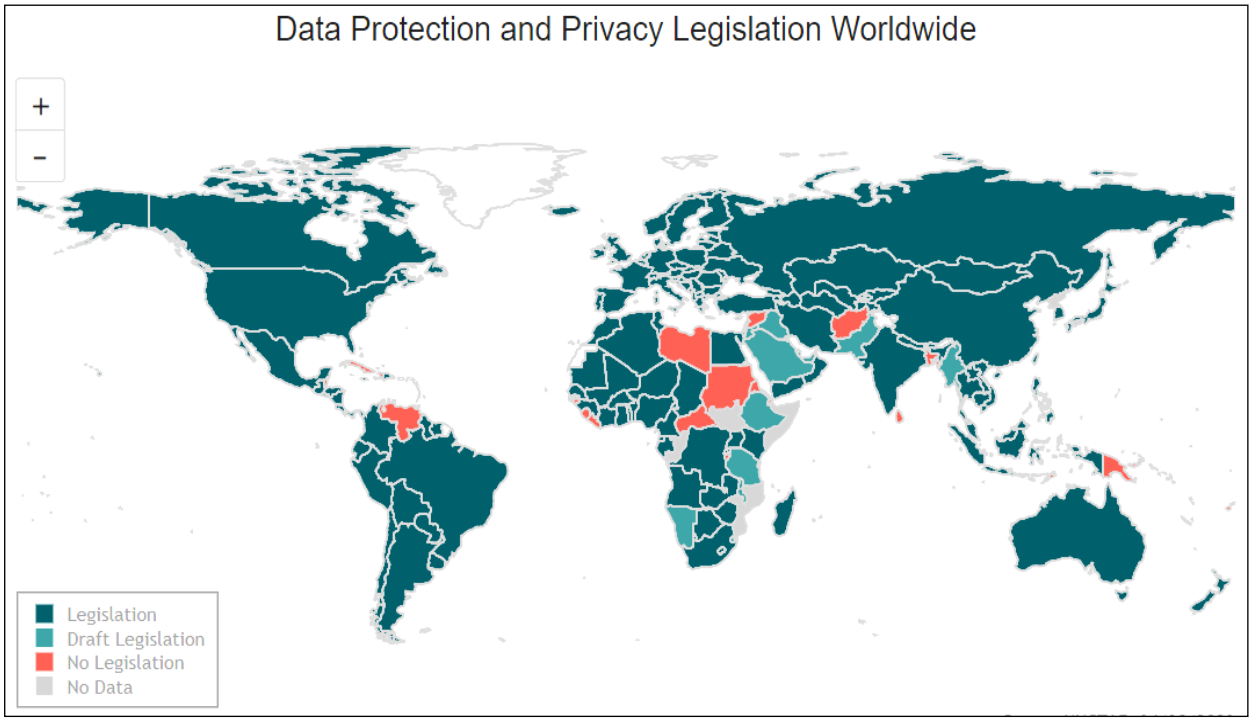
A lei mais recente que trata de forma direcionada, ampla e precisa sobre a proteção e o tratamento dos dados pessoais em ambientes físico ou digital é a Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), a qual será explanada na próxima subseção.

3.1 Lei Geral de Proteção de Dados: objetivos e princípios

A Lei Geral de Proteção de Dados foi sancionada em 14 de agosto de 2018 e tem como finalidade proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018). Quanto às suas bases, a lei brasileira foi inspirada na legislação europeia, ou seja, no *General Data Protection Regulation* (GDPR), em português, Regulamento Geral sobre a Proteção de Dados (RGPD), que regula as regras de privacidade e proteção de dados pessoais em todos os Estados-membros da União Europeia (UE) (SANTOS; CARVALHO, 2020; MASSENO; MARTINS; FALEIROS JÚNIOR, 2020; AL-ABDULLAH *et al.*, 2020).

Cada país tem autonomia para estabelecer as regulamentações sobre a privacidade e a proteção de dados pessoais, em seu território. A Figura 1 apresenta o panorama dessas legislações ao redor do mundo, a partir de uma pesquisa realizada em dezembro de 2021, pela United Nations Conference on Trade and Development (UNCTAD).

Figura 1 - Legislação sobre proteção de dados pessoais e privacidade ao redor do mundo



Fonte: United Nations Conference on Trade and Development (2021).

Segundo os dados do estudo, observa-se que a maioria dos países, cerca de 71%, dispõem de legislação que busca garantir a privacidade e a proteção dos dados pessoais; outros nove% abrangem países com projetos legislativos; há também um percentual significativo de países, englobando cerca de 15%, que ainda estão sem instrumentos legais implementados; e, por fim, em cinco% dos países não foi possível obter dados. Diante disso, verifica-se que o tema da privacidade e da proteção dos dados pessoais vem sendo debatido em vários países ao redor do mundo. Some-se a isso a adoção de ações e os níveis de adequação em todos os continentes, embora alguns apresentem graus mais satisfatórios e outros menos.

