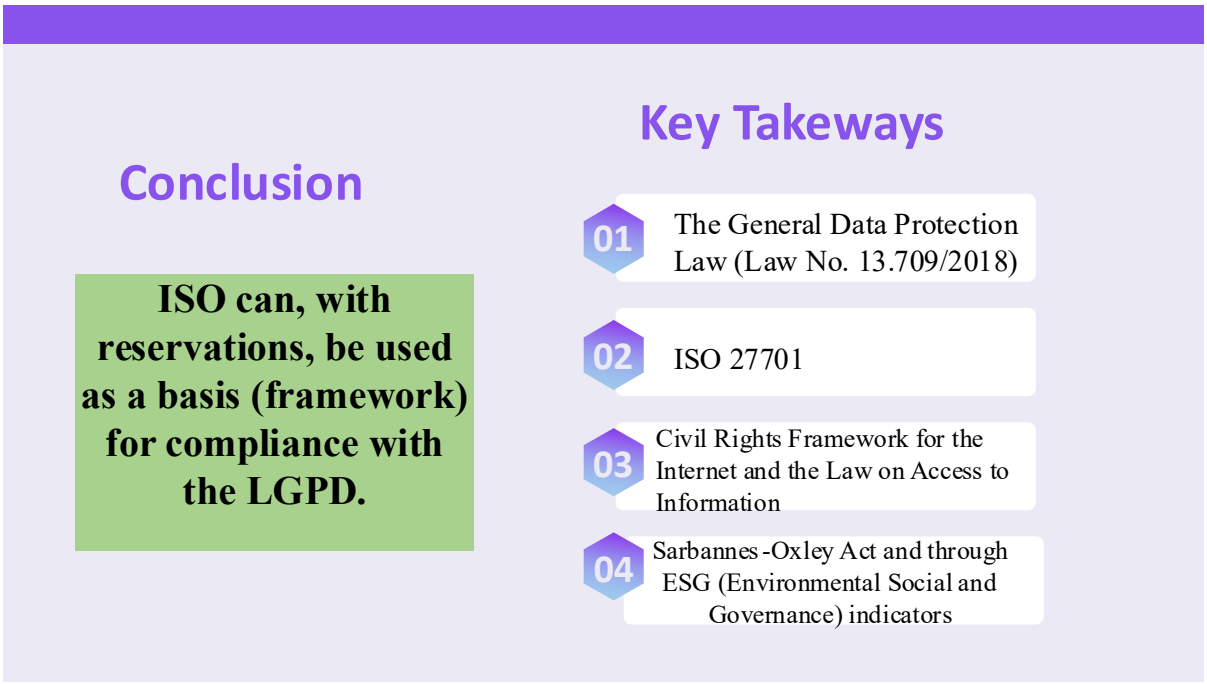
ISSN 2359-4799
Volume 10 / Número 1 / Ano 2024 – p. 01-15
DOI: 10.36524/ric.v10i1.2445

REVISTA ifes ciência

GRAPHICAL ABSTRACT



Lei Geral de Proteção de Dados: uma análise da ISO 27701 como ferramenta de controle para LGPD

General Data Protection Law: an analysis of ISO 27701 as a control tool for GDPR

Evelyn Nicole Ruhmann Chou [1]*, Cícero José Albano, [2] e Paulo Henrique de Almeida, *[3]

[1, 2] Instituto Federal do Paraná Campus Curitiba, R. João Negrão, 1285, Rebouças, 80230-150 Curitiba – PR, Brasil.

[3] Instituto Federal do Paraná Reitoria - Rua Emilio Bertolini, nº 54, Cajuru, 82920-030– Curitiba, PR, Brasil.

*Paulo.almeida@ifpr.edu.br

Artigo submetido em 06/11/2024, aceito em 04/03/2024 e publicado em 25/03/2024.

ORCID – Evelyn Nicole Ruhmann Chou: https://orcid.org/0000-0003-2978-4980
ORCID – Cícero José Albano: https://orcid.org/0000-0001-8608-6164
ORCID – Paulo Henrique de Almeida: https://orcid.org/0000-0001-7125-1593

Resumo: A Lei Geral de Proteção de Dados (Lei n.º 13.709/2018) busca garantir o direito à privacidade dos indivíduos e gera obrigações às organizações no tratamento dos dados pessoais coletados. Contudo, os parâmetros e os controles que devem ser adotados pelas empresas não foram regulamentados pela Autoridade Nacional de Proteção de Dados (ANPD). Desta maneira, o presente estudo propõe a análise dos padrões contidos na norma ISO 27701 como modelo e gestão (framework) de adequação aos requisitos para tratamento de dados conforme estipulados na LGPD. Metodologicamente o trabalho configurou-se como uma revisão bibliográfica sistemática, de caráter exploratória. Para isto, o artigo analisou a era da internet e as legislações vigentes, como o Marco Civil da Internet e a Lei de Acesso à Informação. Através da análise comparativa entre os requisitos da LGPD e as recomendações da ISO 27701 identificou-se que a ISO pode, com ressalvas, ser utilizada como base (framework) para compliance à LGPD, observada a necessidade de complementação de eventuais requisitos à luz dos princípios contidos na lei.

Palavras-chave: Lei Geral de Proteção de Dados; Privacidade; ISO 27701; Compliance, Governança.

Abstract: The General Data Protection Law (Law No. 13.709/2018) seeks to guarantee the right to privacy of individuals and generates obligations to organizations in the treatment of personal data collected. However, the parameters and controls that must be adopted by companies were not regulated by the National Data Protection Authority (ANPD). In thi way, the present proposes the analysis of the standards contained in the ISO 27701 standard as a model and management (framework) of adequacy to the requirements for data processing as stipulated in the LGPD. Methodologically, the work was configured as a systematic bibliographic review of an exploratory nature. For this, the article analyzed the internet age and current legislation, such as the Civil Rights Framework for the Internet and the Law on Access to Information. Through the comparative analysis between the requirements of the LGPD and the recommendations of ISO 27701, it was identified that the ISO can, with reservations, be used as a basis (framework) for compliance with the LGPD, observing the need to complement any requirements in the light of the principles contained in the law.

