UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL MESTRADO

DILÇA CABRAL DE JESUS

PROPOSTA DE UM PROJETO DE CONFORMIDADE A PARTIR DAS PRÁTICAS DA ISO 27701 PARA IMPLEMENTAÇÃO DE UM PROGRAMA COMPLIANCE DE PROTEÇÃO DE DADOS À LUZ DA LGPD NA UNIVERSIDADE DE RIO VERDE

Rio Grande do Sul – RS
2022

DILÇA CABRAL DE JESUS

PROPOSTA DE UM PROJETO DE CONFORMIDADE A PARTIR DAS PRÁTICAS DA ISO 27701 PARA IMPLEMENTAÇÃO DE UM PROGRAMA COMPLIANCE DE PROTEÇÃO DE DADOS À LUZ DA LGPD NA UNIVERSIDADE DE RIO VERDE

Dissertação apresentada no Curso de Mestrado, como requisito para obtenção do grau de Mestre em Mestrado Profissional em Direito das Empresas e dos Negócios.

Orientado: Prof. Dr. Silvio Bittencourt da Silva

Rio Grande do Sul – RS

2022

J58p Jesus, Dilça Cabral de.
Proposta de um projeto de conformidade a partir das práticas da ISO 27701 para implementação de um programa compliance de proteção de dados à luz da LGPD na Universidade de Rio Verde / por Dilça Cabral de Jesus. – 2022.
132 f. : il. ; 30 cm.

Dissertação (mestrado) — Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, São Leopoldo, RS, 2022.
"Orientado: Dr. Silvio Bittencourt da Silva".

1. Dados pessoais. 2. Segurança. 3. Norma técnica. 4. Lei geral de proteção de dados pessoais (LGPD). 5. Lei de acesso à informação. 6. Privacidade. 7. Compliance. 8. Tecnologia. I. Título.

CDU: 343.45

Catalogação na Publicação (CIP):
Bibliotecário Alessandro Dietrich - CRB 10/2338

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL MESTRADO

A tese intitulada: "Proposta de um projeto de conformidade a partir das práticas da ISO 27701 para implementação de um Programa Compliance de proteção de dados à luz da LGPD na Universidade de Rio Verde", elaborada pela mestranda Dilça Cabral de Jesus, foi julgada adequada e aprovada por todo os membros da Banca Examinadora para obtenção do título de MESTRA EM DIREITO.

São Leopoldo, 23 de novembro de 2022

Prof. Dr. Fabiano Koff Coulon
Coordenador do Programa de Pós-Graduação em Direito

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dr. Silvio Bittencourt da Silva
Membro: Dr. Manoel Gustavo Neubarth Trindade
Membro: Dr. Cristiano Colombo
Membro: Dr. Carolina Merida

DEDICATÓRIA

Dedico este trabalho à minha família que tanto torceu por mim.

AGRADECIMENTOS

Agradeço primeiramente à Deus pela vida, e com ela um leque de oportunidades a serem conquistadas.

À Nossa Senhora Aparecida que me acompanhou em todo o trajeto deste trabalho.

Ao meu esposo Fernando Duarte Cabral e minhas joias precisas Enzo Gabriel Duarte Cabral e Antonella Duarte Cabral, pela compreensão e amor nesse período de muito estudo, o qual precisei dedicar com afinco para concretizar este trabalho.

Agradeço também minhas irmãs Carlabianca e Olga, que me amam infinitamente e que desejam o meu melhor sempre.

Aos meus cunhados Renato Canevari pelas sugestões valiosas, Rodrigo e Renato Duarte, obrigada pelas infinitas orações para o alcance desse grande objetivo.

Aos meus sobrinhos que nos momentos cansativos eles estavam ali para me fazer sorrir e acreditar que tudo iria dar certo.

Aos meus pais que sempre ressaltaram a importância do estudo na nossa vida.

À Hérica Cristina Paes Nascimento que sempre acreditou no meu potencial e contribui comigo nessa caminhada.

Meus sinceros agradecimentos ao meu orientador Dr. Silvio Bitencourt da Silva, com a gentileza e sabedoria que me conduziu nesta pesquisa, direcionando de forma primária na construção do conhecimento e produção deste trabalho. Sem o qual não teria alcançado êxito.

À Universidade de Rio Verde que possibilitou a realização deste mestrado, na construção do conhecimento de seu corpo administrativo. O meu sincero agradecimento por este olhar de carinho com seu corpo administrativo.