Em âmbito nacional, a LGPD define os fundamentos, as diretrizes para o tratamento dos dados pessoais e as sanções administrativas para os casos de descumprimento. Sua aplicação está direcionada tanto para os órgãos públicos quanto para as empresas privadas. Depois de sancionada, a LGPD estabeleceu a sua vigência após o período de dois anos, ou seja, a partir de 14 de agosto de 2020, este prazo foi necessário para que todas as instituições pudessem implementá-la e proceder os ajustes e as adequações necessárias.

Contudo, neste período, todo o mundo vivenciava a pandemia da covid-19, que atingiu os diversos setores, econômico, social e político. Assim, em dez de junho de 2020, foi sancionada a Lei nº 14.010, que dentre as medidas de caráter emergencial apresentadas manteve a vigência da LGPD, porém um novo prazo para a aplicação das multas e sanções foi estabelecido, passando a valer a partir de primeiro de agosto de 2021 (BRASIL, 2020b).

O enfoque da LGPD é possibilitar maior "transparência ao armazenamento, ao tratamento e à disponibilização de dados pessoais das cidadãs e cidadãos, seja pelas empresas de redes sociais e outras entidades privadas, seja pelo próprio poder público" (BERNARDI *et al.*, 2022, p. 110). A partir da análise realizada nesta Lei, fica claro o estabelecimento de um efetivo papel ativo ao titular como aquela "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (BRASIL, 2018), sendo garantidos os direitos de obter do controlador o acesso aos dados, a confirmação, a

anonimização, o bloqueio ou a eliminação, a portabilidade e a revogação do consentimento, quando for o caso (BRASIL, 2018). Deste modo, pode-se dizer que a LGPD permite que o titular tenha determinado controle sobre seus dados pessoais, a partir de limites bem claros e estabelecidos.

Em relação a algumas definições apresentadas na Lei, ressalta-se aqui duas consideradas essenciais para a discussão, "dado pessoal" e "dado pessoal sensível". Dado pessoal configura-se como "a informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). O dado pessoal se apresenta como toda e qualquer informação que permita identificar uma pessoa física. Vale aqui salientar que não se insere no rol de proteção da LGPD a pessoa jurídica.

A identificação pode ser caracterizada como direta ou indireta, sendo a primeira referente àquele dado cujo acesso possibilita o reconhecimento imediato da pessoa, como por exemplo, Registro Geral (RG), Cadastro de Pessoa Física (CPF), título de eleitor, nome completo, entre outros; já a segunda é aquela que possibilita, a partir da combinação com outras informações, a identificação do indivíduo (ou seja, passível de identificação) como endereço, placa de automóvel, número de telefone etc. (VARELA-OROL; AMENEIROS RODRÍGUEZ, 2018).

No que tange ao dado pessoal sensível, a LGPD o aponta como:

> [...] dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

Para este tipo de dado, a LGPD conferiu maior proteção, por estar diretamente relacionado aos aspectos mais íntimos da vida de uma pessoa (PERNAMBUCO, 2021). Neste sentido, entende-se que um possível extravio desses dados pode trazer consequências danosas à vida de um indivíduo, de forma a atingir aspectos financeiros, sociais ou emocionais.

No que se refere aos princípios estabelecidos (Quadro 1), a Lei define que o tratamento de dados precisa considerar a boa-fé e mais dez princípios,

sendo eles:

Quadro 1 - Princípios da LGPD

PRINCÍPIOS	ESPECIFICAÇÃO
1. Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular.
2. Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular.
3. Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades.
4. Livre Acesso	Garantia de consulta facilitada e gratuita aos titulares.
5. Qualidade dos dados	Garantia de exatidão, clareza, relevância e atualização dos dados aos titulares.
6. Transparência	Informações claras, precisas e facilmente acessíveis sobre o tratamento.
7. Segurança	Uso de medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados.
8. Prevenção	Adoção de medidas para prevenir a ocorrência de danos aos titulares.
9. Não discriminação	Não utilização para fins discriminatórios, ilícitos ou abusivos.
10. Responsabilização e prestação de contas	Adoção de medidas para comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Fonte: Adaptado pelas autoras da LGPD (BRASIL, 2018).

Dentre os princípios apresentados, optou-se por focar as discussões nos três primeiros. Assim, pode-se dizer que o princípio da **finalidade** corresponde ao escopo da atividade a ser realizada pela instituição, que justifique o tratamento dos dados pessoais, desde que devidamente informado ao titular dos dados. No que concerne à **adequação**, relaciona-se a conformidade entre os dados que são solicitados e a finalidade apresentada ao titular. Por fim, quanto ao princípio da **necessidade**, enquadra-se aqui a regra do mínimo necessário, em que é orientado solicitar somente aqueles dados que são essenciais e suficientes para atender à finalidade proposta. Em outras palavras, o enfoque é retirar os excessos e tratar somente os dados primordiais.

