XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

YURI NATHAN DA COSTA LANNES

MARCELO ANTONIO THEODORO

ANA CLAUDIA SILVA SCALQUETTE

D597

Direito, governança e novas tecnologias III[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Yuri Nathan da Costa Lannes, Marcelo Antonio Theodoro, Ana Claudia Silva Scalquette – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-306-0
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito. 3. Governança e novas tecnologias. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS III

Apresentação

O XXXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, teve como sede a cidade de São Paulo, sendo acolhido com excelência pela Universidade Presbiteriana Mackenzie. O evento reafirmou a centralidade da pesquisa jurídica no enfrentamento dos desafios contemporâneos impostos pela transformação digital, pelas inovações tecnológicas e pelas novas formas de governança e controle institucional.

O GT10 – Direito, Governança e Novas Tecnologias III, realizado no dia 26 de novembro, reuniu pesquisadoras e pesquisadores de diversas regiões do Brasil para discutir os múltiplos impactos das tecnologias emergentes sobre os direitos fundamentais, a administração pública, a proteção de dados, a sustentabilidade e a ordem democrática.

Os artigos apresentados passaram por dupla avaliação cega por pares, garantindo rigor acadêmico e excelência científica. A partir da análise dos trabalhos, foram identificados seis eixos temáticos principais, que organizam os anais de forma a evidenciar os distintos focos de abordagem e permitir ao leitor um percurso estruturado pelo conteúdo:

Proteção de Dados Pessoais, Privacidade e Identidade Digital - Este eixo reúne estudos que exploram a proteção de dados pessoais sob a ótica da privacidade, da publicidade institucional, da sustentabilidade e da construção de novas categorias jurídicas, como a identidade digital.

1 - Big Data e direitos fundamentais: uma análise interdisciplinar dos impactos na privacidade e proteção de dados pessoais no ordenamento jurídico brasileiro

2 - Dados pessoais e desenvolvimento sustentável: fundamentos e desafios do direito à privacidade no século XXI

3 - A proteção de dados pessoais dos servidores públicos do Tribunal de Justiça do Distrito Federal e dos Territórios: conflito entre publicidade e privacidade?

4 - A proteção de dados pessoais como direito difuso e a sustentabilidade no uso de dados pessoais

5 - A proteção constitucional da identidade digital: um novo paradigma dos direitos da personalidade na era da informação

6 - A norma ABNT NBR ISO/IEC 27701 como instrumento de suporte à Lei Geral de Proteção de Dados

7 - A Lei Geral de Proteção de Dados Pessoais: os serviços extrajudiciais – governança e boas práticas

Inteligência Artificial, Sistema de Justiça e Direitos Fundamentais - Debate as aplicações da inteligência artificial no Judiciário e os dilemas éticos, institucionais e regulatórios que envolvem a sua adoção em contextos democráticos e de proteção aos direitos.

8 - A inteligência artificial e o Poder Judiciário: reflexões sobre a prestação jurisdicional e a concretização da cidadania

9 - Entre algoritmos e direitos: a reconstrução do direito frente ao capitalismo de vigilância

10 - Entre o algoritmo e a consciência: impactos das decisões automatizadas no Judiciário e a urgência da educação em direitos humanos

11 - A governança da inteligência artificial e os arranjos institucionais: entre inovação tecnológica e a proteção de garantias fundamentais

12 - Regular ou não a inteligência artificial, essa é a questão principal?

13 - O uso do sistema MIDAS pelo Tribunal de Justiça do Estado do Ceará: inovação tecnológica para a concretização do princípio da duração razoável do processo

14 - Entre a liberdade de expressão e os direitos da personalidade: desafios da inteligência artificial na propaganda eleitoral à luz da condição de pessoas expostas politicamente

15 - Inteligência artificial e proteção das comunidades indígenas em contextos globais

Governança Digital e Sustentabilidade – Reúne trabalhos que tratam da relação entre governança institucional e sustentabilidade, especialmente em temas como compliance ambiental, cidades inteligentes e estratégias de desenvolvimento sustentável.

16 - Governança digital sustentável e proteção de dados em cidades inteligentes: desafios jurídicos no Antropoceno

17 - Governança corporativa e compliance ambiental: estratégias para uma gestão sustentável e eficaz

18 - A inteligência artificial como instrumento de fortalecimento do compliance ambiental

19 - A democratização da energia no Brasil: uma análise sobre o acesso e as possibilidades originadas pela energia solar

Inclusão, Acessibilidade e Justiça Digital - Trabalhos que discutem as lacunas e desigualdades digitais, especialmente em relação à acessibilidade e à implementação de tecnologias digitais no poder público.

20 - Acessibilidade negligenciada: capacitismo digital nas redes sociais do governo federal

21 - Jurimetria e o Direito brasileiro – estatística e conceitos preliminares – aplicabilidade

Infância, Direitos Digitais e Exposição Prematura - Este eixo foca nos desafios da regulação da exposição digital de crianças e adolescentes e nos caminhos jurídicos para proteção da infância no ambiente virtual.

22 - Adultização infantil no meio ambiente digital: entre lacunas regulatórias e a construção de caminhos de proteção jurídica

Plataformas Digitais, Regulação e Impactos Psicossociais - Reflete sobre os impactos sociais e econômicos das plataformas digitais, abordando questões regulatórias, manipulação de resultados e proteção do consumidor.

23 - A ascensão das plataformas de apostas digitais no Brasil: uma análise dos impactos psicossociais, da manipulação de resultados e dos desafios regulatórios

Os trabalhos reunidos neste volume demonstram o vigor da produção acadêmica brasileira em torno dos desafios impostos pelas tecnologias emergentes e reafirmam o papel do Direito como campo estratégico para a mediação entre inovação e proteção de garantias fundamentais. A todos os(as) pesquisadores(as), coordenadores(as) e avaliadores(as), registramos nossos agradecimentos por suas valiosas contribuições.

Desejamos uma leitura instigante e transformadora!