Keywords: Brazilian General Data Protection Law; Privacy; ISO 27701; Compliance; Governance.

1 INTRODUÇÃO

Com a promulgação da Lei 13.709/2018, também denominada de Lei Geral de Proteção de Dados – LGPD, que cria a Autoridade Nacional de Proteção de Dados – ANPD, entidade esta que terá a competência, principalmente de zelar pela proteção de dados pessoais, e pela observância dos segredos comerciais e industriais, surgiu uma nova categoria de risco corporativo. Desta forma todas as instituições (tanto da iniciativa privada, como da administração pública federal, estadual e municipal, direta, autárquica e fundacional) devem buscar se adaptar e atender o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural durante o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado (BRASIL, 2018). Instituições de ensino, pesquisa e extensão vem buscando estudar e propor ações e estratégias para assegurar esse atendimento. Assim, mesmo atuando em instituição de educação profissional tecnológica, que abriga em seu ecossistema professores, alunos, servidores, pais e outros profissionais, nos cabe pesquisar a respeito da proteção da privacidade e os cuidados necessários para evitar excessos de exposição, além do tratamento e armazenamento de informações, trazendo possíveis soluções e estratégias para o atendimento da LGPD.

Compete à ANPD, conforme art. 49 da lei, publicar guias e orientações normativas para a correta aplicação da LGPD, que ainda não foram divulgados pela autoridade. Então, surge para as empresas a necessidade de se adequar à norma e ajustar seus processos, a fim de evitar sanções diante do atual ambiente que cada vez trata mais dados de clientes. Concomitante a isso, falta uma metodologia para orientar os processos de negócios que possa ser auditável e oriente a implantação do modelo de proteção à privacidade de dados com o controle, visando a mitigação dos riscos envolvidos no tratamento diário desses dados nas operações empresariais.

Autores como Alberton (2021) destacam ser provável que a teor do art. 49 da LGPD, por não ser restritivo, permite aplicação de orientações técnicas contidas em normas aceitas no âmbito regulatório da União Europeia, bem como as normas internacionais ISO 27001, 27002, 27701 E 27702. O artigo parte então desse problema analisado se a ISO 27701 pode servir de framework e se conteria os requisitos necessários para ser a ferramenta de controle na adequação à Lei Geral de Proteção de Dados.

Com o confronto das recomendações contidas na norma ISO 27701 e as disposições da Lei 13.709/2018 (LGPD), à luz do referencial teórico levantado, é possível concluir que a Norma ISO 27701, apesar de ser uma extensão da norma ISO 27001 - que trata de cibersegurança – pode com ressalvas, ser utilizada como modelo de compliance à LGPD.

2 REFERENCIAL TEÓRICO

A abundância de dados e informações que trafegam pela internet gerou a necessidade de se garantir o direito à privacidade dos indivíduos pois, segundo Maldonado e Blum (2022, p. 24) a atual capacidade computacional de processamento em que máquinas trocam comandos e informações entre si, não só viabiliza, mas acelera a possibilidade de armazenamento, tratamento e compartilhamento de dados.

Para Doneda (2010, p. 17) a informação pessoal é considerada uma verdadeira mercadoria, a partir da qual novos modelos de negócios aparecem procurando perceber valor monetário relativo ao intenso fluxo de informações pessoais advindas das tecnologias de informação.

Os escândalos financeiros nos anos de 2001 e 2002 nos EUA nas empresas ENRON, Arthur Andersen e MCI

Worldcom motivaram a edição de uma lei para impor maior rigor no controle sobre empresas que negociavam junto a Bolsa de Valores de Nova Iorque (Borgerth, 2007). A empresa de energia e gás natural ENRON, que chegou a ser a quinta maior empresa dos EUA, foi alvo de fraude contábil elaborada pelos executivos e principais sócios da empresa que, maquiavam os demonstrativos contábeis, não consolidando nessas demonstrações prejuízos de mais de 600 milhões de dólares americanos, que eram ocultados por meio de SPE´s (Sociedade de Propósito Específicos) criadas por estes para essa finalidade, em desconformidade com os princípios contábeis geralmente aceitos (USGAAP).

Desse contexto, originou-se a Lei Sarbanes-Oxley, com a finalidade de proteger investidores através da melhoria na acurácia e confiabilidade das demonstrações das companhias abertas em conformidade com a legislação sobre ativos securitários e, outros propósitos. Segundo Mullis (2009), um dos impactos trazidos pela norma é a necessidade de a empresa constituir e prover um sistema efetivo de controle interno, cuja estrutura deve servir para assegurar que os ativos da companhia sejam usados e descartados segundo essa estrutura, e em conformidade com regras instituídas pela SOX (Lei Sarbannes-Oxley). Esse controle interno pode ser realizado por áreas específicas, como a Auditoria Interna.

A função de Auditoria Interna é um dos pilares da governança corporativa. Weidenmier e Ramamoorti (2006) salientam ainda que, a Auditoria Interna ocupa um papel de destaque na governança corporativa considerando que ela é responsável pela coleta e reporte de informações para os outros atores da governança, além de ser parte da estrutura de controle interno da organização.

O cumprimento da norma contida na seção 302 da SOX está diretamente relacionada à Tecnologia da Informação uma vez que a maioria das empresas praticam o comércio eletrônico (BROWN; NASUTI, 2005). Ainda, afirmam estes autores que a necessidade de “compliance” com as normas SOX, levou à introdução do COBIT (Control Objectives for Information and Related Technology) como a estrutura conceitual aceita pelos auditores de TI, para assegurar conformidade à SOX. Segundo Hawkins, Alhajjaj e Kelley (2003), a estrutura conceitual COSO serve de base ao COBIT.

Surgem, então, iniciativas de novas estruturas conceituais, como a Generally Accepted Privacy Principles (GAPP) promovida pela American Institute of Certified Public Accountants e Canadian Institute of Chartered Accountants (AICPA / CICA), que possam permitir aos profissionais contábeis promover os serviços voltados a assegurar (assurance) o cumprimento (compliance) e a auditoria de procedimentos e verificação de conformidade com as normas de proteção de dados pessoais. Nesse aspecto, também resulta importante a adoção de medidas de reporte e construção de indicadores que possam contribuir com a gestão, controle e melhoria de desempenho. Dessa necessidade, surgiram iniciativas como a “ESG” (Environmental, Social, and Governance).