Ante o exposto, é preciso frisar que no caso do setor público, o tratamento dos dados precisa fundamentar-se em uma finalidade **pública**, legítima e amparada em uma base legal; **específica**, estando orientada a uma ação em particular; **explícita**, apresentando-se de forma clara; e **informada**, ou seja, comunicada e disponível de maneira compreensível e em linguagem simples ao titular dos dados (BRASIL, 2022a, grifo nosso).

Ainda que a discussão acima esteja centrada nos três primeiros princípios, considera-se primordial ressaltar que todos os dez são fundamentais para direcionar as boas práticas à efetivação da salvaguarda e do tratamento dos dados pessoais. De modo geral, compreende-se que a LGPD vem reforçar a transparência aos titulares dos dados pessoais quanto aos processos envolvidos em seu tratamento, trata-se de uma perspectiva do uso ético e da transparência dos processos, de forma que o indivíduo esteja ciente do porquê, para quê finalidade e que tratamento será dispensado aos seus dados.

Com base no que foi apresentado, percebe-se que a legislação anterior à LGPD traz questões relacionadas ao direito à privacidade e aos dados ou informações pessoais, contudo, de forma mais fragmentada, sem demais aprofundamentos e especificidades. Assim, buscando efetivar maior rigor à pauta da privacidade e da proteção dos dados pessoais, além de apresentar diretrizes e sanções mais consistentes, foi que a LGPD teve sucesso em sua regulamentação concreta. Por outro lado, observa-se ainda um longo caminho a ser percorrido na implementação das adequações, das boas práticas nas organizações públicas e privadas, e da busca por soluções mediante os desafios encontrados.

É neste cenário que se busca apresentar na próxima seção os aspectos que envolvem os repositórios institucionais em relação à LGPD e, a partir daí, recomendar orientações para as adequações que se fazem necessárias.

4 Repositórios institucionais à luz da LGPD

O avanço dos recursos tecnológicos oportunizou o desenvolvimento de ferramentas que auxiliam no gerenciamento das produções acadêmicas e científicas, dentre elas estão os repositórios institucionais (RIs). Os RIs têm

como principal finalidade gerenciar, garantir a guarda, preservar e prover a ampla disseminação da informação científica, artística, cultural e/ou administrativa que são desenvolvidas nas instituições (SAYÃO *et al.*, 2009). Em outras palavras, os RIs são responsáveis por agregar toda a produção intelectual de determinada instituição (SHINTAKU; SUAIDEN, 2015).

Além de permitir o registro e o armazenamento das produções, os repositórios oportunizam acessá-las com uma maior rapidez e de qualquer lugar que disponha do acesso à internet, perpassando assim as barreiras de espaço e tempo. Considerando que para isso o fornecimento de alguns dados pessoais se faz necessário, seja para o depósito ou para a realização de cadastro no sistema para a oferta de serviços personalizados, é que atenção especial precisa ser dada para evitar o descumprimento de quaisquer aspectos da LGPD.

Centrando as discussões nas instituições públicas de ensino superior, enquanto detentoras dessas ferramentas, verifica-se que elas precisam atentar-se às novas diretrizes regulatórias sobre o tratamento e a proteção dos dados pessoais, tendo em vista se inserirem no rol do tratamento pelo poder público. No âmbito da Lei, as universidades, enquanto pessoa jurídica de direito público, atuam como o 'controlador', que é "[...] a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018).

Em outras palavras, é a quem concerne decidir que dados serão tratados, a definição da finalidade que justificam o uso dos dados e os elementos essenciais dos meios de tratamento (PERNAMBUCO, 2021). Ademais, é atribuído ao controlador o dever de adotar medidas que garantam a transparência do tratamento dos dados pessoais em seu legítimo interesse (BRASIL, 2018).

Segundo o Art. 23 da LGPD, o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (BRASIL, 2018). As instituições públicas devem informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas

atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; indicar um encarregado de dados quando realizam operações de tratamento de dados pessoais, nos termos do art. 39 da LGPD (BRASIL, 2022a).

Uma das principais providências a serem tomadas antes de realizar o tratamento de dados pessoais é a de identificar a base legal aplicável. O tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas nos art. 7º e art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais, no âmbito do Poder Público.

Com relação às políticas públicas, deve-se considerar a existência de ato formal que institui a política pública, o que pode ocorrer mediante ato normativo (lei ou regulamento) ou por ajustes contratuais (contratos, convênios e instrumentos congêneres), ou pela definição de um programa ou ação governamental específica, a ser executado por uma entidade ou por um órgão público.

As universidades públicas devem cumprir a LGPD, pois fazem parte da administração direta e respondem administrativamente por seus atos. Ao não adequar seus processos à LGPD, podem sofrer sanções administrativas impostas pela Autoridade Nacional de Proteção de Dados (ANPD) e processos jurídicos impostos pelos titulares dos dados.

A LGPD é uma oportunidade de adequar processos que promovam mais segurança e sistematização do tratamento de dados pessoais, requer treinamentos e investimentos, contudo, a não adequação pode trazer inúmeras consequências, como até mesmo o fechamento de universidades e perda de credibilidade, ao ter problemas de vazamento de dados pessoais.