A um amigo José Idelfonso pelas explicações sobre a ISO 27701/2019

RESUMO

A sociedade atual, marcada pelas revoluções ocorridas nas últimas décadas, tem suas relações, de variados níveis, pautadas na troca de informações. Esta nova dinâmica impulsionada, principalmente, pelo surgimento e expansão da internet, trouxe inegáveis benefícios. Diante disto, o estudo teve como objetivo abordar a questão da proteção de dados, com enfoque para a Universidade de Rio Verde, a fim de avaliar a necessidade de implantação no âmbito da instituição, de um programa de *compliance* de dados pautado na LGPD e na ISO 27701. Para isso, desenvolveu-se uma pesquisa baseada em três etapas, identificação do problema, organização documental da pesquisa (referencial teórico) e a aplicabilidade dela, por meio da sugestão de implementar um programa *compliance* de proteção de dados à luz da LGPD e da ISO 27701 na UniRV – Universidade de Rio Verde. Por conta dos transtornos gerados pelo compartilhamento de dados pessoais, o legislador, ao longo dos anos, buscou soluções, com a elaboração de normas legais diversas, até culminar com a criação de uma lei específica, a Lei n. 13.709, de 14 de agosto de 2018, denominada de Lei Geral de Proteção de Dados ou LGPD. Surge, então, para as organizações, o desafio de ajustar suas atividades para estar em conformidade com a legislação e, concomitantemente, garantir a segurança dos dados pessoais aos quais tem acesso, o que, também, se tornou um diferencial competitivo no mercado. Isto, porém, exige mudanças e ajustes práticos, motivo pelo qual elas recorrem às normas técnicas, como é o caso da ISO 27701, explorada neste estudo, esta que, em conjunto com a LGPD, é capaz de balizar um sistema de conformidade apto a ser utilizado na Universidade de Rio Verde e, ainda, outras instituições desta natureza.

Palavras-chave: Dados pessoais. Segurança. Norma técnica.

ABSTRACT

Today's society, marked by the revolutions that have taken place in recent decades, has its relationships, at various levels, based on the exchange of information. This new dynamic, driven mainly by the emergence and expansion of the internet, has brought undeniable benefits. In view of this, the study aimed to address the issue of data protection, focusing on the University of Rio Verde, in order to assess the need to implement, within the institution, a data compliance program based on the LGPD and the ISO 27701. For this, a research was developed based on three stages, problem identification, documental organization of the research (theoretical framework) and its applicability, through the suggestion of implementing a data protection compliance program in light of the LGPD and ISO 27701 at the UniRV – University of Rio Verde. Due to the inconvenience generated by the sharing of personal data, the legislator, over the years, sought solutions, with the elaboration of different legal norms, until culminating with the creation of a specific law, Law n. 13,709, of August 14, 2018, called the General Data Protection Law or LGPD. Therefore, organizations face the challenge of adjusting their activities to comply with legislation and, at the same time, guarantee the security of the personal data to which they have access, which has also become a competitive differentiator in the market. This, however, requires changes and practical adjustments, which is why they resort to technical standards, such as ISO 27701, explored in this study, which, together with the LGPD, is capable of defining a compliance system capable of be used at the University of Rio Verde and other institutions of this nature.

Keywords: Personal data. Safety. Technical norm.

RESUMEN

La sociedad actual, marcada por las revoluciones acaecidas en las últimas décadas, tiene sus relaciones, en varios niveles, basadas en el intercambio de información. Esta nueva dinámica, impulsada principalmente por el surgimiento y expansión de internet, ha traído innegables beneficios. Frente a esto, el estudio tuvo como objetivo abordar el tema de la protección de datos, centrándose en la Universidad de Rio Verde, con el fin de evaluar la necesidad de implementar, dentro de la institución, un programa de cumplimiento de datos basado en la LGPD y la ISO 27701. Para ello, se desarrolló una investigación, basada en tres etapas, identificación del problema, organización documental de la investigación (marco teórico) y su aplicabilidad, mediante la sugerencia de implementar un programa de cumplimiento de protección de datos a la luz de la LGPD y la ISO 27701 en la Universidad. . Debido a los inconvenientes generados por el intercambio de datos personales, el legislador, a lo largo de los años, buscó soluciones, con la elaboración de diferentes normas legales, hasta culminar con la creación de una ley específica, la Ley n. 13.709, del 14 de agosto de 2018, denominada Ley General de Protección de Datos o LGPD. Por tanto, las organizaciones se enfrentan al reto de ajustar sus actividades para cumplir con la legislación y, al mismo tiempo, garantizar la seguridad de los datos personales a los que tienen acceso, lo que también se ha convertido en un diferenciador competitivo en el mercado. Esto, sin embargo, requiere cambios y ajustes prácticos, por lo que recurren a normas técnicas, como la ISO 27701, explorada en este estudio, que junto con la LGPD es capaz de definir un sistema de cumplimiento susceptible de ser utilizado en la Universidad. de Rio Verde y otras instituciones de esta naturaleza.

