Revista de
Direito Magis

A SEGURANÇA DA INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS EM AMBIENTE ESCOLAR

INFORMATION SECURITY AND THE GENERAL DATA PROTECTION LAW IN THE SCHOOL ENVIRONMENT

Gerson Souza Silva[1]
Michel Canuto de Sena[2]

Resumo: A segurança da informação deve ser observada em todos os cenários possíveis, dentre eles destaca-se o ambiente escolar, tendo em vista, que as escolas detêm dados de crianças e de adolescentes, que são considerados como sensíveis. Desse modo, se ocorrer falhas ou violações acerca da adequação da Lei Geral de Proteção de Dados nas escolas, poderá a instituição ser multada, conforme a legislação. A Metodologia adotada foi a de revisão de literatura.
Palavras-chave: Dados; Prevenção de Danos; Segurança da Informação; Dados Sensíveis; Proteção de dados.

Abstract: Information security must be observed in all possible scenarios, among which the school environment stands out, considering that schools hold data on children and adolescents, which are considered sensitive. Therefore, if failures or violations regarding the adequacy of the General Data Protection Law occur in schools, the institution may be fined, according to the legislation. The methodology adopted was literature review.
Keywords: Data; Damage Prevention; Information Security; Sensitive Data; Data protection.

1 CONSIDERAÇÕES INICIAIS

A Lei Geral de Proteção de Dados - LGPD, que dispõe acerca do tratamento de dados pessoais, inclusive nos meios digitais, de modo extensivos para a pessoa natural e jurídica, ainda podendo ser de direito

[1] Graduado em Administração (UNIB). Especialista em Segurança da Informação e Governança da Tecnologia (UNICAMP). Coordenador de Governança de Segurança.
[2] Advogado. Pós-doutor (UEMS). Doutor (UFMS). Mestre (UFMS). Professor de Direito.

público ou privado, com objetivo de proteger os direitos da liberdade, da privacidade e do livre desenvolvimento, entre outros direitos fundamentais, ainda no artigo segundo dispões acerca da disciplina da proteção de dados pessoais e seus fundamentos, como é caso do respeito a privacidade, da inviolabilidade da intimidade, da honra e da imagem, ainda do desenvolvimento econômico e tecnológico, bem como da inovação (Sarlet; Ruaro, 2021).

Conforme o artigo sétimo, existe um rol de hipóteses sobre o tratamento de dados pessoais que pode seguir as recomendações: (I) mediante o fornecimento de consentimento pelo titular, ou seja, podendo ser por intermédio de TCLE – Termo de Consentimento Livre e Esclarecido, com objetivo de tornar público e confortável o meio de pesquisa no qual a pessoa será submetida, inclusive com a possibilidade de responder em partes ou até mesmo desistir do questionário. Ainda, existe a possibilidade da aplicação do TALE – Termo de Assentimento Livre e Esclarecido, nesse caso, o documento deve ser elaborado com linguagem acessível, pois é destinado para pessoas menores de idade ou para os incapazes, ou seja, quem por causa permanente ou transitória não puder expressar sua vontade plena (Soares, 2021).

Importante destacar que tanto a adequação de dados, quanto a necessidade dos termos citados são aplicáveis na administração pública direta e indireta, ou seja, na primeira aplica-se a União, aos Estados, aos Municípios e ao Distrito Federal, já na indireta estão alojados os demais entes, em outros termos, as fundações, as sociedades de economia mista, as autarquias, entre outras (Rapôso *et al*., 2019).

O problema da presente pesquisa consiste nos desdobramentos em razão da falta de adequação da Lei Geral de Proteção de Dados nas escolas, bem como a ausência de mecanismos de controles de segurança da informação.

A justificava do presente pré-projeto consiste na possível falta de adequação da Lei Geral de Proteção de Dados nas escolas, bem como as implicações legais pela não observância das normas. Ainda, a ausência de rotinas pode prejudicar não somente os protocolos de adequação, mas também a formação social e educacional de crianças e de adolescentes.