Ana Claudia Silva Scalquette - Universidade Presbiteriana Mackenzie

Marcelo Antonio Theodoro- Universidade Federal de Mato Grosso

Yuri Nathan da Costa Lannes – Faculdade de Direito de Franca

A NORMA ABNT NBR ISO/IEC 27701 COMO INSTRUMENTO DE SUPORTE À LEI GERAL DE PROTEÇÃO DE DADOS

THE ABNT NBR ISO/IEC 27701 STANDARD AS AN INSTRUMENT TO SUPPORT THE BRAZILIAN GENERAL DATA PROTECTION LAW

Monica Olivo
Odisséia Aparecida Paludo Fontana

Resumo

A revolução tecnológica das últimas décadas intensificou a coleta e o tratamento de dados pessoais, o que motivou o surgimento de legislações específicas em diversos países, entre elas a Lei Geral de Proteção de Dados (LGPD) no Brasil. Contudo, a LGPD, apesar de estabelecer princípios e obrigações essenciais, apresenta limitações práticas por não detalhar de forma suficiente os mecanismos técnicos e organizacionais necessários para a proteção de dados. Nesse contexto, destacam-se as normas internacionais da família ISO/IEC 27000, em especial a ISO/IEC 27701, que estabelece diretrizes para a gestão da privacidade da informação como extensão da ISO/IEC 27001 e ISO/IEC 27002. O presente artigo busca analisar de que forma a aplicação da Norma ABNT NBR ISO/IEC 27701 pode auxiliar no cumprimento da LGPD, tomando como referência o mapeamento de compatibilidade entre seus requisitos e os dispositivos da legislação brasileira. A análise evidencia que, ao traduzir os princípios gerais da LGPD em controles objetivos e verificáveis, a ISO/IEC 27701 amplia a capacidade das organizações de garantir conformidade, segurança da informação e governança da privacidade. Conclui-se que, embora a extensão e a linguagem técnica das normas ISO representem desafios, sua adoção conjunta com a LGPD constitui um caminho sólido para a consolidação de uma cultura organizacional voltada à proteção de dados pessoais.

Palavras-chave: Proteção de dados, Lgpd, Iso/iec 27701, Segurança da informação, Governança da privacidade

Abstract/Resumen/Résumé

The technological revolution of recent decades has intensified the collection and processing of personal data, leading to the creation of specific data protection laws around the world, including the Brazilian General Data Protection Law (LGPD). However, despite establishing essential principles and obligations, the LGPD presents practical limitations by not providing sufficient detail regarding the technical and organizational mechanisms required to ensure data protection. In this context, international standards of the ISO/IEC 27000 family stand out, especially ISO/IEC 27701, which provides guidelines for privacy information management as an extension of ISO/IEC 27001 and ISO/IEC 27002. This article aims to analyze how the application of the ABNT NBR ISO/IEC 27701 Standard can support

compliance with the LGPD, based on the compatibility mapping between its requirements and the provisions of the Brazilian legislation. The analysis demonstrates that, by translating the general principles of the LGPD into objective and verifiable controls, ISO/IEC 27701 strengthens organizations' ability to ensure compliance, information security, and privacy governance. The study concludes that, although the extension and technical language of ISO standards may pose challenges, their adoption alongside the LGPD represents a solid path toward consolidating an organizational culture focused on data protection and privacy.

Keywords/Palabras-claves/Mots-clés: Data protection, Lgpd, Iso/iec 27701, Information security, Privacy governance

INTRODUÇÃO

A revolução tecnológica vivenciada nas últimas décadas trouxe preocupações antes impensadas. A coleta, armazenamento e processamento intensivo de dados gerou discussões e legislações pelo mundo. No Brasil o cenário não foi diferente, o que culminou na edição da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018.

O artigo 46 da LGPD impõe aos agentes de tratamento a adoção de medidas de segurança para proteger dados pessoais contra acessos não autorizados e incidentes que resultem em uso inadequado ou ilícito. Embora a lei atribua à Autoridade Nacional de Proteção de Dados (ANPD) a responsabilidade de definir diretrizes para a Política Nacional de Proteção de Dados, atualmente, poucas resoluções tratam de aspectos práticos, deixando lacunas na aplicação efetiva dessas exigências.

Assim cresce a relevância de padrões e certificações internacionais como referência para orientar a conformidade e fortalecer a proteção de dados. Uma das certificações internacionais mais importantes é a *International Organization for Standardization* (ISO), criada em 1946 e sediada em Genebra, que reúne organismos de normalização de cerca de 160 países para desenvolver padrões que promovem comércio, boas práticas e inovação tecnológica. No Brasil, a representação é feita pela Associação Brasileira de Normas Técnicas (ABNT) e, no campo da proteção de dados, destaca-se a Norma ABNT NBR ISO/IEC 27701.

Diante desse contexto, o presente artigo tem como problema de pesquisa: como a aplicação da Norma ABNT NBR ISO/IEC 27701 auxilia no cumprimento da LGPD na segurança dos dados? Para resolver esse problema o objetivo geral é verificar o impacto da aplicação das instruções da Norma ABNT NBR ISO/IEC 27701 ao cumprimento da LGPD na segurança dos dados. Os objetivos específicos são: estudar o contexto e a evolução das normativas de proteção de dados brasileiras; entender a definição de “ISO”, seu papel e as especificidades da Norma ABNT NBR ISO/IEC 27701; analisar, com base no mapeamento de artigos compatíveis apresentado pela própria Norma ABNT NBR ISO/IEC 27701, a compatibilidade da respectiva ISO com a LGPD.

Para tanto, será adotada uma abordagem metodológica dedutiva analítica qualitativa, baseada na análise do mapeamento de artigos abrangidos trazidos ao final da Norma ABNT NBR ISO/IEC 27701 e na pesquisa bibliográfica em legislações, livros, artigos acadêmicos e documentos institucionais, permitindo um embasamento teórico sobre a temática.

1. CONTEXTO DA PROTEÇÃO DE DADOS E A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

As crescentes inovações tecnológicas, principalmente as desenvolvidas na américa do norte no Vale do Silício, formaram a primeira revolução da tecnologia da informação. Essa revolução tecnológica teve, em grande parte, apoio e financiamento do Estado, entretanto, foi com o apoio da iniciativa privada que ela se desenvolveu e cresce até os dias atuais (Castells, 2002).

Em especial nos anos 70, o mercado começou a conduzir as inovações - por meio de mentes inovadoras impulsionadas pela paixão de produzir algo novo e pela ambição de conquistar novos nichos de produtos e de mercado - tornando o processo de desenvolvimento tecnológico mais rápido e dinâmico (Castells, 2002).

Esse impulsionamento é visto na crescente oferta por produtos e serviços tecnológicos para a população de um modo geral, formando um "Estado de bem-estar privatizado", no qual funcionalidades básicas, como mobilidade urbana, são subsidiadas por empresas privadas (Morozov, 2018).