Nesse contexto, os repositórios institucionais, como parte do conjunto de serviços ofertados pelas universidades públicas, e ferramenta tecnológica que precisa dispor de equipe técnica multidisciplinar e gestão para sistematizar as demandas, necessitam revisitar tanto as práticas adotadas como os documentos institucionais que regulamentam seu uso em âmbito institucional, buscando identificar que ajustes e adequações serão necessários realizar. Desta forma,

com base no disposto na LGPD e a partir da análise dos trabalhos de Carvalho (2020), Lemos e Passos (2020) e Pernambuco (2021), são apresentadas a seguir algumas propostas que podem colaborar com as adaptações dos RIs à LGPD.

4.1 RI e LGPD: propostas para a adequação

Carvalho (2020), em um estudo sobre a aplicação da LGPD nas instituições de educação, considera que a primeira medida a ser tomada é a realização do mapeamento dos dados pessoais e do seu ciclo de vida na instituição, pois a partir disso será possível identificar os riscos mais elevados no tratamento e na segurança desses dados.

Corroborando com a autora e fazendo um paralelo com os RIs, sugere-se realizar este trabalho primordial de **mapear o fluxo de atividades do RI** (quanto ao cadastramento, padrão de metadados, gestão documental e outros), buscando identificar os dados pessoais e/ou dados pessoais sensíveis que são solicitados. Essa ação permitirá realizar um diagnóstico situacional do panorama atual e possibilitará fazer as revisões e adequações posteriores. A partir disso, observa-se como necessário também proceder uma análise e avaliação quanto à real demanda de fornecimento desses dados pelos usuários considerando, especialmente, os princípios da finalidade, adequação e necessidade. O foco aqui é solicitar somente o essencial, o mínimo possível, tendo uma justificativa razoável para o seu fornecimento pelo titular.

Para que se possa realizar o tratamento de dados pessoais e/ou dados pessoais sensíveis, é essencial **fundamentar a necessidade** e **amparar-se em uma das hipóteses legais** previstas nos artigos 7º e 11 da LGPD (BRASIL, 2018). Assim, é importante que os gestores de RI as verifiquem e elaborem os argumentos baseando-se em ordenamento jurídico que justifique o tratamento de dados pelo RI.

No âmbito do Poder Público, particularidades precisam ser observadas. Conforme o disposto no Guia Orientativo da Autoridade Nacional de Proteção de Dados (BRASIL, 2022a), algumas bases legais têm uso limitado ao setor público, como é o caso do consentimento pelo titular e os interesses legítimos do controlador. Essas bases podem ser consideradas como bases legais residuais,

não sendo recomendado o seu uso para a justificativa de tratamento dos dados pessoais pelos RIs, visto que a função do repositório se direciona mais ao cumprimento de obrigações, seja para cumprir exigências de órgãos superiores (como o Ministério da Educação (MEC), por exemplo) ou atender normativas organizacionais da instituição.

Desta forma, considera-se pertinente basear-se na hipótese da obrigação legal ou regulatória pelo controlador, a qual dispensa a necessidade de consentimento do titular, contudo, mantém-se a necessidade de atender todos os princípios já mencionados e as garantias do titular, previstas na Lei.

Dentre alguns documentos que podem ser utilizados para embasar os argumentos, estão as normativas governamentais do MEC, mais especificamente o "Instrumento de avaliação de cursos de graduação", do Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), que aponta a necessidade de depósito dos Trabalhos de Conclusão de Cursos (TCC) em repositório institucional próprio, como requisito necessário para o alcance do conceito cinco (INEP, 2017a, 2017b).

Outrossim, a Portaria da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) nº 13/2006, que dispõe sobre a disponibilização de teses e dissertações na internet, também pode contribuir com a construção dos argumentos, ou, ainda, a Portaria nº 36/2022, do MEC, que trata sobre a conversão do acervo acadêmico[1] das instituições federais de ensino superior para o meio digital, e veda a produção de novos documentos referentes ao acervo acadêmico dos discentes em suporte físico (BRASIL, 2022b).

De forma geral, os documentos acima mencionados podem colaborar com a formulação inicial dos argumentos baseados em ordenamento jurídico para justificar o tratamento dos dados pelos RIs. Ademais, outros documentos institucionais, que estabeleçam normas da organização como estatutos, regimentos, instruções normativas ou portarias também podem ser utilizados para melhor fundamentar o embasamento. Assim, vale frisar que os dados pessoais poderão ser coletados e tratados, desde que devidamente justificados em uma das hipóteses legais e observando os princípios definidos na Lei.

Tendo fundamento em uma das hipóteses legais e realizado o

mapeamento do fluxo de atividades do RI, pode-se partir para as discussões em torno do **tratamento dos dados**. Segundo a LGPD, em seu Art. 5º, inciso X, o tratamento de dados consiste em:

> [...] 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).