A metodologia e reporte ESG, deriva da evolução do pensamento acerca da Governança Corporativa e da Responsabilidade Social Corporativa, partindo do pressuposto que o gestor não pode apenas se concentrar na maximização do lucro para os acionistas (shareholders), mas também levar em consideração os diversos stakeholders e a sociedade como um todo. Isto porque caso a empresa tivesse como objetivo único obter lucro, sem trazer qualquer benefício social, ou até gerar eventual prejuízo social, esta não teria razão de existir (Post et al., 2002). As origens do ESG remontam à década de 1970, quando empresas como General Motors, Ford e Cummins Engine começaram a preparar um relatório sobre suas atividades filantrópicas

e envolvimento com a comunidade (WILBURN e WILBURN, 2013).

Na década seguinte, são incorporados também os aspectos ambientais, com uma ênfase originada pela ocorrência de desastres ambientais, como o vazamento de produtos químicos pela empresa Union Carbide, na região de Bhopal, na Índia, em 1984. Em virtude do aumento das demandas por informações as companhias passaram a, voluntariamente, divulgar em vários meios - como a internet - relatórios apartados com um conjunto cada vez mais complexo de informações. Sendo assim, surgiu o modelo integrado de relatório que possui como objetivo principal apresentar a performance social, financeira e ambiental da empresa de forma concisa e interconectada (de VILLIERS et al., 2014). O dogma da ESG é sua suposta capacidade de gerar sustentabilidade, o que atrai o interesse dos investidores que alinham seus aportes em empresas que são além de lucrativas, socialmente e ambientalmente responsáveis, conforme experimentado em décadas recentes (KOCMANOVÁ et al., 2011). Isso, portanto, motiva a adoção de estruturas (frameworks) de governança como a ESG.

A empresa Cambridge Analytica, fundada em 2013, foi acusada em março de 2018 por apropriação de dados de mais de 50 milhões de usuários do Facebook sem consentimento. Os dados foram coletados por meio de um aplicativo, inserido no Facebook, chamado de “This is Your Digital Life”. Os termos de uso do aplicativo solicitavam acesso aos dados dos usuários, como também de toda sua rede de amigos. Posteriormente, os perfis dos usuários eram analisados e categorizados de acordo com a demografia, comportamento do consumidor e atividade na internet, localizando potenciais eleitores, conforme destaca Humble (2020). Desta forma, os usuários foram atingidos pontualmente pela prática de “profiling” e influenciados politicamente nas eleições de 2010 dos Estados Unidos, por meio de Fake News e discursos de ódio (VAN DIJCK, 2020).

O escândalo da Cambridge Analytica disparou o alarme do impacto que a coleta, armazenamento e tratamento de dados pessoais por empresas provoca na sociedade. Lehfeld et al. (2021) afirma que a inexistência de proteção aos titulares no ambiente online pode ser uma violação aos direitos fundamentais, uma vez que os dados devem ser vistos não apenas como fonte de lucro, mas também como fonte de poder, devido ao seu potencial de impacto e manipulação em massa da escolha individual. Desta maneira, o Regulamento Geral de Proteção de Dados (GDPR) foi criado em 2016, pela União Europeia, para assegurar os direitos dos titulares e obrigações legais na segurança de dados das organizações localizadas nos países da União Europeia e, no Brasil, com base no GDPR da união Europeia foi criada a Lei Geral de Proteção de Dados (LGPD) em 2018.

Entretanto, antes da LGPD, surge a Lei de Acesso à Informações (Lei 12.527/2011) que é composta de 6 (seis) capítulos e 47 (quarenta e sete) artigos. Em seu preâmbulo, constata-se que a sua finalidade é de regulamentar o direito fundamental (art. 3º) de acesso à informação previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Analisando a Lei de Acesso à Informação nos aspectos de proteção de dados pessoais e a privacidade, o Art. 4º estabeleceu o conceito de informação pessoal, antes da LGPD, como sendo aquela relacionada à pessoa natural identificada ou identificável. A Lei Geral de Proteção de Dados nº 13.709, originada do Regulamento Geral de Proteção de Dados (GDPR), foi aprovada em 14 de agosto de 2018 e entrou em vigor em 18 de setembro de 2021. É aplicável à pessoa natural ou jurídica de direito público ou privado, que realiza o tratamento de dados pessoais, sensíveis ou não, de pessoas físicas, em meios físicos e digitais.

Para promoção das boas práticas de governança corporativa, conforme art. 50, os agentes de tratamento, controladores e os

operadores devem estabelecer regras que compreendam o regime de funcionamento, as condições de organização, reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas de cada tratamento, os controles internos de supervisão e mitigação de riscos e as ações educativas que serão realizadas na organização. Por sua vez, o parágrafo 2º do art. 50 trata da implementação de um programa de governança que deverá: demonstrar comprometimento na adoção de políticas e normas de privacidade de dados; atue de forma transparente para estabelecer confiança; esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; seja atualizado constantemente.

Para Doneda e Mendes (2018) a Lei 13.709/2018 – (LGPD) inaugura no Brasil um regime geral de proteção de dados pessoais. Para os autores "a referida Lei vem complementar o marco regulatório brasileiro da Sociedade da Informação ao compor, juntamente com a Lei de Acesso à Informação, o Marco Civil da Internet e o Código de Defesa do Consumidor", formando um conjunto normativo modernizado de tratamento da informação no Brasil (DONEDA; MENDES, 2018, p. 470). Os autores ressaltam que o objetivo é "proporcionar garantias aos direitos do cidadão, ao mesmo tempo em que fornece as bases para o desenvolvimento da economia da informação, baseada nos vetores da confiança, segurança e valor" (DONEDA; MENDES, 2018, p. 470).