Entretanto, a oferta desses serviços é condicionada ao fornecimento de dados pelo usuário, o que culmina em um processamento de dados excessivo por parte dessas empresas de tecnologia, situação que se tem denominado pela literatura de "dataficação". Ou seja, a "dataficação" é a prática de "conversão dos fluxos da vida em fluxos de dados", tornando possível quantificar e analisar o comportamento humano (Schiavi; Silveira, 2022). Essa prática, embora traga ganhos de eficiência e personalização, levanta questionamentos sobre privacidade e concentração de poder informacional.

A captura desses dados se dá, via de regra, por grandes empresas de tecnologia situadas, em sua maioria na América do Norte, denominadas de "Big Tech", e foi destinada ao desenvolvimento da inteligência artificial, em um ambiente carente de legislação ou controle social. Desse modo, argumenta Evgeny Morozov (2018) que essa ausência de regulação deu às Big Tech um poder excessivo, ao ponto que elas coletam os dados de forma indiscriminada e sem regulação, os transformam em produtos para após monetizar sobre isso, o que acaba por fomentar as desigualdades sociais e não o contrário.

Com esse cenário, a discussão em volta da proteção de dados vem ganhando força e regimes jurídicos pelo mundo. Danilo Doneda (2023) destaca que a proteção de dados pessoais começou a se estruturar de forma autônoma quando o processamento de dados começou a ser automatizado e com isso os riscos se tornaram mais iminentes.

Ou seja, o crescimento tecnológico é caracterizado como um fator de risco para a proteção de dados. Um dos primeiros momentos formais de discussão desse risco se deu em 1928, durante o julgamento perante a Suprema Corte Americana no caso Olmstead v. United States.

Referido julgamento discutiu o direito contra a intromissão e buscas não autorizadas na residência de uma pessoa, em especial por meio de tecnologias como as escutas telefônicas, tendo como destaque o voto do Juiz Louis Brandeis, que trouxe a necessidade de interpretar a Constituição Norte Americana não apenas com o presente, mas também diante da transformações futuras, considerando que os avanços científicos poderiam dotar o Estado de meios cada vez mais invasivos de vigilância, capazes de acessar os aspectos mais íntimos da vida privada, mesmo sem violar fisicamente a residência de um indivíduo. Brandeis alertava que o progresso científico poderia proporcionar meios para explorar crenças, pensamentos e emoções humanas sequer expressadas (Doneda, 2023).

A primeira lei específica de proteção de dados que se tem conhecimento foi desenvolvida na Alemanha, no Estado alemão Hesse, em 1970. Seguida de várias outras leis europeias, até o desenvolvimento, em 2016, do Regulamento Geral de Proteção de Dados (RGPD) da União Europeia que entrou em vigor em 25 de maio de 2018 e se tornou referência global e inspirou várias legislações pelo mundo, inclusive a legislação de proteção de dados brasileira.

No Brasil, o primeiro grande marco para a regulação específica na proteção de dados se deu com a Lei n. 12.965/2014, conhecida com a Lei do Marco Civil da Internet. Referida lei não é uma lei específica de proteção de dados pessoais, entretanto, possui como um de seus principais fundamentos a privacidade dos internautas brasileiros. O Marco Civil da Internet, com inspiração na Carta de Direitos Fundamentais da União Europeia, estabeleceu regras sobre a proteção de dados pessoais no âmbito da internet em três pontos focais, quais sejam: princípios e direitos dos usuários; guarda de registros; e acesso e tratamento de dados pessoais (Itagiba; Viola, 2018).

Ocorre que, conforme mencionado, o Marco Civil da Internet não é uma lei de proteção de dados. Desse modo, careciam de regulação vários pontos envolvendo a proteção de dados, em especial a transferência internacional de dados, vazamento de dados, dados anonimizados entre outros (Itagiba; Viola, 2018). Com isso, após várias discussões no âmbito do legislativo e do executivo brasileiro, o projeto de lei da Câmara n. 53/2018 foi sancionado pelo presidente Michel Temer, dando origem a Lei n. 13.709/2019, Lei Geral de Proteção de Dados (LGPD) - a qual foi alterada pela Lei n. 13.853 de 2019, sancionada pelo presidente Jair

Messias Bolsonaro - com vigência para agosto de 2020, exceto com relação às sanções administrativas, que entraram em vigor apenas em agosto de 2021.

A alteração provocada pela Lei n. 13.853 de julho de 2019 determinou expressamente que se trata da Lei de Proteção de Dados Pessoais e criou a Autoridade Nacional de Proteção de Dados (ANPD) – originalmente vetada na publicação da Lei n. 13.709 - fato visto pela doutrina como essencial para garantia da executabilidade da lei (Almeida; Soares, 2022). Ao analisar especificamente a Lei Geral de Proteção de Dados (LGPD) brasileira, tem-se que ela é dividida em dez capítulos, com base essencial conceitual e principiológica. A norma define quatro sujeitos centrais em sua aplicação: o titular dos dados pessoais, o controlador, o operador e o encarregado pelo tratamento.

O titular corresponde à pessoa natural a quem se referem os dados pessoais submetidos a tratamento, nos termos do artigo 5º, inciso V, da LGPD. O controlador é a pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões relativas ao tratamento de dados pessoais, conforme artigo 5º, inciso VI. O operador, por sua vez, é a pessoa natural ou jurídica, também de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, conforme artigo 5º, inciso VII. Já o encarregado é a pessoa designada pelo controlador e pelo operador para atuar como canal de comunicação entre estes, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), nos termos do artigo 5º, inciso VIII.

Em consonância com o artigo 50 da LGPD, controladores e operadores podem elaborar regras de boas práticas e de governança que definam a estrutura organizacional, o regime de funcionamento, os procedimentos para tratamento de reclamações e solicitações de titulares, as normas de segurança, os padrões técnicos, as obrigações de cada agente de tratamento, as ações educativas, bem como os mecanismos internos de supervisão e mitigação de riscos, entre outros aspectos relacionados ao tratamento de dados pessoais.

Necessário ponderar que a aplicações das normas de proteção de dados orbita, em especial, em ambientes tecnológicos, com constantes e rápidas modificações e de difícil entendimento pela maioria das pessoas, o que, por vezes, gera dificuldades em sua aplicação e gera questionamentos no cotidiano. No campo prático, o artigo 46 da LGPD exige dos agentes de tratamento que estes adotem medidas de segurança “aptas a proteger os dados pessoais e sensíveis de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito”, referido artigo está alocado no capítulo VII da LGPD, que trata da segurança e boas práticas.