Revista de Direito Magis | V. 3 | N. 1 | P. 41-53 | 2025
DOI: 10.5281/zenodo.14618267

2 REVISÃO DE LITERATURA

2.1 Aplicação da LGPD nas Escolas

Inicialmente, torna-se necessário discorrer sobre as políticas públicas acerca da proteção de dados, tendo em vista que o ambiente escolar é destinado para os vulneráveis, ou seja, crianças e adolescentes. Desse modo, destacam-se duas políticas públicas no segmento, a primeira é a LGPD (Brasil, 2018) e a segunda é a LDB - Lei de Diretrizes e Bases da Educação Nacional (Brasil, 1996). Importante destacar que ambas possuem regramento próprio, porém a LDB traz o direcionamento para o ambiente escolar e a LGPD evolve as diretrizes de proteção de dados (De Teffé, 2020).

Do mesmo modo, se torna importante destacar o artigo 14 que dispõe sobre o tratamento de dados pessoais de crianças e de adolescentes, devendo observar que somente deverá ser realizado de acordo com o seu melhor interesse, ou seja, com ações e planejamentos que tragam benefícios para esse grupo vulnerável. Ainda, o tratamento de dados pessoais de crianças e de adolescentes poderá ser realizado mediante o consentimento específico dos pais ou dos responsáveis legais (De Teffé, 2020).

De acordo com o parágrafo quinto, o controlador tem o dever de realizar a comunicação para que ocorra a validação do consentimento pelos pais ou responsáveis pela criança ou adolescente, levando em consideração as tecnologias disponíveis (Brasil, 2018).

De acordo com o artigo 37, da LGPD, a escola, ora controladora, deverá eleger os responsáveis pelo tratamento de dados. Na mesma linha, deve manter o registro das operações de tratamento de dados pessoais. Do mesmo modo, cabe ao operador realizar o tratamento seguindo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções, bem como das normas sobre a matéria (Brasil, 2018).

Do mesmo modo, a lei prevê a segurança e o sigilo dos dados, conforme o artigo 46 da LGPD. Nesse sentido, os agentes de tratamento

devem adotar medidas de segurança da informação com a finalidade de garantir a proteção dos dados pessoais em casos que envolvam atos ou rotinas ilícitas ou até mesmo que possa desencadear alteração, perda ou tratamento inadequado dos dados (Sarlet; Rodrigues, 2022).

Cabe ao controlador realizar a comunicação à Autoridade Nacional de Proteção de Dados - ANPD em casos de incidentes de vazamentos que possam causar danos e consequentemente incorrer em responsabilização civil para a instituição de ensino (Brasil, 2018). Em outras palavras, caso não ocorra a adequação pertinente, a escola poderá ter que pagar multas e indenizações volumosas, em caso de danos individuais ou coletivos.

2.2 Violação de Direitos Fundamentais na Escola por Descumprimento da Lei Geral de Proteção de Dados - LGPD

Os direitos humanos consistem em tratados e convenções internacionais, com foco no desenvolvimento humano e social, a título de exemplo, toda e qualquer conduta destinada à uma pessoa não pode ser em desacordo com a dignidade da pessoa humana. Ainda, quando o assunto é tratamento, armazenamento e descarte de dados, as normativas nacionais e internacionais devem ser utilizadas, tanto na prevenção de danos, quanto na preservação dos indivíduos (Ribeiro, 2020).

Do mesmo modo, o ambiente escolar é um local de convivência de crianças e adolescentes, logo deve possuir uma rotina sobre a proteção de dados, tendo em vista que este grupo é considerado como vulnerável. Ainda, com a expansão da *internet*, os direitos fundamentais que podem ser entendidos como, direito à imagem, direito à vida, direito à integridade física e psicológica, direito à convivência harmônica e não violenta, entre outros, não podem ser reduzidos ou até mesmo violados em qualquer ambiente (Rezende *et al*., 2021).

Destarte, a escola pode ser um fato gerador de incidências das violências sociais, em decorrência de possíveis vazamentos de dados ou de informações sensíveis. Tal vazamento pode ocorrer justamente pela ausência de controles desses dados, bem como, pela falta de delegação e

de responsabilidade dos agentes de tratamento dessas ações (De Sena *et al*., 2024).

Ademais, é necessário que o gestor da instituição de ensino conheça os requisitos exigidos pela LGPD e os normativos internacionais de segurança da informação, bem como o ciclo de vida dos dados, desde a coleta até o descarte de forma segura. Ainda, de modo especial, deve conhecer e inventariar os dados considerados sensíveis, conforme a lei, com o objetivo de proteger contra o vazamento e a exposição de imagem e privacidade, inclusive constituir rotinas preventivas para o ambiente escolar (Rodrigues; Dias, 2017).