Para Doneda (2010) a Lei Geral de Proteção de Dados procura fortalecer as relações entre consumidores que fornecem os dados e as entidades que retem esses dados, estabelecendo assim um equilíbrio entre as relações de consumos e satisfazendo direitos elencados na Constituição como fundamentais e invioláveis (DONEDA, 2010, p. 42). Ao comentar o disposto no art. 49 da LGPD, Alberton (2021) afirma que, ao contrário da GDPR, a LGPD não determina quais medidas específicas de segurança devem ser adotadas pelo controlador ou processador, embora de acordo com o ato ordinatório nº 11/2021, se espera que a Autoridade Nacional de Proteção de Dados, venha a prover um mínimo de padrões técnicos que possam auxiliar os agentes a cumprir com os padrões de segurança e privacidade de dados requeridas pela LGPD, ressaltando ainda que, por não ser restritiva, deva permitir a aplicação de orientações técnicas contidas em normas aceitas no âmbito regulatório da União Europeia, bem como as normas internacionais ISO 27001, 27002, 27701 E 27702.

International Organization for Standardization é uma entidade suíça fundada em 1947, com a finalidade de facilitar as transações entre empresas por meio da conciliação das normas industriais de diversos países. Desta forma, foram desenvolvidas as principais normas ISO 9000, ISO 9001 e ISO 9004 que apoiam as empresas para que alcancem um sistema de gestão de qualidade efetivo. Segundo Muncinelli et al. (2020), os padrões ISO integram um conceito de sistema de gestão, ou seja, oferecem parâmetros de como as atividades se coordenam, permitindo o controle e a direção para que a organização possa atingir seus objetivos. Portanto a norma ISO/IEC 27001, se constitui Sistema de Gestão de Segurança da Informação, especificando requisitos para estabelecer, implementar, manter e desenvolver melhorias contínuas da gestão de segurança da informação, além e conter requisitos, de forma genérica, para verificação de tratamentos dos riscos à segurança de informação (MUNCINELLI, et al., 2020).

As normas ISO 27000, ISO 27001 e ISO 27002, proveem a proteção dos sistemas de informação, objetivos de controle, especificações de controle, requisitos e guias, com os quais a empresa consegue alcançar uma proteção. O conjunto dessas normas permitem à empresa ser certificada por meio dos padrões nela contidos, de modo que a gestão

de segurança da informação possa ser documentada, aplicada com rigor, e gerenciada de acordo com um reconhecido padrão internacional de organização (DISTERER, 2013).

Segundo Culot (2021), dentre os sistemas de segurança de informação, a ISO 27001 é provavelmente a mais conhecida e ocupa o terceiro lugar dentre as certificações mundiais mais difundidas da ISO, atrás das normas ISO 9001 e ISO 14001.Por sua vez, a norma ISO 27701, é uma extensão da norma ISO 27001, para abranger também a privacidade de dados, elastecendo os requisitos também para a proteção de dados pessoais. Em agosto de 2019 a ISO - International Standardization Organization publicou a norma ISO 27701:2019, elaborada como uma extensão às normas que já tratavam do sistema de gestão de segurança da informação ISO 27001 e ISO 27002, com a finalidade de normatizar também os procedimentos de proteção à captura, responsabilidade, disponibilidade, integridade e confidencialidade de dados pessoais (LACHAUD, 2020).

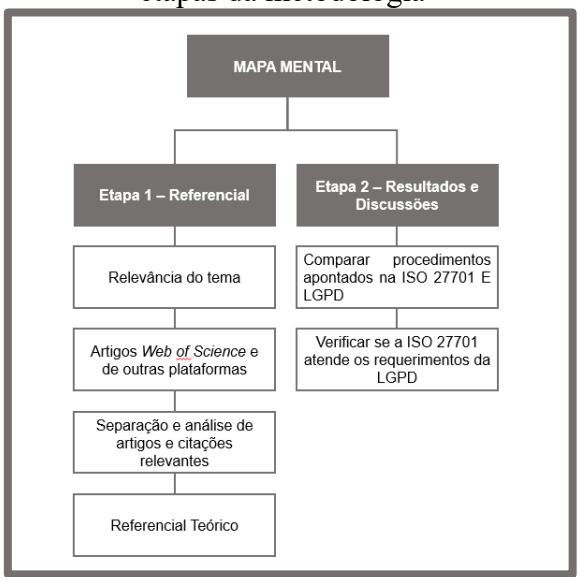
Milagre (2019, p. 3) afirma que a ISO 27701 tem o objetivo de "contribuir para que empresas demonstrem a agências, órgãos públicos, investidores e sociedade que a organização está empenhada em adotar controles eficazes e que são considerados melhores práticas internacionais em proteção de dados". Assim a norma ISO 27701 além de especificar os requisitos também fornece as diretrizes para se estabelecer, implementar, e realizar a manutenção e melhoria contínua de um sistema de gestão de privacidade da informação. Para Lachaud (2020, p. 4) a ISO/IEC 27701:2019 em conjunto com a ISO/IEC 27001:2013 "propõe uma abordagem consistente que mistura segurança da informação e proteção de dados (Privacidade)".

Ressalta-se que a norma 27701 amplia ou estende os requisitos e orientações trazidas pela ISO 27001 (requisitos) e 27002 (códigos de prática), e estar em "conformidade com a norma 27701 é inovar e garantir atendimento aos requisitos de privacidade das principais regulamentações de proteção de dados" (MILAGRE, 2020, p. 3). Assim, certificar-se na ISO 27001 e de forma estendida na ISO 27701, demonstra o reconhecimento por parte dos atores interessados e pela própria Autoridade, de que a empresa adota e se preocupa com as melhores práticas no que diz respeito a privacidade da informação. Milagres (2020) ressalta ainda que a ISO 27701 se apresenta como o "guia do que fazer" para que as empresas estejam em conformidade com a LGPD.