Com as referidas previsões normativa surgem dúvidas de o que efetivamente seriam

essas medidas de segurança. Referido instituto normativo apresenta, ainda, como obrigação da Autoridade Nacional de Proteção de Dados a incumbência de elaborar diretrizes para a Política Nacional de Proteção de Dados, em seu artigo 55-J, em especial nos incisos "III, VII, VIII, X, XIII, XVIII". A Autoridade Nacional de Proteção de Dados possui natureza jurídica de autarquia especial, possuindo autonomia técnica e decisória (artigo 55-A da lei n.13.709). Atualmente, a autarquia elaborou 23 Resoluções, ocorre que, essas resoluções em sua maioria tratam apenas da organização interna da autarquia, existindo apenas quatro resoluções com aspectos mais práticos, sendo elas:

RESOLUÇÃO CD/ANPD nº 2, de 27 de janeiro de 2022	Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.
RESOLUÇÃO CD/ANPD Nº 15, DE 24 DE ABRIL DE 2024	Aprova o Regulamento de Comunicação de Incidente de Segurança.
RESOLUÇÃO CD/ANPD Nº 18, DE 16 DE JULHO DE 2024	Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.
RESOLUÇÃO CD/ANPD Nº 19, DE 23 DE AGOSTO DE 2024	Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.

Figura 1 - Quadro elaborado pelas autoras com base nas informações do site: https://www.gov.br/anpd/pt-br

Essas resoluções acabam por também trazer normas mais gerais e principiológicas, não especificando um padrão prático para o dia-a-dia, desse modo, é possível perceber que a lei geral de proteção de dados brasileira e as poucas resoluções atualmente existentes não resolvem problemas práticos, o que gera a necessidade de buscas por padrões e certificações. Com isso, ganham espaço no brasil e no mundo as certificações internacionais.

2. A Norma ABNT NBR ISO/IEC 27701: Estrutura e Finalidade

Segundo o site do INMETRO, o termo "ISO" se refere a Organização Internacional de Normalização (*International Organization for Standardization*), que possui sede em Genebra, na Suíça, tendo como objetivos criar normas que facilitem o comércio e promovam boas práticas de gestão e o avanço tecnológico, além de disseminar conhecimentos. Essa organização foi criada em 1946 e tem como associados organismos de normalização de cerca de 160 países (INMETRO, s/d). Entre esses associados, no Brasil, tem-se a Associação Brasileira de Normas Técnicas (ABNT), que é uma entidade privada e sem fins lucrativos responsável pela normalização técnica no Brasil e representante da ISO (ABNT, s/d).

A sigla ABNT NBR ISO/IEC 27701 reúne informações sobre a origem e a natureza da norma. “ABNT” refere-se à Associação Brasileira de Normas Técnicas. O termo “NBR” significa Norma Brasileira, indicando que a norma internacional foi traduzida ou adotada oficialmente pela ABNT. A sigla “ISO” se refere a Organização Internacional de Normalização (*International Organization for Standardization*). Já “IEC” corresponde à *International Electrotechnical Commission*, ou Comissão Eletrotécnica Internacional, organização global, sem fins lucrativos, líder na preparação e publicação de normas internacionais para todas as tecnologias elétricas, eletrônicas e correlatas que frequentemente elabora normas em conjunto com a ISO (IEC, s/d).

Por fim, o número “27701” identifica especificamente a norma, no campo da segurança da informação, que encontra direta relação com a proteção de dados e faz parte da família ISO/IEC 27000, que conta com várias normativas específicas para implantação de um sistema de segurança da informação em vários aspectos.

A Norma ISO/IEC 27701 – Sistema de Gestão da Privacidade da Informação, é uma extensão da norma ISO/IEC 27001 e ISO/IEC 27002 - Código de prática para controles de segurança da informação, e tem como objetivo adicionar novos controles ao sistema de gestão da informação para auxiliar gestão de riscos de privacidade relacionados com dado pessoal. Desse modo, para se aplicar a ISO/IEC 27701 será necessário também aplicar a ISO/IEC 27001 e a ISO/IEC 27002, trabalhando a segurança da informação e após de forma específica a proteção de dados.

A ISO/IEC 27001 trabalha o Sistema de Gestão da Segurança da Informação (SGSI), sendo que seu objetivo é estabelecer requisitos que permitam identificar, avaliar e tratar riscos relacionados à segurança da informação, por meio de um conjunto de controles e processos sistematizados. A Norma foca em sua essência na gestão de risco, busca identificar quais potenciais problemas podem ocorrer com a informação e, desse modo, visa implementar medidas de controle. Sendo composta por vários processos de segurança interligados que quanto melhor definidos estes processos são, menos riscos à informação existirão (Cardorim, 2022).

A ISO/IEC 27002 complementa a 27001 ao oferecer diretrizes detalhadas de boas práticas para implementação dos controles de segurança, fornecendo orientações práticas para a aplicação de medidas técnicas, administrativas e organizacionais voltadas à proteção das informações. Entre os temas abordados estão: controles de acesso, segurança física e ambiental, gestão de ativos, criptografia, segurança em redes e gestão de incidentes.

A ISO/IEC 27701, por sua vez, possui enfoque específico na gestão da privacidade da informação. Seu propósito é orientar organizações que atuam como controladoras ou operadoras de dados pessoais na implementação de um Sistema de Gestão de Informações de Privacidade (PIMS), alinhando práticas internas a legislações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia. A norma introduz requisitos e controles relacionados à coleta, uso, retenção, compartilhamento e descarte de dados pessoais, bem como à transparência, gestão do consentimento, atendimento aos direitos dos titulares e comunicação de incidentes de privacidade.