Como visto, o tratamento envolve atividades que são realizadas ao longo do ciclo de vida dos dados, desde a sua criação até o seu uso final. Buscando melhor sistematizar todas essas atividades, o Guia de boas práticas para implementação da LGPD na administração pública (BRASIL, 2020a) as divide em cinco fases, conforme mostra a Figura 2.

Figura 2 - Ciclo de vida dos dados pessoais

Fonte: Brasil (2020a).

Segundo o Guia, o processo de coleta de dados envolve: o momento em que os dados pessoais são gerados, produzidos ou recepcionados; a retenção compreende o arquivamento ou o armazenamento desses; a etapa de processamento abrange as operações de classificação, utilização, reprodução, avaliação ou controle da informação, extração e a modificação dos dados pessoais pelo controlador; o compartilhamento engloba a transmissão, a distribuição, a comunicação, a transferência e a difusão; e por último, a eliminação contempla a destinação final do dado (BRASIL, 2020a). No que se refere ao acesso, os autores frisam que ele se faz presente em todas as etapas, visto que é uma condição fundamental para as demais.

No que tange a etapa de eliminação neste fluxo, considera-se necessário mencionar a importância do documento "Classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da Administração Pública", do Conselho Nacional de Arquivos (CONARQ)

(CONSELHO NACIONAL DE ARQUIVOS, 2001), para que sejam estabelecidos os critérios para esta última etapa do ciclo de vida dos dados pessoais. Torna-se também fundamental ressaltar a realização deste trabalho pelos profissionais arquivistas, os quais possuem *expertise* na área de seleção e descarte de documentos, assim, acredita-se que eles possam contribuir com sua aplicação no âmbito dos dados pessoais.

Ainda em relação aos aspectos voltados para o tratamento dos dados pessoais, é apontada na LGPD a responsabilidade do controlador em adotar ações que possam mitigar os riscos de perda ou extravio dos dados pessoais dos titulares. Para que isso ocorra, se faz necessário planejar e efetivar "técnicas adequadas e específicas a assegurar a disponibilidade, integridade e confidencialidade de todas as formas de informação, durante todo o ciclo de vida dos dados, até o seu descarte" (CARVALHO, 2020, p. 125).

Nesse sentido, observa-se clara preocupação em garantir a segurança desses dados, além de estabelecer a definição prévia de medidas de prevenção que evitem possíveis danos à privacidade dos titulares, sendo inclusive mensurada a necessidade de registro no relatório de impacto (BRASIL, 2018). Desta forma, sugere-se a realização do **mapeamento dos possíveis riscos** que venham a ocorrer, considerando os parâmetros escalares que são utilizados para representar os níveis de probabilidade e do impacto do risco (BRASIL, 2020c). Outrossim, a definição de estratégias para prevenir e mitigar os riscos e de como proceder nos casos de incidentes, também são necessárias.

A atuação da instituição enquanto controladora e responsável pelo tratamento e segurança dos dados pessoais requer da sua gestão a realização de um trabalho conjunto, integrado e participativo que envolva todos os setores que a compõem e seus respectivos representantes. Acredita-se que a partir disso será possível proceder a realização de uma discussão institucional, que busque o planejamento e o estabelecimento de processos e de fluxos de trabalho, para o efetivo tratamento dos dados pessoais, conforme preconiza a LGPD. Assim, sugere-se a **participação do gestor do RI nessas discussões institucionais**; além disso, caso a instituição já disponha de uma política institucional de privacidade ou de proteção de dados, recomenda-se que o profissional busque

apropriar-se das diretrizes que nela constam; e caso a instituição não disponha, que ele possa contribuir junto a uma equipe multidisciplinar na sua construção.

Após serem definidas as novas diretrizes e práticas institucionais para o tratamento e segurança dos dados pessoais, sugere-se a **revisão das políticas do RI** para verificar a necessidade de alterações na normativa vigente e que novas definições precisam ser incorporadas. Entende-se que a revisão constante das políticas é um trabalho primordial para mantê-las sempre atualizadas e concernentes com a sua finalidade.

Outro aspecto necessário é priorizar a **transparência** de modo que a comunidade que utiliza o RI esteja ciente acerca dos dados pessoais que o repositório coleta, para qual finalidade e que tratamento é destinado a eles. Ter a clareza desses procedimentos pode trazer mais segurança para os usuários. Acerca disso, Lemos e Passos (2020) orientam a alocação de um espaço no site das bibliotecas para apresentar tais informações. Entende-se como necessária a aplicação dessa mesma orientação aos RIs, trazendo assim mais esclarecimentos à comunidade interna e externa.

Por último, sugere-se como orientação, também de suma importância, a capacitação de todos os funcionários que estão envolvidos com as demandas relativas ao repositório institucional, aqui incluídas tanto a equipe técnica como as equipes de apoio. As **ações de capacitação** envolveriam a realização de treinamentos junto às equipes para apresentar as novas diretrizes norteadoras e orientar quanto aos novos procedimentos adotados em cada fluxo de trabalho, visando garantir um efetivo tratamento e a segurança dos dados pessoais.