Além disso, a Lei n. 9394 de 1996, conhecida como LDB, dispõe sobre as políticas de educação nacional, bem como os protocolos a serem aplicados nas instituições educacionais, tanto particulares, quanto públicas. Inclusive, a LDB, dispõe que as normativas além de serem impositivas, ainda são de caráter universal, ou seja, são aplicáveis à todas as escolas, independentemente da região ou até mesmo da classificação, ou seja, governamental ou não (Magni; Maia; Parreiras, 2024).

Dessa feita, torna-se necessário estabelecer mecanismos de funcionamento, como é o caso do processo de governança de dados. Nesse ínterim, existe a compressão de que a gestão do ciclo de vida deve atender os requisitos pautados pelos normativos, ora ISO. Bem como, as políticas públicas direcionadas, como é o caso da LGPD e da LDB (Magni; Maia; Parreiras, 2024).

Frente ao exposto, surge a necessidade da classificação dos dados. Como é o caso de informações públicas, confidenciais, restritas e as internas. Assim, destaca-se a importância do inventário com o objetivo de conhecer os dados, bem como elaborar o protocolo para a proteção adequada.

2.3 Os Controles de Segurança da Informação

O conceito de controles pode ser entendido como medidas direcionadas em proteção, ou seja, a implementação de rotinas com foco em proteção, bem como em prevenção de danos. Inclusive, essa rotina é

necessária em ambiente escolar, tendo em vista que os dados armazenados são de crianças e de adolescentes (Sotolani *et al*., 2024).

Existem diversos controles para garantir a segurança da informação e atender as exigências da LGPD, bem como garantir que o ambiente tecnológico da escola possa assegurar a proteção de dados de criança e de adolescente e de seus colaboradores. Diante disso, se torna necessário a realização de uma avalição diagnóstica de como está o ambiente escolar sobre as tecnologias. Esse procedimento pode ser realizado por meio de *frameworks* e normativos utilizados pelas melhores práticas, a título de exemplo, o Instituto Nacional de Padrões e Tecnologia (NIST) e a Organização Internacional de Normalização (ISO) n. 27001 de 2022, com objetivo de medir o nível de maturidade sobre a segurança da informação (Dos Santos, 2023).

Desse modo, é fundamental a observância e adequação de controles para evitar vazamentos de dados sensíveis que podem ser de pessoas vulneráveis, como é o caso de crianças e de adolescentes em formação, com propósito de evitar danos que podem ser desde à imagem até mesmo por prejuízos maiores (Dos Santos, 2023).

Dessa feita, se destaca a necessidade de estabelecer, implementar, manter um Sistema de Gestão de Segurança da Informação (SGSI) que consiste em um conjunto de controles com o objetivo de mitigar riscos e garantir a proteção da informação. Ademais, estabelecer um programa de melhoria contínua, bem como elaborar estratégias de proteção dos dados, ainda planejar e priorizar as medidas de segurança (Sotolani *et al*., 2024).

Nesse sentido, as definições dos requisitos de segurança, bem como a implementação do SGSI deve levar em consideração as particularidades, as necessidades, os objetivos, os processos e a dimensão da estrutura da instituição. No caso em tela, para que ocorra a implementação de adequação nas escolas, faz-se necessário além de profissional qualificado, ainda o mapeamento das necessidades de cada instituição, tendo em vista que, cada região a ser pesquisada poderá demonstrar realidades diferentes (Sotolani *et al*., 2024).

Além das funções do Sistema de Gestão de Segurança da Informação, o especialista em segurança da informação deve atuar no planejamento dos pilares de segurança, como é o caso, da confidencialidade, ou seja, a informação deve ser acessada, disponibilizada ou divulgada às pessoas, instituições ou processos com a devida autorização (Borges *et al*., 2023).

Ainda, o especialista deve atuar para manter a integridade, em outras linhas, a informação deve ser mantida, atualizada e de forma clara, desde a sua concepção, visando protegê-la, na guarda e transmissão, contra alterações indevidas ou acidentais (Borges *et al*., 2023).

No que tange a disponibilidade, a informação deve ser acessível e utilizável, desde que o acesso seja devidamente autorizado. Ainda, deve garantir a autenticidade, pois a informação necessita de originalidade e exatidão de seu conteúdo, bem como a autoria e eventuais atualizações, além do não repúdio da informação (Borges *et al*., 2023).