Sendo organizada da seguinte forma:

Seção 5	apresenta os requisitos específicos de um SGPI e outras informações relacionadas aos requisitos de segurança da informação da ABNT NBR ISO/IEC 27001, **apropriados para uma organização que atue como um controlador de dados pessoais ou como um operador de dados pessoais**.
Seção 6	apresenta as diretrizes específicas de um SGPI e outras informações relacionadas aos controles de segurança da informação contidos na ABNT NBR ISO/IEC 27002 e diretrizes específicas de um SGPI para uma **organização que esteja atuando como um controlador de dados pessoais ou como um operador de dados pessoais.**
Seção 7	apresenta as diretrizes adicionais da ABNT NBR ISO/IEC 27002 para os **controladores** de dados pessoais
Seção 8	fornece as diretrizes adicionais contidas na ABNT NBR ISO/IEC 27002 para os **operadores** de dados pessoais.
Anexos	Anexo A apresenta os controles e objetivos de controles específicos de um SGPI para uma organização que atue como um controlador de dados pessoais; Anexo B apresenta os controles e objetivos de controles específicos para uma organização que atue como um operador de dados pessoais; Anexo C apresenta um mapeamento com a ISO/IEC 29100; Anexo D apresenta um mapeamento dos controles deste documento com o Regulamento da União Europeia sobre a Proteção de Dados; Anexo E apresenta um mapeamento com a ABNT NBR ISO/IEC 27018 e com a ISO/IEC 29151; Anexo F explica como as ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 são estendidas à proteção da privacidade, quando do tratamento de dados pessoais.

Figura 2 - Quadro elaborado pelas autoras com base na Norma ABNT NBR ISO/IEC 27701

Essas três normas - ISO/IEC 27001, ISO/IEC 27002 e a ISO/IEC 27701 - quando aplicadas de forma integrada, proporcionam uma estrutura robusta de governança da informação, em que a ISO/IEC 27001 estabelece a estrutura de gestão, a ISO/IEC 27002 oferece

as melhores práticas para implementação dos controles, e a ISO/IEC 27701 expande essas diretrizes para o contexto específico da privacidade e proteção de dados pessoais. Tal integração viabiliza não apenas a mitigação de riscos operacionais e de segurança, mas também a conformidade regulatória e o fortalecimento da confiança entre organizações e titulares de dados (Cardorim, 2022).

Com essa visão, tem-se que a aplicação da norma ISO/IEC 27701 representa um avanço significativo na consolidação de práticas de privacidade e proteção de dados, ao estruturar processos para controladores e operadores. Trata-se de um instrumento que, além de complementar a segurança da informação já prevista pela ISO/IEC 27001 e ISO/IEC 27002, acrescenta um olhar específico para a privacidade. Diante disso, torna-se relevante examinar em que medida essa norma dialoga com a realidade brasileira, especialmente ao se considerar seu mapeamento de compatibilidade com a Lei Geral de Proteção de Dados, ponto que será desenvolvido no próximo tópico.

3. ANÁLISE DE ABRANGÊNCIA DA ABNT NBR ISO/IEC 27701 À LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA

No tópico supra, verificou-se que a ISO/IEC 27701 é um complexo da família ISO/IEC 27000, em especial pelo fato de a própria norma internamente já trazer a necessidade de implantação de mais duas normas da família ISO/IEC 27000, quais sejam: a ISO/IEC 27001 e a ISO/IEC 27002. Isso demonstra uma certa complexidade tanto na análise quanto na aplicação das normativas, diante de sua extensão e multidisciplinariedade, trazendo contextos de gestão, administração, direito, tecnologia, entre outras áreas.

Ao final da versão brasileira da ISO/IEC 27701 existe um mapeamento entre as provisões da respectiva ISO com e a Lei Geral de Proteção de Dados brasileira. Diante do obstáculo imposto pela própria limitação de páginas de um artigo, a presente análise se limitará ao mapeamento apresentado na própria ISO, com o foco de verificar como artigos da LGPD citados são efetivamente respeitados.

Os itens de efetivo conteúdo da ISO/IEC 27701 são os itens “5”. “6”, “7” e “8”. O item “5”, como já ponderado no tópico acima trata dos requisitos específicos para implantação de um Sistema de Gestão da Segurança da Informação - SGPI estabelecido pela ABNT NBR ISO/IEC 27001. No quadro de mapeamento de compatibilidade da ISO/IEC 27701 com a LGPD, consta que referido item asseguraria o cumprimento dos artigos: 5º, VI, VII e IX, 38 e 50 da LGPD.

O artigo 5º, VI, VII e IX, estabelece os conceitos de “controlador”, “operador” e “agentes de tratamento”. Referidos conceitos são trabalhados e exigido seu conhecimento em toda a normativa, sendo que ela é justamente direcionada para este público, ou seja, as pessoas que irão tratar os dados pessoais.

O artigo 38 estabelece que a autoridade nacional poderá determinar ao controlador que este elabore relatório de impacto à proteção de dados. O item “5”, em especial os subitens “5.4.1.2” e “5.4.1.3” trazem, dentro da estrutura da implantação do Sistema de Gestão da Segurança da Informação – SGPI a necessidade da avaliação de riscos, propondo uma organização para implantação de um processo constante de avaliação dos riscos causados pela atividade. Desse modo, nesse ponto a ISO/IEC 27701 exige mais que a LGPD, ao impor como dever a análise de risco, enquanto que a lei estabelece uma faculdade da autoridade nacional em exigir referido relatório.

Por fim, quanto ao item “5”, o mapeamento estabelece que este item também cumpre o estabelecido no artigo 50, que prevê a possibilidade de os controladores e operadores formularem regras de boas práticas e de governança. Importante destacar que o item “5” é direcionado especificamente na aplicação da ABNT NBR ISO/IEC 27001, que estabelece o Sistema de Gestão da Segurança da Informação – SGPI.

Daniel Cardorim (2022) explica que o Sistema de Gestão de Segurança da Informação (SGSI) consiste em uma abordagem estruturada destinada a estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar as práticas de segurança da informação de uma organização, com o propósito de assegurar o alcance de seus objetivos de negócio.

Referido sistema é basicamente um manual de boas práticas e governança, trabalhando sete itens para sua implantação, sendo eles: a) contexto e organização; b) liderança; c) planejamento; d) apoio; e) operação; f) avaliação de desempenho; g) melhoria. As etapas de gestão descritas na ISO/IEC 27001 e estendidas pela ISO/IEC 27701 configuram um ciclo que busca a proteção contínua das informações e a conformidade com legislações como a LGPD. Essas etapas estruturam o Sistema de Gestão da Segurança da Informação (SGSI) e, em sua ampliação, o Sistema de Gestão da Privacidade da Informação (SGPI).