Face ao exposto, buscando sistematizar todas as orientações que foram propostas, é apresentada no Quadro 2 uma síntese de cada uma delas, a partir da organização por categorias e suas respectivas especificações.

Quadro 2 - Síntese das orientações para a adequação dos RIs à LGPD

Categoria	Orientação
Cadastramento	1. Mapear os dados pessoais e/ou sensíveis utilizados no cadastramento do perfil de usuários, buscando considerar os princípios da finalidade, adequação e necessidade, solicitando apenas aqueles dados considerados essenciais.

Categoria	Orientação
Capacitação	2. Realizar treinamentos junto à equipe técnica dos repositórios, bem como com os demais funcionários envolvidos nas demandas relativas ao RI, para orientar quanto aos novos procedimentos e fluxos de trabalho para a proteção dos dados pessoais.
Gestão de risco	3. Identificar por meio de um mapeamento os possíveis riscos considerando a probabilidade e o impacto que podem envolver a perda e o extravio dos dados pessoais. A partir disso definir estratégias para prevenir e mitigar os riscos e como proceder nos casos de incidentes.
Gestão documental	4. Mapear o ciclo de vida dos dados pessoais nos arquivos físico e digital: coleta, uso, armazenamento, eliminação e outros.
Gestão institucional	5. Participar das discussões institucionais relativas ao estabelecimento de processos e fluxos que compreendam o ciclo do tratamento dos dados pessoais e sensíveis; bem como apropriar-se da política institucional de privacidade ou de proteção de dados, caso a instituição já disponha; caso não, contribuir junto a uma equipe multidisciplinar com a sua elaboração.
Metadados	6. Proceder ao mapeamento dos padrões de metadados de cada tipo de documento para identificar os dados pessoais e/ou sensíveis solicitados. Revisar e basear-se nos princípios da finalidade, adequação e necessidade.
Políticas de informação do RI	7. Revisar as políticas de informação do RI buscando realizar as adequações necessárias a partir das novas diretrizes institucionais.
Site do RI	8. Disponibilizar na página do RI uma seção com informações acerca da coleta, finalidade e tratamento dos dados pessoais.

Fonte: Elaborado pelas autoras.

Desta forma, é importante ressaltar que foram apresentadas aqui apenas algumas possíveis ações a serem realizadas, sem querer esgotar o assunto, pois acredita-se que outros estudos também poderão colaborar com a temática, apresentando novas proposições teóricas e práticas para os RIs.

5 Considerações finais

Esta pesquisa discutiu a LGPD e suas aplicações no âmbito dos repositórios institucionais. Para tanto, discorreu-se sobre alguns marcos regulatórios que tratam sobre a privacidade e a proteção dos dados pessoais, no âmbito do

cenário nacional. Conforme esclarecido, foram utilizadas como base a LAI e o Marco Civil da Internet, que evidenciam diretrizes mais pontuais sobre os dados pessoais, além da LGPD que traz maior rigor e consistência, especialmente na definição regras e sanções mais precisas para os casos de descumprimento.

No que se refere aos repositórios institucionais, observou-se que a literatura científica carece de discussões sobre a temática, entretanto, a partir das análises realizadas junto à LGPD, foi verificado que adequações precisam ser realizadas para se estar em conformidade com o previsto na referida Lei.

Assim, foram sistematizadas propostas quanto aos ajustes que precisam ser feitos, principalmente no que se referem: (1) ao mapeamento de processos e fluxos de trabalho, com vistas a identificar os dados pessoais e/ou sensíveis que são atualmente coletados; (2) a fundamentação da necessidade de tratamento desses dados e o alinhamento às hipóteses legais previstas na Lei; (3) à revisão de documentos institucionais e das próprias políticas dos RIs, com o intuito de ajustar às novas diretrizes a serem adotadas; (4) à oferta de capacitação às equipes de trabalho para orientar os novos procedimentos destinados ao tratamento dos dados; e (5) à adoção de estratégias que orientem maior transparência às práticas de tratamento dos dados pessoais adotadas.

Diante disso, conclui-se que as discussões sobre a privacidade e a proteção dos dados pessoais precisam ser mais fomentadas na sociedade, pois é necessário que se desenvolva nova cultura que se preocupe com a salvaguarda desses dados, sendo fundamental estender esse diálogo às instituições e aos repositórios institucionais. Considera-se que os objetivos estabelecidos foram alcançados e sugere-se que futuras investigações analisem outros aspectos sobre os dados pessoais nas políticas e nos sites dos RIs ou averiguem a percepção e a prática dos gestores.