3 PROCESSOS METODOLÓGICOS

Foi selecionada uma abordagem de pesquisa qualitativa que se desenvolverá pela revisão da bibliografia sobre os temas: privacidade de dados, Lei Geral de Proteção de Dados – LGPD, GDPR – General Data Protection Regulation e ISO 27701. O levantamento dos dados bibliográficos, foi realizado a partir dos filtros disponíveis na plataforma Web of Science, obtendo-se 122 resultados. Posteriormente, foi aplicado o filtro de ano de publicação, para artigos publicados de 2017 a 2021, totalizando 24 artigos, que foram analisados e excluídos os periódicos de assunto: Mobilidade Urbana, Ciência Biológicas, Bioquímica, Medicina, Análise de Sistemas. Desta forma, restam 6 artigos de acordo com o tema objeto desta pesquisa.

FIGURA 1 – Mapa mental contendo as etapas da metodologia



Fonte: elaborado pela autora (2022).

Utilizando-se da Análise de Conteúdo, que segundo Bardin (1997, p. 42) se refere a "um conjunto de técnicas de análises das comunicações visando obter, por procedimentos, sistemáticos e objetivos da descrição do conteúdo das mensagens, indicadores (quantitativos ou não) que permitem a inferência de conhecimentos relativos às condições de produção/recepção (variáveis inferidas) destas mensagens", para então realizarmos a comparação dos temas eventualmente contidos nas respectivas normas legal e técnica, com a finalidade de responder ao questionamento que norteia a pesquisa.

Além disso, para elaboração do referencial teórico relativo aos 7 (sete) temas adicionais, por meio de pesquisa nas plataformas Google Scholar e Web of Science foram escolhidos artigos sobre: 1) Marco Civil da Internet; 2) Lei de Acesso à Informação; 3) Cambridge Analytica; 4) Inteligência Artificial; 5) International Organization for Standardization; 6) Governança corporativa de dados e indicadores ESG; 7) Sarbanes-Oxley. Em relação aos temas Marco Civil da Internet e Lei de Acesso à Informação foi essencial a verificação das Leis n° 12 965/2014 e nº 12.527/2011, respectivamente. Após revisão dos resumos dos artigos foram eleitos outros 41 (quarenta e um) artigos que colaboram com a construção do estudo.

Por meio da análise de conteúdo realizada na LGPD foi possível identificar 9 (nove) tópicos para comparação com a ISSO 27701, sendo: Compartilhamento de dados entre empresas; Papéis dos Agentes; Princípios da LGPD; Sigilo e segurança de dados; Requisitos de tratamento de dados; Dados pessoais sensíveis; Término do tratamento; Transferência internacional; Encarregado de dados e; Boas práticas de governança.

4 RESULTADOS E DISCUSSÃO

A subseção 8.5.5 da norma ISO 27701, prescreve a possibilidade de divulgação de dados pessoais em casos específicos, e recomenda a rejeição de solicitações que não sejam legalmente obrigatórias, ressalvando a possibilidade de solicitações "contratualmente" acordadas, mediante autorização do cliente. A recomendação contida na ISO 27701 é mais genérica ao tratar da divulgação de dados legalmente obrigatória. A LGPD é mais restritiva, haja vista que excetua a aplicação da Lei para dados pessoais em hipóteses expressas na lei, como os de eventual solicitação por órgãos do poder público. Acerca dos dados pessoais e o compartilhamento destes entre empresas privadas por questões contratuais e comerciais, esta é permitida, desde que com autorização específica do titular, nos termos do art. 5º, IX e art. 7º, § 5º da LGPD.

Em relação ao compartilhamento de dados obtidos por transferência internacional, nos modos descritos no art. 4º, IV da LGPD, recomenda a norma ISO 27701, na subseção 6.15.1.3, que a organização retenha os documentos relativos aos procedimentos para suprir eventual solicitação dos órgãos competentes, por exemplo em caso de litígio. A norma ISO 27701 recomenda que quando a organização atua tanto como

controlador, quanto como operador, sejam determinados papéis distintos. Contudo, a LGPD não faz distinção entre tais papéis e considera ambos, controlador e operador, agentes de tratamento de dados.

O art. 6º da LGPD estabelece que "as atividades de tratamento de dados pessoais deverão observar a boa fé e os seguintes princípios":

I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (BRASIL, 2018).

No caso brasileiro, o legislador foi mais detalhista e descreveu o conceito de cada princípio, por sua vez a norma ISO é imprecisa, citando apenas algumas recomendações que guardam apenas parcial relação com os princípios da LGPD. A título de exemplo, conforme consta do anexo da norma ISO 27001, é possível citar o teor da subseção 8.3 e 8.3.1, que enfatiza a necessidade de informação e consentimento do titular (princípio do livre acesso).

Apesar das recomendações enfatizarem a necessidade de minimização da coleta de dados, estabelecendo inclusive que estes devam ter relação com os propósitos identificados (princípios da necessidade e adequação), bem como, a manutenção da qualidade e precisão dos dados (qualidade dos dados), há princípios que não encontram recomendação compatível, tais como: transparência, segurança, prevenção, não-discriminação, responsabilização e prestação de contas.
Em relação ao sigilo e segurança de dados pessoais o art. 46° da LGPD estipula que os agentes de tratamento, controladores e operadores, devem estabelecer controles com capacidade para proteger as informações dos titulares de acessos ilícitos, destruição, perda, alteração, ou qualquer outro tratamento não autorizado.

Neste contexto, a ISO 27701 aborda os aspectos que podem ser adotados como meio de promoção da segurança das informações nas subseções 6.3.2.1, 6.5.2.1, 6.5.2.2, 6.5.3.1, 6.5.3.2, 6.5.3.3, 6.6.2.1, 6.6.2.2, 6.6.4.2, 6.7.1.1, 6.8.2.7, 6.8.2.9, 6.9.3.1, 6.9.4.1, 6.9.4.2, 6.10.2.1, 6.10.2.4, 6.11.1.2, 6.11.3.1, 6.12.1.2, 6.13.1.1, 8.4.1,

8.4.2, 8.4.3, contendo os temas: Política para o uso de dispositivo móvel, Classificação da informação, Rótulos e tratamento da informação, Gerenciamento de mídias removíveis, Descarte de mídias, Transferência física de mídias, Registro e cancelamento de usuário, Provisionamento para acesso de usuário, Procedimentos seguros de entrada no sistema (log-on), Política para o uso de controles criptográficos, Reutilização ou descarte seguro de equipamentos, Política de mesa limpa e tela limpa, Cópias de segurança das informações, Registros de eventos (logs), Proteção das informações dos registros de eventos (logs), Políticas e procedimentos para transferência de informações, Acordos de confidencialidade e não divulgação, Serviços de aplicação seguros em redes públicas, Proteção dos dados para teste, Identificando segurança da informação nos acordos com fornecedores, Responsabilidades e procedimentos, Arquivos temporários, Retorno, transferência ou descarte de DP, Controles de transmissão de DP, respectivamente.