A primeira etapa, contexto e organização, prevista na ISO/IEC 27001, estabelece que a organização deve compreender seu ambiente interno e externo, identificando partes interessadas, requisitos legais, regulatórios e contratuais aplicáveis. Esse diagnóstico inicial permite alinhar o sistema de gestão às necessidades específicas de privacidade e segurança da informação. Na sequência, a etapa de liderança enfatiza o papel da alta administração, que deve assumir compromisso com a política de segurança e privacidade, fornecendo direção estratégica

e integrando esses valores à cultura organizacional, bem como, designar responsabilidades e assegurar recursos adequados para a implementação eficaz do sistema.

O planejamento é a fase dedicada à análise de riscos e oportunidades. De acordo com a ISO/IEC 27001 e com a extensão da ISO/IEC 27701, a organização deve identificar ameaças, vulnerabilidades e impactos relacionados ao tratamento de dados pessoais. Com base nisso, são definidos objetivos, controles de segurança e medidas de privacidade alinhadas a obrigações legais como as previstas na LGPD. A etapa de apoio envolve a alocação de recursos, competências e conscientização. As normas ISO exigem que as organizações promovam treinamentos contínuos e estabeleçam canais de comunicação eficazes sobre segurança e privacidade, garantindo que todos os colaboradores compreendam suas responsabilidades. Além disso, a gestão documental e o controle da informação registrada constituem instrumentos essenciais para a rastreabilidade e auditoria.

Na fase de operação, a norma prevê a implementação efetiva dos planos de tratamento de riscos e controles definidos anteriormente. Isso inclui procedimentos técnicos, administrativos e contratuais, como o gerenciamento de incidentes de segurança, a proteção de dados sensíveis, o controle de acessos e a garantia de conformidade na transferência internacional de dados. A avaliação de desempenho, por sua vez, exige monitoramento contínuo do sistema. A organização deve realizar auditorias internas, revisões pela direção e medições de indicadores de eficácia, assegurando que o sistema não apenas exista formalmente, mas funcione na prática.

Por fim, a etapa de melhoria, conforme a ISO/IEC 27001 e a ISO/IEC 27701, estabelece a necessidade de corrigir não conformidades e implementar ações preventivas e corretivas. Esse processo cíclico assegura a evolução constante do sistema, adaptando-o a novos riscos, tecnologias emergentes e mudanças no marco regulatório. Assim, as sete etapas — contexto e organização, liderança, planejamento, apoio, operação, avaliação de desempenho e melhoria — formam a espinha dorsal de um modelo de governança que, ao ser estendido para a privacidade pela ISO/IEC 27701, traduz princípios legais em práticas verificáveis.

Essa sistematização garante que o tratamento de dados pessoais não apenas atenda aos requisitos mínimos da LGPD, mas seja continuamente aprimorado com a análise fática o que é aplicado. Desse modo, novamente as normas da ISO vão além das previstas na LGPD, considerando que o que a lei prevê como “possibilidade” a norma ISO impõem como dever de implantação.

O item “6” da ISO/IEC 27701 amplia as diretrizes de segurança da informação estabelecidas na ISO/IEC 27002, detalhando controles técnicos e organizacionais que

asseguram tanto a proteção dos dados quanto à conformidade com a privacidade. Esses controles são relacionados a áreas como política de segurança da informação, gestão de ativos, controle de acesso, criptografia, segurança física, segurança nas operações, segurança nas comunicações, gestão de incidentes, continuidade do negócio e compliance.

No mapeamento com a LGPD, observa-se a correspondência com os artigos 5º, I e X; 6º, VII e §1º;12, §3º; 32; 38; 41; 46; 47; 48; 49; 50 e 51. O artigo 5º, I e X, estabelece a definição de dado pessoal e tratamento de dados pessoais, conceitos que permeiam a totalidade da ISO 27002. O artigo 6º, VII e §1º, por sua vez, relaciona-se com o princípio da segurança, impondo o dever de adotas medidas técnicas e administrativas aptas a proteger os dados. Essa exigência é contemplada de forma mais detalhada pela norma, que especifica controles para mitigar riscos e prevenir incidentes.

Já o artigo 12, §3º, que trata de informações pessoais de crianças e adolescentes, se conecta à medias da norma voltadas à classificação e proteção de dados sensíveis e de alto risco. O artigo 32, que impõe a adoção de medidas de segurança, técnicas e administrativas para proteger dados pessoais, é amplamente coberto pela ISO/IEC 27002, que traz não apenas diretrizes gerais, mas também orientações práticas e mensuráveis.

O artigo 38 (relatórios de impacto) e o artigo 41 (nomeação do encarregado) também encontram respaldo nos controles previstos no item 6, pois a norma exige processos claros de responsabilidade e governança, garantindo a designação de funções e a documentação das ações de segurança e privacidade. Os artigos 46 a 51, que tratam da segurança, boas práticas e governança, são igualmente observados, já que a norma institui não apenas a adoção de medidas, mas também o monitoramento, auditoria e melhoria contínua. Portanto, verifica-se que o item 6 da ISO/IEC 27701 não apenas cumpre, mas aprofunda a aplicação dos dispositivos da LGPD, transformando obrigações genéricas da lei em controles objetivos.

O item 7 da ISO/IEC 27701 estabelece diretrizes adicionais para controladores de dados pessoais, ampliando o escopo dos controles de segurança para contemplar requisitos específicos de privacidade. A vinculação com os artigos da LGPD é ampla, abrangendo desde conceitos e princípios até obrigações específicas de tratamento. No mapeamento com a LGPD, observa-se a correspondência com os artigos 5º, XII, XVII; 4º, §3º; 6º, III, V; 7, II, §5º; 8º, §4º, §5º; 9º, I, §2º; 10, III; 11; 14, §6; 16; 18, II, §6º; 26, IV; 32; 34, I; 37; 38; 39.

O artigo 5º, XII e XVII, define respectivamente “consentimento” e “bloqueio” de dados, ambos tratados na norma no contexto de gestão do ciclo de vida da informação, incluindo procedimentos para obtenção de consentimento, manutenção de registros e suspensão do tratamento. O art. 4º, §3º, que assegura o cumprimento da LGPD inclusive por quem esteja

localizado fora do Brasil quando houver tratamento de dados no território nacional, é reforçado pela norma, que prevê controles de governança voltados à conformidade internacional.

O artigo 6º, III e V, relativos aos princípios da finalidade e livre acesso, são traduzidos em controles operacionais que garantem o tratamento para propósitos legítimos e a disponibilização de mecanismos para que o titular possa acessar seus dados. Enquanto que o artigo 7º (e seus incisos e parágrafos) que trata sobre hipóteses de tratamento de dados, é incorporado pela norma por meio da exigência de políticas documentadas e mecanismos para verificar a base legal de cada tratamento.