No que se refere às limitações da pesquisa, pode-se mencionar a análise acerca da privacidade e da proteção de dados pessoais circunscrita a três leis: LAI, Marco Civil da Internet, LGPD e ao *Guia Orientativo de tratamento de dados pessoais pelo poder público*. Neste sentido, acredita-se que outras leis podem abranger essas discussões, entretanto para atender os objetivos estabelecidos, a delimitação foi necessária e contribuiu para responder às

questões de pesquisa, além de ter possibilitado trazer reflexões quanto à premente necessidade de proteção dos dados pessoais no âmbito das universidades e, mais precisamente, nos repositórios.

Referências

AL-ABDULLAH, Muhammad *et al.* Designing privacy-friendly data repositories: a framework for a blockchain that follows the GDPR. **Digital Policy, Regulation and Governance,** United Kingdom, v. 22, n. 5/6, p. 389-411, 2020. Disponível em: https://https://doi.org/10.1108/DPRG-04-2020-0050. Acesso em: 9 jun. 2022.

BARROS, Matheus. Bradesco financiamentos anuncia possível vazamento de dados de 53 mil clientes. **Olhar Digital**, São Paulo, 17 maio 2022.

BERNARDI, Ana Julia *et al*. **10 anos da lei de Acesso à Informação**: de onde viemos e para onde vamos. São Paulo: Artigo 19, 2022.

BEZERRA, Arthur Coelho; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil. **Revista de Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura**, Florianópolis, v. 16, n. 2, p.157-171, maio/ago. 2014.Disponível em: https:// http://ridi.ibict.br/handle/123456789/858. Acesso em: 30 maio 2022.

BOURKE, Thomas. Bibliographic control of research datasets: reflections from the EUI library. **Italian Journal of Library Science, Archival Science and Information Science,** Firenze, v. 13, n. 1, p. 321-334, 2022. Disponível em: https:// https://doi.org/10.4403/jlis.it-12723. Acesso em: 28 jul. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo**: tratamento de dados pessoais pelo poder público. Brasília: ANPD, 2022a.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília: Presidência da República, 1988.

BRASIL. Governo Federal. **Guia de boas práticas**: Lei Geral de Proteção de Dados (LGPD). Brasília: o Governo, 2020a.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal [...]. **Diário Oficial da União**: seção 1, Brasília, ano 148, n. 221-A, p. 1, 18 nov. 2011.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**: seção 1, Brasília, ano 151, n. 77, p. 1, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**: seção 1, Brasília, ano 155, n. 157, p. 59, 15 ago. 2018.

BRASIL. Lei nº 14.010, de 10 de junho de 2020. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (covid-19). **Diário Oficial da União**: seção 1, Brasília, ano 158, n. 111, p. 1, 12 jun. 2020b.

BRASIL. Ministério da Economia. **Guia de Avaliação de Riscos de Segurança e Privacidade**: Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, nov. 2020c.

BRASIL. Ministério da Educação. Portaria nº 360, de 18 de maio de 2022. Dispõe sobre a conversão do acervo acadêmico para o meio digital. **Diário Oficial da União**: seção 1, Brasília, ano 160, n. 94, p. 40, 19 maio 2022b.

CARVALHO, Adriana Cristina França Leite de. Da segurança e das boas práticas LGPD na educação. *In*: SANTOS, Regiane Martins dos; CARVALHO, Adriana Cristina França Leite de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: OAB, 2020. Cap. 9, p. 122-135.

CNN BRASIL. **Dados de cerca de 300 mil usuários do Mercado Livre vazam**. São Paulo, CNN Brasil, 8 mar. 2022.

CONSELHO NACIONAL DE ARQUIVOS (Brasil). **Classificação, temporalidade e destinação de documentos de arquivo relativos às atividades-meio da Administração Pública**. Rio de Janeiro: Arquivo Nacional, 2001.

COSTA, Michelli Pereira da; LEITE, Fernando César Lima. **Repositórios institucionais da América Latina e o acesso aberto à informação científica**. Brasília: IBICT, 2017.

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. Sistema Nacional de Avaliação da Educação Superior. **Instrumento de avaliação de cursos de graduação**: presencial e a distância: autorização. Brasília: INEP, 2017a.

INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. Sistema Nacional de Avaliação da Educação Superior. **Instrumento de avaliação de cursos de graduação**: presencial e a distância: reconhecimento e renovação de reconhecimento. Brasília: INEP, 2017b.

LEMOS, Amanda Nunes Lopes Espiñeira; PASSOS, Edilenice. A adequação das bibliotecas à Lei Geral de Proteção de Dados. **Cadernos de Informação Jurídica**, Brasília, v. 7, n. 1, p. 85-103, jan. /jun. 2020. Disponível em: https://www.arca.fiocruz.br/handle/icict/43226. Acesso em: 10 maio 2022.

LUZ, Pedro Henrique Machado da; LOREIRO, Maria Fernanda Battaglin. Privacidade e proteção de dados pessoais: os novos desafios na sociedade em rede. **Meritum**, Belo Horizonte, v. 13, n. 1, p. 69-86, jan. /jun. 2018.