Os itens descritos na ISO reforçam a essencialidade do entendimento e estabelecimento do fluxo de processamento dos Dados Pessoais (DP), desde sua origem – coleta – ao seu término – descarte/eliminação. As subseções 6.6.2.1, 6.6.2.2 e 6.6.4.2 tratam abrangentemente de técnicas para a prevenção do acesso não autorizado pelo gerenciamento de perfis de usuários. Eventuais situações acidentais ou ilícitas de perda de dados seriam mitigadas pela adoção das recomendações contidas na subseção 6.9.3.1 que trata do backup. O controle de alterações dos dados é abordado nas subseções 6.9.4.1 e 6.9.4.2, itens nos quais são recomendados o registro de eventos (log) e a proteção desse registro.

Quanto à segurança da comunicação dos dados, existe recomendação de utilização de criptografia de ponta a ponta, o que excede, em princípio, os requisitos contidos na LGPD. Tais medidas são mencionadas na subseção 6.10.2.1, que trata da comunicação e transferência dos dados, assim como na subseção 6.10.2.4 que recomenda seja realizado acordo de confidencialidade com terceiros que solicitem acesso a estes. Desta maneira, o art. 47 da LGPD que precisa que todos os agentes que mediam o tratamento dos dados estão obrigados a adotar salvaguardas na segurança das informações são assegurados por meio do acordo de confidencialidade.
Outrossim, o art. 48 da LGPD que trata da comunicação às autoridades sobre incidentes de privacidade é abordado suficiente na subseção 6.13.1.5 da ISO 27701.

Observa-se que os controles mencionados na ISO 27701 são majoritariamente originários da NBR ISO/IEC 27002:2013, normativa na qual são definidos parâmetros para a prática de gestão de segurança da informação e técnicas de segurança. Sendo assim, a ISO 27701 acrescenta mínimas modificações, se não nenhuma, no que tange aos controles que devem ser implementados pelos agentes de tratamento. Conquanto, as recomendações expostas na ISO 27701 atendem às exigências básicas do art. 46 e art. 47 da LGPD sobre o sigilo e segurança das informações.

O tratamento de dados pessoais somente poderá ser realizado caso esteja embasado nas 10 (dez) hipóteses legais constantes no art. 7° da LGPD. A ISO 27701 subseção 7.2.2, identificação de bases legais, recomenda que a organização se adeque às hipóteses legais de tratamento, levando em consideração a previsão da jurisdição de acordo com cada processo.

A primeira hipótese legal condiciona o tratamento de dados ao consentimento do titular. Por sua vez, as demais hipóteses não necessitam de consentimento por se tratar de processamentos regulamentares, contratuais, de saúde, ou que tenham por finalidade a pesquisa científica. Ressalva-se, todavia, que a norma ISO 27701 na subseção 7.2.7, ao tratar do conjunto de dados pessoais recomenda apenas que se determine as responsabilidades e os papéis

para tratamento dos dados com eventual controlador conjunto.

A partir da definição de consentimento, que está descrita no artigo 5º da LGPD como sendo a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", a legislação garante os direitos do cidadão, proporcionando autonomia e segurança tanto para ele como para seus dados (LGPD Brasil, 2023). Neste quesito, a Lei Geral de Proteção de Dados exige que para o compartilhamento de dados com outro controlador seja solicitado novo consentimento específico para essa finalidade (Art. 7° § 5º). Além disso, são nulas as autorizações genéricas de consentimento e estas deverão referir-se à finalidade determinada (Art. 8° § 4º).

As subseções 7.3.1 e 7.3.3 da ISO 27701 propõem que a informação seja ofertada ao titular de forma clara, como também aconselha a divulgação do ponto de contato do encarregado de dados, sugerindo inclusive que se utilize a mesma forma pela qual se obteve o consentimento para conceder o acesso aos dados do titular, o que cumpre com as exigências contidas no caput do art. 9° da LGPD.

Já a subseção 7.3.2 determina que os titulares sejam informados sobre o propósito do tratamento realizado com seus dados, desta forma, satisfazendo a requisição acerca da finalidade (Art. 9°, I). Em relação ao disposto no inciso VII do art. 9° da LGPD, embora conste do anexo da norma ISSO 27701 que as subseções 8.2.2 e 8.2.3 se referem a essa exigência, observa-se que não há expressa recomendação a que se informe o titular dos dados pessoais de seus direitos (Art. 18 da LGPD). Tampouco consta nessas subseções qualquer menção acerca da necessidade de distribuição das responsabilidades entre os controladores conjuntos, conforme art. 9°, VI da LGPD.

A mudança no propósito de tratamento que não seja compatível ao consentimento fornecido inicialmente, o controlador deve informar o titular sobre a possibilidade de revogação do consentimento, caso o titular não possua interesse em aditar o consentimento para os novos propósitos (art. 9° § 2). Desta forma, a interpretação conjunta das subseções 7.3.2, 7.3.4 e 7.3.5 da ISO apresenta a responsabilidade do controlador em relação ao repasse da informação sobre a alteração de finalidade ao titular e a realização de novo termo de consentimento.

O art. 10° da LGPD condiciona o tratamento de dados pessoais para finalidades legítimas que se fundamente no legítimo interesse do controlador, a partir de situações concretas. Nesse aspecto, a norma ISO 27701 estabelece nas subseções 8.2.1, 8.2.2 e 8.2.3 que os dados sejam tratados apenas para propósito expresso, legítimo e claramente definido.