A escolha de controles de segurança da informação depende da tomada de decisão da instituição. Outro fator que merece destaque é a observâncias das exigências das legislações e regulamentações, como é o caso da LGPD (Brasil, 2018).

Ainda, deve ser considerado a forma pela qual os controles se inter-relacionam para reduzir os riscos, bem como promover a proteção de forma segura. Para tanto, na implementação de rotina, importante destacar que os normativos recomendam a utilização de controles alinhados aos objetivos para identificar, proteger, detectar e recuperar (Vargas *et al*., 2023).

No que tange ao identificar, cabe a escola criar o processo de gerenciamento de riscos e de ativos, como é o caso dos inventários dos dados sensíveis, de aplicações e *softwares*, equipamentos, dispositivos, ainda rever as políticas, procedimentos para assegurar o processo de gestão de ativos e o gerenciamento do ciclo de vida de vulnerabilidades, bem como elaborar plano de remediação de vulnerabilidades identificadas. Em outras linhas, a escola deve identificar os ativos relevantes, bem como documentar o ciclo de vida da informação de modo que seja considerado a criação, o processamento, o armazenamento, a

transmissão, a exclusão e a sua destruição da informação de modo seguro (Vargas *et al*., 2023).

Outro aspecto importante, é de a escola investir em proteção de dados com a finalidade de construir um ciclo de gestão de vida de identidade de acessos, bem como a implementação de solução visando o processo de criação, de alteração e de exclusão de identidade. Outro ponto que deve ser observado, é o da atribuição de acesso obedecendo os princípios do privilégio mínimo possível, ou seja, atribuir somente para o usuário o acesso necessário para realização de suas atribuições (Dos Santos *et al*., 2023).

Nesse ínterim, existe a necessidade em criar campanhas de conscientização e treinamento de colaboradores escolares, bem como de terceiros envolvidos no ambiente escolar sobre os temas de segurança da informação e LGPD. Além disso, existe a necessidade de publicação de políticas e normativos internos (Dos Santos *et al*., 2023).

Ainda, a escola deve observar a segurança da informação e os registros de dados que devem ser protegidos desde a coleta passando pelo armazenamento, a transferência, o tratamento, bem como a eliminação segura dos dados. Nesse sentido, as atividades para proteção de dados devem envolver o gerenciamento com objetivo de garantir os pilares da segurança da informação, como é o caso da confidencialidade, da integridade e a da disponibilidade de informações (Dos Santos *et al*., 2023).

Além dos protocolos mencionados, é necessário adotar rotina de detecção, ou seja, monitoramento contínuo de segurança de informação e os ativos para identificar incidentes de segurança cibernética. Ainda, verificar a eficácia das medidas de proteção com possíveis soluções de *antimalware* e códigos maliciosos, que são conhecidos como vírus, ou seja, assegurar que as informações estão protegidas contra códigos maliciosos (De Araújo *et al*., 2024).

Para a prevenção dessas situações recomenda-se o uso de ferramentas de detecção, de prevenção e de bloqueio de ataques como é o caso do *firewall* na camada do perímetro. Em outras linhas, essa medida é crucial para bloqueio de tentativas de invasão e blindagem das

aplicações com saídas externas para *internet* por meio de solução de WAF - *firewall* de aplicativos da *web* - com objetivo de proteger os aplicativos *web* para os usuários da rede (De Azevedo, 2023).

A Escola deve ainda investir em medidas de segurança adicionais, como é caso do múltiplo fator de autenticação, que tem como objetivo evitar o acesso de usuários não autorizados, ainda implementar o uso de mecanismos de criptografia que possam contribuir com a proteção da privacidade dos dados pessoais contra invasores. Assim, investir em medidas de proteção da informação que estão em repouso, a título de exemplo, como um arquivo em um repositório, e em trânsito, como é o caso da transferência de dados entre instituições (De Azevedo, 2023).

Outro aspecto relevante para continuidade do negócio, a escola deve elaborar um plano de *backup* e estabelecer uma política interna para definir os requisitos sobre as cópias das informações. Desse modo, tal controle tem como finalidade assegurar a recuperação das informações, caso ocorra falhas de uma mídia ou um possível desastre (Bittercourt Jr; Santana. 2024).

As escolas devem se ater as políticas públicas que são formatadas e direcionadas para elas, ou seja, normas que são aplicáveis para as instituições de ensino, tanto pública, quanto privada. Nesse sentido, quando ocorre o descumprimento de qualquer uma das normas impositivas pela LDB, a escola poderá ser responsabilizada de forma civil, administrativa ou até mesmo criminal (Bittercourt Jr; Santana. 2024).