O artigo 8º, §§4º e 5º, e o artigo 9º (com seus incisos e parágrafos), que tratam de dados sensíveis e transferência internacional, são cobertos com controles de segurança reforçados e critérios rigorosos para compartilhamento de dados com terceiros. O artigo 10, III, e o artigo 11, que abordam legítimo interesse e hipóteses específicas de tratamento, encontram correspondência em processos de avaliação de impacto e registros de justificativa para uso dessa base legal.

Além disso, artigos como o 14, §6º (tratamento para tutela da saúde), 16 (eliminação de dados), 18 (direitos do titular), 26, IV (cooperação com o poder público), 32 (medidas de segurança), 34, I (transferência internacional), 37 (registro das operações), 38 (relatórios de impacto) e 39 (comunicação com o encarregado) têm previsão expressa nos controles do item 7, garantindo que o controlador disponha de mecanismos formais para cumprimento da lei.

Dessa forma, o item 7 demonstra alinhamento com a LGPD, transformando previsões legais genéricas em procedimentos verificáveis e auditáveis, reduzindo riscos e fortalecendo a governança do controlador.

Por fim, o item 8 da ISO/IEC 27701 aborda as diretrizes específicas para operadores de dados pessoais, ou seja, entidades que realizam o tratamento em nome do controlador. A correspondência com a LGPD envolve um conjunto amplo de artigos, com foco em obrigações operacionais e salvaguardas contratuais, sendo eles: 4º, III, IV; 6º, I a X; 9º, I a VII; 10, I e II;15, I a IV;16, I a IV;18; 23; 33, I a IX; 34, I a VI; 37; 39; 41; 42; 44; 45; 46; 49.

O artigo 4º, III e IV, que define "controlador" e "operador", serve de base para a norma, que detalha responsabilidades específicas, limites de atuação e obrigações de registro. O artigo 6º, I a X, que traz os princípios do tratamento, é incorporado por meio de controles para garantir que todas as atividades estejam alinhadas a princípios como finalidade, adequação, necessidade, qualidade dos dados, segurança e prevenção.

O artigo 7º, I a X, que trata das hipóteses legais de tratamento, é operacionalizado pela exigência de comprovação documental da base legal indicada pelo controlador. O artigo 9º

(dados sensíveis) e o artigo 10 (legítimo interesse) também são tratados de forma a garantir que o operador implemente medidas adicionais para dados de maior risco e só atue dentro dos limites definidos contratualmente.

Os artigos 15 e 16, que estabelecem obrigações quanto à eliminação de dados e ao término do tratamento, são contemplados com a previsão pela norma de processos para devolução, anonimização ou destruição segura dos dados ao final do contrato. O artigo 18 (direitos do titular) e o artigo 23 (tratamento pelo poder público) são endereçados pela norma ao exigir mecanismos para atender solicitações de acesso, correção ou eliminação.

O artigo 33 (transferência internacional) e o artigo 34 (requisitos para compartilhamento) têm respaldo em controles que exigem cláusulas contratuais específicas e avaliação prévia de riscos. Já os artigos 37 (registro das operações), 39 (comunicação com o encarregado), 41 (designação do encarregado), 42 a 45 (responsabilidade e ressarcimento de danos), 46 (medidas de segurança) e 49 (governança) são incorporados por meio de processos documentados, auditorias e monitoramento contínuo. Assim, o item 8 da ISO/IEC 27701 assegura que o operador disponha de um arcabouço robusto para atuar em conformidade com a LGPD, reforçando a corresponsabilidade entre controlador e operador e garantindo rastreabilidade e segurança nas operações de tratamento.

A análise integrada dos itens 5, 6, 7 e 8 da ABNT NBR ISO/IEC 27701 demonstra que a norma oferece um arcabouço detalhado e estruturado que não apenas se alinha às disposições da Lei Geral de Proteção de Dados, mas também as amplia em termos de exigência e aplicabilidade prática. Enquanto a LGPD estabelece princípios e obrigações de forma geral, a ISO 27701 traduz essas diretrizes em controles mensuráveis, abrangendo desde a gestão de riscos e implementação de políticas até a definição de responsabilidades e mecanismos de monitoramento contínuo.

No caso dos controladores, a norma reforça aspectos de governança, responsabilidade e transparência; para os operadores, estabelece salvaguardas contratuais, rastreabilidade e medidas técnicas específicas. Assim, observa-se que a aplicação conjunta da LGPD e da ISO/IEC 27701 potencializa a proteção de dados pessoais no Brasil, fortalecendo a conformidade normativa, a segurança da informação e a confiança nas relações entre titulares, controladores e operadores.

Contudo, é necessário ponderar que a extensão e a multidisciplinariedade dos conceitos e regras trazidas pelas normas ISO da família 27000 representam também um desafio. O detalhamento traz robustez técnica e operacional, mas torna sua compreensão difícil por vários momentos. Assim, a efetividade da ISO/IEC 27701 depende da capacidade das

organizações em transformar esse conteúdo técnico em práticas realmente aplicáveis ao seu contexto.

CONCLUSÃO

A presente pesquisa partiu da indagação central sobre como a aplicação da Norma ABNT NBR ISO/IEC 27701 pode auxiliar no cumprimento da Lei Geral de Proteção de Dados (LGPD) no que se refere à segurança dos dados pessoais. Ao longo do estudo, verificou-se que, embora a LGPD constitua um marco regulatório fundamental para a proteção da privacidade no Brasil, sua efetividade prática ainda é limitada pela ausência de diretrizes operacionais detalhadas, especialmente no tocante à implementação de medidas técnicas e organizacionais capazes de assegurar, de forma contínua, a conformidade e a mitigação de riscos.

Nesse contexto, a ISO/IEC 27701 se revelou um importante instrumento de governança da privacidade, ao traduzir os princípios e obrigações legais em controles mensuráveis e alinhados a padrões internacionais. A análise dos itens 5, 6, 7 e 8 da norma evidenciou que ela não apenas cumpre as exigências da LGPD, mas também amplia seu alcance, impondo práticas rigorosas de gestão de riscos, segurança da informação, definição de responsabilidades e monitoramento constante.