A Lei Geral de Proteção de Dados limita as possibilidades de tratamento de dados sensíveis e lista as hipóteses no art. 11, I e II. Contudo, a norma ISO, nas subseções 7.2.3, 7.2.2 e 7.2.4, somente refere ao consentimento e observância da base legal. Aliás, iguais disposições e recomendações são indicadas para o tratamento de dados pessoais de crianças e adolescentes (art. 14, §6 da LGPD).

O término do tratamento de dados pessoais ocorrerá, conforme art. 15 da LGPD, quando a finalidade for alcançada, o período determinado tiver terminado, o titular revogar o consentimento, ou por determinação da ANPD em casos de violação da lei. Destas hipóteses, somente quando a finalidade for alcançada e o prazo de retenção do dado tiver acabado são abordadas nas subseções 7.4.6 e 7.4.7 da ISO 27701. Verifica-se, portanto, neste quesito a norma atende parcialmente os requerimentos da LGPD.

Embora a ISO, subseção 7.4.7, não recomende a retenção de dados após o alcance da finalidade o art. 16 da LGPD prevê exceções que autorizam a retenção para as seguintes finalidades: Cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida, sempre que possível, a

anonimização dos dados pessoais; transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Acerca da transferência internacional de dados as subseções 8.5.1 e 8.5.2 da ISO estabelecem que o controlador deve documentar o compartilhamento por meio de contrato e constituir cláusulas identificando os países aos quais os dados serão transferidos e as circunstâncias nas quais ocorrerão o compartilhamento, com a finalidade de informar o titular.

Isto posto, a ISO não fornece orientação satisfatória em adequação ao art. 33 da LGPD, que por sua vez restringe o compartilhamento internacional em nove hipóteses, principalmente à países e organizações internacionais que estão sujeitos à normas de proteção de dados equivalentes, em casos que se possa garantir normativamente a devida proteção aos dados com cláusulas contratuais; cooperação jurídica internacional; a transferência for necessária à proteção à vida; autorizada pela ANPD; necessária execução de política pública; consentido pelo titular; necessário ao cumprimento do art. 7°.

A subseção 6.3.1.1 da ISO define sobre a nomeação do encarregado de dados que: “Convém que a organização indique uma ou mais pessoas responsáveis pelo desenvolvimento, implementação, manutenção e monitoramento de um programa amplo de privacidade e governança da organização, para assegurar compliance com todas as leis e regulamentações aplicáveis, relacionadas ao tratamento de DP.”

Entretanto para a LGPD, art. 41, o controlador deve indicar apenas um encarregado de dados.

Por fim, em relação às boas práticas de governança corporativa determina o art. 50 da Lei Geral de Proteção de Dados que as organizações poderão formular regras de boas práticas de governança para tratamento dos dados. Para tanto, contata-se que o conjunto de normas ISO 27001, 27002, 29100 e 27701 integram um sistema que comtempla procedimentos e técnicas que auxiliam a organização a constituir o seu sistema de gerenciamento de segurança e gestão de privacidade.

O Quadro 1, apresenta de forma simples uma análise da relação entre as orientações da ISO e os tópicos da LGPD.

QUADRO 1 – Análise Comparativa entre tópicos da LGPD e a ISO

TÓPICO	ANÁLISE
Compartilhamento de dados entre empresas	A ISO 27701 é genérica ao tratar da divulgação de dados legalmente obrigatória, já a LGPD é restritiva e excetua hipóteses expressas na lei.
Papéis dos Agentes	Para a LGPD controlador e operador são agentes de tratamento. Por sua vez, a ISO determina que sejam segregados os papéis entre controlador e operador.
Princípios da LGPD	Não são abordados em sua totalidade na ISO 27701. Assim sendo, não há recomendação compatível para os princípios da transparência, segurança, prevenção, não-discriminação, responsabilização e prestação de contas.
Sigilo e segurança de dados	A ISO 27701 excede os requisitos contidos na LGPD, sendo assim é suficiente.
Requisitos de tratamento de dados	A ISO apenas sugere o cumprimento da lei e observação da legislação local.
Dados pessoais sensíveis	A LGPD é limitante no que tange ao tratamento de dados pessoais sensíveis, no entanto a ISO somente se refere ao consentimento e observância da base legal.
Término do tratamento	Para a LGPD o término do tratamento possui exceções (Art. 16 da LGPD), contudo para a ISO o tratamento deverá ser finalizado quando a finalidade foi alcançada, sem ressalvas.

Transferência internacional	Não recebe orientação suficiente na ISO em adequação ao art. 33 da LGPD, que conta com nove hipóteses visando a garantia do compartilhamento seguro para outros países.
Encarregado de dados	A ISO confere a possibilidade de indicação de um ou mais responsáveis para exercício da função, entretanto a LGPD estabelece a indicação de apenas um encarregado de dados.
Boas práticas de governança	O conjunto das normas ISO 27001, 27002, 29100 e 27701 contemplam parâmetros e procedimentos que asseguram as boas práticas de governança, em conformidade com o art. 50 da LGPD.

Fonte: Elaborada pela autora, 2022.

Doneda e Mendes (2018) ressaltam que é preciso "desenvolver uma cultura de proteção de dados, construir uma sólida estrutura institucional para a aplicação da LGPD, assim como uma doutrina aprofundada sobre os diferentes temas tratados pela Lei", propiciando, assim, "uma segurança jurídica para os atores da economia digital, a proteção da confiança do titular dos dados e incentivando o desenvolvimento econômico do país nessa área" (DONEDA; MENDES, 2018, p. 482).

5 CONCLUSÃO & PERSPECTIVAS

A LGPD é imprescindível à asseguração do direito fundamental de privacidade e ao exercício da liberdade individual na promoção da democracia. Inicialmente, o Marco Civil da Internet e Lei de Acesso à Informações nº 12.527/2011 quebraram os preceitos de que a internet era uma terra sem lei, na qual as organizações poderiam se apropriar e tratar dados em prol de seu lucro, seguindo o exemplo da empresa Cambridge Analytica.

A adoção de um framework adequado é essencial para assegurar (assurance) o cumprimento (compliance) e a auditoria de procedimentos e verificação de conformidade das normas de segurança e proteção de dados pessoais, sendo este trabalho desenvolvido por profissionais contábeis.