No caso em tela, a função social da escola é justamente a formação da criança e do adolescente, fase essa que é marcada por mudanças comportamentais, bem como no que tange aos momentos de aquisição de conhecimentos. Assim, quando surge alguma violação no ambiente educacional, a escola deve se posicionar ou até mesmo já possuir protocolos estipulados para o combate dessas mazelas (Bittercourt Jr; Santana. 2024).

Surge nesse cenário, as novas modalidades de violências sociais, como é o caso do *stalking*, do *bullying*, do *cyberbullying*, da pornografia de vingança, bem como da *deap fake*. Todas essas modalidades podem

interferir diretamente no desenvolvimento da criança e do adolescente, gerando assim, danos não somente para a escola, mas para as crianças ou adolescentes, além dos pais ou responsáveis (Da Silva; Santiago, 2024).

Nesse cenário, surge o questionamento acerca da adequação ou até mesmo a falta em LGPD e proteção de dados. Em outras linhas, como a escola possui o dever de contratar profissional qualificado para realizar a implementação dessas rotinas, a responsabilidade recai sobre ela. Uma solução para a regularização é justamente a adequação dos dados escolares em conformidade com a LGPD, bem como demais leis do ordenamento jurídico nacional, como é o caso da própria LDB (Da Silva; Santiago, 2024).

3 CONSIDERAÇÕES FINAIS

Para isso, além dessa contratação, a escola necessita se adequar as novas modalidades sociais de alunos (as), tendo em vista que, a geração atual é considerada como hiperconectada. Ainda, a instituição não pode ignorar as demais modalidades de violações sociais, como é o caso da população LGBTQIAPN+, pessoas com deficiência, racismo, gordofobia, entre outros.

Dessa forma, em caso de omissão da escola no que tange ao acompanhamento, se houver danos aos discentes, caberá a instituição de ensino reparar os prejuízos causados à vítima em qualquer situação, conforme mencionado. Ainda, deve ofertar assistência educacional, como é o caso de equipe qualificada e que possuam habilidades no acompanhamento de rotinas educacionais ou em casos mais graves, que possa ocasionar danos internos, gerando gastos para a escola com assistência psicológica ou psiquiátrica.

Nesses casos, com a ocorrência desses desdobramentos, a escola deverá arcar com os custos envolvendo os danos causados. Ainda, deve acompanhar os casos de alunos que foram violados em detrimento da não observância das regras impostas pela LPGD.

Nesse sentido, se torna necessário a contratação de especialistas capacitados para atuarem em projetos de implementação de controles de

Revista de Direito Magis | V. 3 | N. 1 | P. 41-53 | 2025
DOI: 10.5281/zenodo.14618267

proteção para assegurar o cumprimento das políticas públicas, com propósito de evitar prejuízos econômicos e reputacionais, tal investimento é de suma importância para evitar novos danos.

Desse modo, é necessário investir em programas de capacitações do corpo docente e técnico, bem como a realização de campanhas de conscientização acerca de segurança de informação e tratamentos de dados. Outra possibilidade consiste na distribuição de material educacional e informativo, com o objetivo de criar práticas complementares sobre a proteção e segurança dos dados.

REFERÊNCIAS

BITTENCOURT JR, Nilton Ferreira; SANTANA, Silvano Ramos. ARQUIVOS ESCOLARES E ACERVOS DIGITAIS NO NORDESTE BRASILEIRO: limites e possibilidades. **Momento-Diálogos em Educação**, v. 33, n. 1, p. 169-184, 2024.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Dispõe sobre a Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 nov. 2024.

BRASIL. **Passo a passo para elaboração de cartilhas** – Educapes. 2023. Disponível em: https://educapes.capes.gov.br/handle/capes/704485. Acesso em: 20 set. 2024.

BORGES, Rodrigo Cândido *et al*. Segurança da informação: realidades na atenção primária em uma metrópole brasileira. **Journal of Health Informatics**, v. 15, n. Especial, 2023.

DA SILVA, Sonaí Maria; SANTIAGO, Flávio. Cibersegurança no contexto escolar: o que dizem as pesquisas a respeito do cyberbullying. **Cadernos de Educação Tecnologia e Sociedade**, v. 17, n. 1, p. 183-194, 2024.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica. com**, v. 9, n. 1, p. 1-38, 2020.