MARTINS, Marcelo Guerra; JORGETTO, Leonardo Felipe de Melo Ribeiro Gomes; SUTTI, Alessandra Cristina Arantes. Big data e a proteção do direito à privacidade no contexto da sociedade da informação. **Revista Jurídica Cesumar**, Maringá**,** v. 19, n. 3, p. 705-725, set. /dez. 2019. Disponível em: https://10.17765/2176-9184.2019v19n3p705-725. Acesso em: 18 maio 2022.

MASSENO, Manuel David; MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. A segurança na proteção de dados: entre o RGPD europeu e a LGPD brasileira. **Revista do Cejur: Prestação Jurisdicional**, Florianópolis, v. 8, n. 1, p. 1-28, 2020. Disponível em: https://doi.org/10.37497/revistacejur.v9i1.367. Acesso em: 10 maio 2022.

OLIVEIRA, Adriana Carla Silva de *et al.* Empoderamento digital, proteção de dados e LGPD. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, João Pessoa, v. 15, n. 3, p. 247-261, 2020.

PERNAMBUCO (Estado). Secretaria da Controladoria-Geral. **Manual de proteção de dados pessoais.** Recife: SCGE, 2021.

SANTOS, Regiane Martins dos; CARVALHO, Adriana Cristina França Leite de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: OAB, 2020.

SAYÃO, Luis *et al.* (org.). **Implantação e gestão de repositórios institucionais**: políticas, memória, livre acesso e preservação. Salvador: EDUFBA, 2009.

SHINTAKU, Milton; SUAIDEN, Emir. Repositório institucional como componente de sistemas de informação gerencial para universidades. **Biblos**: **Revista do Instituto de Ciências Humanas e da Informação**, Rio Grande, v. 29, n. 1, p. 28-40, 2015.

SIEBRA, Sandra de Albuquerque; XAVIER, Gabriela Araújo Cavalcanti. Políticas de privacidade da informação: caracterização e avaliação. **Biblos**: **Revista do Instituto de Ciências Humanas e da Informação**, Rio Grande, v. 34, n. 2, p. 72-88, 2020. Disponível em: https://doi.org/10.14295/biblos.v34i2.11870. Acesso em: 28 abr. 2022.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil Análise a partir do Marco Civil da Internet. **Pensar**: **Revista de Ciências Jurídicas, Fortaleza**, v. 22, n. 1, p. 108-146, 2017. Disponível em: https://doi.org/10.5020/2317-2150.2017.6272. Acesso em: 6 jun. 2022.

TRIVIÑOS, Augusto Nibaldo Silva. **Introdução à pesquisa em ciências sociais**: a pesquisa qualitativa em educação. São Paulo: Atlas, 1987.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Data protection and privacy legislation worldwide.** Geneva**,** 14 dez. 2021.

VARELA-OROL, Concha; AMENEIROS RODRÍGUEZ, Rocío. La protección de datos personales en las bibliotecas universitarias españolas en el entorno digital. **Revista General de Información y Documentación**, Madrid, v. 28, n. 2, p. 685-702, 2018. Disponível em: https://doi.org/10.5209/RGID.62844. Acesso em: 3 set. 2022.

General Data Protection Law and institutional repository: reflections and compliance

Abstract: This article discusses the General Data Protection Law in the context of institutional repositories. It focuses on the necessary adjustments to be done. This study presents a brief overview of Brazilian legislation about privacy and data protection. This research is characterized as exploratory by its ends, bibliographic and documentary by its means, and it has a qualitative approach. The results demonstrates that the General Data Protection Law presents consistent guidelines and sanctions so that institutions can guarantee an adequate treatment and security of personal data. The repositories need to be adapted regarding data protection. The study proposes recommendations about processes and workflows, such as review of institutional documents, training, and transparency actions. This study concludes that discussions about privacy and protection of personal data need to be encouraged in society, including the repositories in this application scenario.

Keywords: General Data Protection Law; privacy; institutional repository

Recebido: 20/09/2022
Aceito: 28/03/2023

Declaração de autoria:

Concepção e elaboração do estudo: Bruna Laís Campos do Nascimento, Edilene Maria da Silva.
Coleta de dados: Bruna Laís Campos do Nascimento, Edilene Maria da Silva.

Análise e interpretação de dados: Bruna Laís Campos do Nascimento, Edilene Maria da Silva.
Redação: Bruna Laís Campos do Nascimento, Edilene Maria da Silva.
Revisão crítica do manuscrito: Bruna Laís Campos do Nascimento, Edilene Maria da Silva.

Como citar

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais: reflexões e adequações. **Em Questão**, Porto Alegre, v. 29, e-127314, 2023. DOI: https://doi.org/10.1590/1808-5245.29.127314

[1] Segundo a Portaria considera-se como acervo acadêmico "o conjunto de documentos produzidos e recebidos por instituições públicas ou privadas que ofertam educação superior, pertencentes ao sistema federal de ensino, referentes à vida acadêmica dos estudantes e necessários para comprovar seus estudos [...]" (BRASIL, 2022b).