O artigo desdobra os seguintes pontos: Compartilhamento de dados entre empresas, papéis dos agentes, princípios da LGPD, sigilo e segurança de dados, requisitos de tratamento de dados, dados pessoais sensíveis, término do tratamento, transferência internacional, encarregado de dados e boas práticas de governança. A análise dos pontos em comparação aos procedimentos apontados na ISO 27701 demonstra lacunas que devem ser preenchidas pela ANPD com as futuras normatizações.

Conclui-se, portanto, que a ISO 27701 cumpre parcialmente com os requisitos da LGPD, servindo como base e framework para conformidade com a Lei Geral de Proteção de Dados, desde que o gestor complemente as recomendações mais genéricas à luz dos princípios contidos na lei.

REFERÊNCIAS

ALBERTON, C. S. C. The fundamental right of confidentiality and integrity of IT systems in Germany: a call for "IT Privacy" right in Brazil?. **International Cybersecurity Law Review**, v. 2, n. 2, p. 253-269, 2021.

ABNT. **ASSOCIAÇÃO Brasileira De Normas Técnicas** (2013), NBR ISO/IEC 27002 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT. 99p, 2013.

ABNT. **ASSOCIAÇÃO Brasileira De Normas Técnicas** (2006), NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos. Rio de Janeiro: ABNT. 34p., 2006.

ABNT. **ASSOCIAÇÃO Brasileira De Normas Técnicas** (2019), NBR ISO/IEC 27701 – 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. 82p., 2019.

BARDIN, L. **Análise de conteúdo**. Lisboa, Portugal: Edições 70, 1997.

BORGERTH, V. M. C. SOX: **Entendendo a Lei Sarbanes-oxley**. São Paulo: Thomson Learning, 116p. 2007.

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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm, 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm, 2014

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm, 2018.

BROWN, W.; NASUTI, F. What ERP systems can tell us about Sarbanes-Oxley. **Information Management & Computer Security**, v. 13, n. 4, p. 311-327, https://doi.org/10.1108/09685220510614434, 2005.

CULOT, G. et al. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. **The TQM Journal**, v. 33, n. 7, p. 76-105, https://doi.org/10.1108/TQM-09-2020-0202, 2021.

DE VILLIERS, C. et al. Integrated Reporting: Insights, gaps and an agenda for future research. **Accounting, Auditing & Accountability Journal**, v. 27, n. 7, p. 1042-1067, https://doi.org/10.1108/AAAJ-06-2014-1736 , 2014.

DISTERER, G. **ISO/IEC 27000, 27001 and 27002 for information security management**. Journal of Information Security, v. 4, p. 92 -100, http://dx.doi.org/10.4236/jis.2013.42011, 2013.

DONEDA, D. (org). **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Brasília: SDE/ DPDC, 2010.

HAWKINS, K. W.; ALHAJJAJ, S.; KELLEY, S. S. Using CobiT to secure information assets. **The Journal of Government Financial Management**, v. 52, n. 2, p. 22, 2003.

HUMBLE, K. P. International law, surveillance and the protection of privacy. **The International Journal of Human Rights**, v. 25, n. 1, p. 1-25, 2020.

KOCMANOVÁ, A. et al. Sustainability: environmental, social and corporate governance performance in Czech SMEs. In: **The 15th World Multi-Conference on Systemics, Cybernetics and Informatics**. 2011. p. 94-99.

LACHAUD, E. **Third-Party Certification and Cross-Border Flows in the GDPR: Which Workable Option?** Preprint, 2020. Disponível em: https://www.researchgate.net/publication/339988867_ISOIEC_27701_Threats_and_Opportunities_for_GDPR_Certification. Acesso em: Fev. 2024.

LEHFELD, L. S. et al. A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, p. 10, 2021.

LGPD Brasil. **Consentimento: conheça uma das bases legais mais importantes da LGPD.** Disponível em Consentimento: conheça uma das bases legais mais importantes da LGPD - LGPD (lgpdbrasil.com.br) acesso em out 2023.

MALDONADO, V. N; BLUM, R. O. LGPD: Lei Geral de Proteção de Dados Comentada. São Paulo: **Revista dos Tribunais**, 4ª ed. 2022.

MILAGRES, J. ISO 27701: Como a norma se harmoniza com a LGPD e como adequar e certificar sua empresa? Jusbrasil, 2020. Disponível em https://www.jusbrasil.com.br/artigos/iso-27701-como-a-norma-se-harmoniza-com-a-lgpd-e-como-adequar-e-certificar-sua-empresa/783012120. Acesso em Fev. 2024.

MILAGRES, J. ISO 27701: O que é ISO 27701 e como entender a aplicação da norma para gestão da privacidade da informação em 5 passos. Jusbrasil, 2019. Disponível em https://www.jusbrasil.com.br/artigos/o-que-e-iso-27701-e-como-entender-a-aplicacao-da-norma-para-gestao-da-privacidade-da-informacao-em-5-passos/791257034. Acesso em Fev. 2024.

MULLIS, J. **The Impact of the Sarbanes-Oxley Act of 2002 on Computer Forensic Procedures in Public Corporations**. University of Oregon
Eugene, OR, 2009.

MUNCINELLI, G. et al. **Components of the Preliminary Conceptual Model for Process Capability in LGPD** (Brazilian Data Protection Regulation) Context. Transdisciplinary Engineering for Complex Socio-technical Systems – Real-life Applications, J. Pokojski et al. (Eds.), 2020.

POST, J. E. et al. **Redefining the corporation: Stakeholder management and organizational wealth**. Stanford University Press, 2002.

VAN DIJCK, J. Governing digital societies: Private platforms, public values. **Computer Law & Security Review**, v. 36, p. 105377, April 2020.

WILBURN, K.; WILBURN, R. Using global reporting initiative indicators for CSR programs. **Journal of Global Responsibility**, v. 4, n. 1, p. 62-75, 2013.

WEIDENMIER, M. L.; RAMAMOORTI, S. Research opportunities in information technology and internal auditing. **Journal of Information Systems**, v. 20, n. 1, p. 205-219, 2006.