DE SENA, Michel Canuto *et al*. BULLYING: VIOLAÇÃO DE DIREITOS FUNDAMENTAIS NA ESCOLA. **Revista da Seção Judiciária do Rio de Janeiro**, v. 28, n. 61, p. 28-45, 2024.

DE ARAÚJO, Igor Pinheiro Henriques *et al*. Antimalware applied to IoT malware detection based on softcore processor endowed with authorial sandbox. **Journal of Computer Virology and Hacking Techniques**, p. 1-21, 2024.

DE AZEVEDO, Marcelo Teixeira. **Segurança em cloud e ambientes web**. Editora Senac São Paulo, 2023.

DE SOUSA, Luyd Nuan Pimentel Andrade; DE SOUSA SANTOS, Monalisa Davinci; DE OLIVEIRA, Edjôfre Coelho. CYBERBULLYING: RESPONSABILIDADE CIVIL SEUS EFEITOS NA SOCIEDADE. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 5, p. 4226-4239, 2024.

DOS SANTOS, João Vitor Franco. Cibersegurança e a importância do direito digital. **Revista Multidisciplinar do Nordeste Mineiro**, v. 12, n. 1, 2023.

DOS SANTOS, Domingos Sávio *et al*. Tecnologias, Cidadania e Educação: Estratégias para Lidar com os Riscos das Práticas Digitais nas Instituições Escolares. **Revista Amor Mundi**, v. 4, n. 7, p. 11-22, 2023.

SOTOLANI, Rodrigo Silva *et al*. Vulnerabilidades de Segurança da Informação na Indústria 4.0: Proposição de Critérios para o uso de Análise Multicritério. **Exacta**, v. 22, n. 2, p. 491-522, 2024.

MAGNI, Ana Carolina Cordeiro; MAIA, Francisca Paula Soares; PARREIRAS, Vicente Aguimar. CONHECIMENTOS E LIMITAÇÕES DE DIRETORES DE ESCOLAS MUNICIPAIS E CMEIs SOBRE A REDE DE PROTEÇÃO À CRIANÇA E AO ADOLESCENTE. **Revista Orbis Latina-Racionalidades, Desenvolvimento e Fronteiras-ISSN: 2237-6976**, v. 14, n. 2, p. 154-185, 2024.

RAPÔSO, Cláudio Filipe Lima *et al*. LGPD-lei geral de proteção de dados pessoais em tecnologia da informação: Revisão sistemática. **RACE-Revista de Administração do Cesmac**, v. 4, p. 58-67, 2019.

REZENDE, Caroline Martins *et al*. INFLUÊNCIAS DA LGPD E IMPLICAÇÕES NA GESTÃO DE DOCUMENTOS: ESTUDO DE CASO EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR. **Revista H-TEC Humanidades e Tecnologia**, v. 5, n. Edição Esp, p. 100-115, 2021.
RIBEIRO, Marcio Vinicius Machado. NOSSOS DADOS NA ERA DIGITAL (LGPD). **Conhecimento Interativo**, v. 14, n. 2, 2020.

RODRIGUES, Adriana Alves; NÓBREGA, Emeide; DIAS, Guilherme Ataíde. Desafios da gestão de dados na era do big data: perspectivas profissionais. **Informação & Tecnologia**, v. 4, n. 2, p. 63-79, 2017.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)–L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, v. 26, n. 2, p. 81-106, 2021.

SARLET, Gabrielle Bezerra Sales; RODRIGUEZ, Daniel Piñeiro. A Autoridade Nacional de Proteção de Dados (ANPD): elementos para uma estruturação independente e democrática na era da governança digital. **Revista Direitos Fundamentais & Democracia**, v. 27, n. 3, p. 217-253, 2022.

SOTOLANI, Rodrigo Silva *et al*. Vulnerabilidades de Segurança da Informação na Indústria 4.0: Proposição de Critérios para o uso de Análise Multicritério. **Exacta**, v. 22, n. 2, p. 491-522, 2024.

THIOLLENT, Michel. **Metodologia da pesquisa-ação**. Cortez editora, 2022.

VARGAS, Thales Tayson do Nascimento *et al*. KOALA: implementação tecnológica de cibersegurança de um projeto webapp. **Revista Camalotes**, p. 312-327, 2023.