Palabras clave: Datos personales. La seguridad. Norma técnica.

LISTA DE FIGURAS

Figura 1. Linha do tempo até a criação a LGPD. 64
Figura 2. Garantias da LGPD. 73
Figura 3. Família ISO 27000. 80
Figura 4. Implementação ISO 27000. 82

LISTA DE QUADROS

Quadro 1. Comparativo entre ISO/IEC 27701:2019 e a LGPD 93
Quadro 2. Aspectos correlacionados entre a norma ISO 27701/2019 e a LGPD.....100

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CF	Constituição Federal
CIO	Chief Information Officer
ISO	*International Organization for Standardization*
GDPR	Regulamento Geral de Proteção de Dados
IEC	The International Electrotechnical Commission
IE	*Internet of Things*
IEs	Instituições de Ensino Superior
IoT	Internet das Coisas
ISO	International Organization for Standardization
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
LIBRAS	Língua Brasileira de Sinais
MEC	Ministério da Educação e Cultura
NBR	Normas Brasileiras de Regulação
NTIC	Novas Tecnologias da Informação e Comunicação
NT	Novas Tecnologias
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OGP	Open Government Partnership
ONU	Organização das Nações Unidas
PDCA	Plan-Do-Check-Act
PIMS	Privacy Information Management System
RGPD	Regulamento Geral de Proteção de Dados
RH	Recursos Humanos
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
SGSI	Sistema de Gestão de Segurança da Informação
SGPI	Sistema de Gestão da Privacidade da Informação
TD	Transformação Digital
TIC	Tecnologias de Informação e Comunicação
UniRV	Universidade de Rio Verde

SUMÁRIO

1 INTRODUÇÃO 13
1.1 Tema 20
1.2 Delimitação do tema 20
1.3 Formulação do problema 21
1.4 Hipótese 21
1.5 Objetivos 23
1.5.1 Objetivo geral 23
1.5.2 Objetivos específicos 23
1.6 Justificativa 23
2 FUNDAMENTAÇÃO TEÓRICA 27
2.1 Transformação Digital 27
2.2 Tecnologias Emergentes Da Quarta Revolução Industrial 37
2.3 Dados 44
2.4 Privacidade 45
2.5 Compliance aplicado à proteção de dados 49
2.5.1 Gestão de Compliance 51
2.6 Arcabouço legal 55
2.6.1 LGPD 65
2.6.1.1 Principais pontos da GDPR 66
2.6.1.2 Lei Geral de Proteção de Dados Brasileira 69
2.7 Normas 76
2.7.1 Normas de gestão 76
2.7.2 ISO 27000:2019 80
2.7.3 ISO 27701:2019 83
3 METODOLOGIA 86
3.1 Caso (UniRV) 87
4 COMPARATIVO ENTRE A ISO 27701: 2019 e a LGPG 90
4.1 Elementos da LGPD abordados pela ISO/IEC 27701:2019 93
4.2 Aspectos da norma ISO/IEC 27701:2019 que abrangem além dos requisitos da LGPD e que constam na legislação mas não faz parte da ISO 107

5 MODELO INTEGRADO DE CONFORMIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NA UNIRV 108
5.1 Planejamento 108
5.2 Execução 109
5.3 Controlar 110
5.4 Agir 111
6 CONSIDERAÇÕES FINAIS 112
7 CONCLUSÕES 115
REFERÊNCIAS 117

1 INTRODUÇÃO

O homem, desde os tempos primórdios, almeja a evolução, com vistas a ampliar a sua capacidade de se relacionar com o mundo, de modo que buscava desenvolver técnicas que o auxiliasse na execução das suas atividades cotidianas. No decorrer da história humana, a ocorrência das revoluções provocou mudanças profundas na maneira de os seres humanos criarem valor, a fim de atender as suas demandas.