Ao exigir processos estruturados para controladores e operadores, a ISO/IEC 27701 fortalece a rastreabilidade das operações de tratamento, a clareza nas funções e a adoção de medidas proativas de prevenção de incidentes. A integração com a ISO/IEC 27001 e a ISO/IEC 27002 complementa esse cenário, oferecendo um arcabouço normativo e técnico capaz de atender, de forma sistêmica, às demandas de proteção de dados em um ambiente de constantes transformações tecnológicas.

Os resultados obtidos indicam que a adoção conjunta da LGPD e da ISO/IEC 27701 resulta em uma estratégia institucional de fortalecimento da segurança da informação e de promoção da confiança nas relações entre empresas, órgãos públicos, titulares de dados e sociedade. Em um contexto no qual a coleta e o processamento massivo de informações pessoais se intensificam, essa integração se mostra fundamental para garantir que o avanço tecnológico ocorra de forma ética, segura e em conformidade com os direitos fundamentais.

A ISO/IEC 27701 se apresenta como um manual denso e técnico, demandando conhecimento de várias áreas para sua implantação. Esse caráter multidisciplinar, embora represente uma força por integrar aspectos de administração, tecnologia e governança, acaba por dificultar a compreensão por profissionais que não têm familiaridade com termos técnicos

ou metodologias de todas as áreas do conhecimento abarcadas. Tal realidade pode gerar uma barreira prática à adoção dessas normas, especialmente em pequenas e médias organizações que carecem de estrutura para implementar requisitos tão detalhados ou não conseguem contratar profissionais qualificados.

Assim, conclui-se que a aplicação da ABNT NBR ISO/IEC 27701, em conjunto com a LGPD, representa não apenas uma solução para as lacunas regulatórias ainda existentes, mas também um caminho sólido para a consolidação de uma cultura organizacional voltada à proteção de dados e à preservação da privacidade no Brasil. Contudo, a própria extensão e complexidade das normas ISO da família 27000 representam um desafio. Se, por um lado, esse nível de detalhamento garante maior robustez técnica e operacional, por outro, dificulta sua compreensão ampla.

Nesse sentido, a efetividade das normas ISO, em especial da ISO/IEC 27701, dependerá da capacidade das organizações de traduzirem esse conteúdo técnico em práticas aplicáveis ao seu contexto. Assim, a principal contribuição dessas normas talvez não esteja apenas em sua adoção integral, mas na possibilidade de servirem como referência estruturante, auxiliando a transformar os princípios legais da LGPD em procedimentos operacionais efetivos.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Sobre a ABNT: descubra nossa história, missão e valores**. Disponível em: <https://abnt.org.br/institucional/sobre-abnt-2/>. Acesso em: 13 ago. 2025.

ALMEIDA, Siderly C. D; SOARES, Tania A. **Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital.** Perspectivas em Ciência da Informação, v.27, n.3, p. 26-45. 2022.https://doi.org/10.1590/1981-5344/25905.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.** Rio de Janeiro: ABNT, 2022. 39 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2022 – Tecnologia da informação — Técnicas de segurança — Controles de segurança da informação.** Adoção idêntica à ISO/IEC 27002:2022. Rio de Janeiro: ABNT, 2022. 69 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019 – Versão Corrigida 2020 – Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.** Rio de Janeiro: ABNT, 2019. 82 p.

BRASIL. **LEI 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 13 ago. 2025

BRASIL. **LEI Nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 13 ago. 2025. Acesso em: 13 ago. 2025.

BRASIL. **LEI Nº 13.853, de 08 de julho de 2019.** Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm>. Acesso em: 13 ago. 2025;

BRAIL. **RESOLUÇÃO CD/ANPD Nº 2, de 27 de janeiro de 2022.** Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018 (LGPD), para agentes de tratamento de pequeno porte. DOU, 28 jan. 2022, Seção 1. Anexo I. Disponível em: < https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022>. Acesso em: 13 ago. 2025

BRASIL. **RESOLUÇÃO CD/ANPD Nº 15, de 24 de abril de 2024.** Aprova o Regulamento de Comunicação de Incidente de Segurança. DOU, 25 abr. 2024. Disponível em: < https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>. Acesso em: 13 ago. 2025.

BRASIL. **RESOLUÇÃO CD/ANPD Nº 18, de 16 de julho de 2024.** Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais. DOU, 17 jul. 2024. Disponível em: < https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074>. Acesso em: 13 ago. 2025.

BRASIL. **RESOLUÇÃO CD/ANPD Nº 19, de 23 de agosto de 2024.** Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais. DOU, 23 ago. 2024, Seção 1, p. 123-127. Disponível em: < https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396>. Acesso em: 13 ago. 2025

CARDORIM, Daniel. **COMO IMPLEMENTAR A ISO 27001 NA PRÁTICA**. Canal TIexames. YouTube, 15 mar. 2022. Disponível em: <https://www.youtube.com/watch?v=uaEJyiDZ3jY>. Acesso em: 9 ago. 2025.

CASTELLS, Manuel. A **sociedade em rede – A era da Informação: Economia, Sociedade e Cultura.** Traduzido por Roneide Venâncio Majer. 6.ed. São Paulo: Paz e Terra, v.1, 1999.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luiz (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2023.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA (INMETRO). **O que é ISO**. Disponível em: <http://www.inmetro.gov.br/qualidade/responsabilidade_social/o-que-iso.asp>. Acesso em: 13 ago. 2025.

INTERNATIONAL ELECTROTECHNICAL COMMISSION (IEC). **Quem somos — Who we are.** IEC, 2025. Disponível em: <https://www.iec.ch/who-we-are>. Acesso em: 18 ago. 2025.

ITAGIBA, Gabriel; VIOLA, Mario. **Privacidade e Dados Pessoais**. In: BOTTINO, Celina; LEMOS, Ronaldo; SOUZA, Carlos Affonso (coord.). Marco Civil da Internet: Jurisprudência Comentada. São Paulo: Revista dos Tribunais, 2018.

MOROZOV, Evgeny. **Big Tech: a ascensão dos dados e a morte da política**. Traduzido por Claudio Marcondes. São Paulo: Ubi Editora, 2018.

SCHIAVI, Iara; Silveira, Sérgio Amadeu. **A cidade neoliberal e a soberania de dados: mapeamento do cenário dos dispositivos de dataficação em São Paulo**. urbe. Revista Brasileira de Gestão Urbana, v.14, e20210145. 2022. https://doi.org/10.1590/2175-3369.014.e20210145.