A Primeira Revolução Industrial, na metade do século XVIII, ocorrida na Inglaterra, tem como destaque a invenção da máquina a vapor, com sua utilização na produção têxtil. Este processo trouxe grandes mudanças no aspecto econômico e na sociedade, com reflexos na expansão das cidades e no surgimento de novas profissões. Sob o enfoque das inovações tecnológicas, a Segunda Revolução Industrial se destaca pelo surgimento da metalúrgica, siderúrgica e da química, o que propiciou o desenvolvimento de novos métodos de produção.

Provocada pelo avanço tecnológico, a Terceira Revolução, em meados do século XX, com o advento da tecnologia da informação, eletrônica e das telecomunicações, implicou em desdobramentos sociais, econômicos e jurídicos.

A mudança no início do século XXI pautou-se na revolução digital, em que tecnologias digitais causaram rupturas à terceira revolução industrial, por meio do uso de diversas tecnologias, como Big Data, Inteligência Artificial, Internet das Coisas, (IoT), robótica, veículos autônomos, impressão em 3D, cada vez mais sofisticadas e integradas e, consequentemente, as quais transformaram a humanidade e a economia global e permitindo diferentes conexões e possibilidades ainda inimagináveis.

A ascensão no uso de softwares, sistemas de análises de dados cada vez mais interligados, automatização e o crescimento contínuo do acesso à internet, com inúmeras possibilidades para a oferta de produtos e serviços, possibilitou às empresas automatizar tarefas, reduzir custos de produção e alcançar novos mercados, de forma a construir um caminho de relacionamento com o cliente, independente de barreiras geográficas[1].

Segundo teóricos, a humanidade passa por uma transição de época e uma nova fase se inicia com a chamada Quarta Revolução Industrial. De acordo com Schwab e Davis[2], esta revolução transformará fundamentalmente o modo de vida das pessoas, os meios de

[1] DUNBRACK, Lynne, et al. **IOT and Digital Transformation:** a Tale of Four IndustrIEs. 2016. Disponível em: https://vods.dm.ux.sap.com/publicsectoruk/2016/pdfs/IoTandDigitalTransformation_ATalesofFourIndustrIEs.pdf. Acesso em: 18 mar. 2021.

[2] SCHWAB, Klaus; DAVIS Nicholas. **A Quarta Revolução Industrial.** Tradução de: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

comunicação, as relações sociais, trabalhos, negócios, com impacto em toda uma cadeia de valores, o que provocará mudanças de padrões e influenciará a maneira de gerar riquezas num país.

Neste sentido, Rogers[3] coloca que a Transformação Digital (TD) representa uma mudança de cultura organizacional, uma vez que as regras dos negócios mudaram, pois a difusão de novas tecnologias digitais transforma os modelos e processos de negócios.

Vê-se que o progresso tecnológico, além dos avanços econômicos, propiciou importantes mudanças sociais e culturais no decorrer das revoluções vividas na história da humanidade. Dentre as transformações geradas por estas novas tecnologias, se destaca o aumento da disponibilidade dos dados pessoais, pois o uso deles é essencial, tanto para as organizações, no desenvolvimento de suas atividades, quanto para as pessoas comuns, que estão cada vez mais conectadas.

Evidencia-se que a criação de regulamentações legais mais consistentes no campo da proteção de dados pessoais teve maior impulso a partir dos anos 90, diretamente relacionado com o desenvolvimento de novos modelos de negócios e impulsionado pelo progresso tecnológico e pela globalização.

Nota-se, neste contexto de transformação da sociedade e, consequentemente, de surgimento de normas legais que a rege, o crescimento acentuado da preocupação com a gestão de dados pessoais e os riscos que isto representa. Tal inquietação se justifica pelo fato de que a posse, uso e exploração inadequados destas informações tem potencial de fomentar inúmeras condutas subversivas, como manipulação virtual, espionagem, marketing direcionado, etc.

Ao partir do pressuposto de que o mundo econômico gira ao redor das necessidades das pessoas, os dados são, portanto, uma valiosa fonte de análise comportamental. A discussão acerca da proteção à privacidade e os limites da coleta dos dados pessoais por aplicativos, sistemas ou formulários físicos, bem como a maneira como estas informações são tratadas, necessita da devida atenção, para se chegar a uma solução para a problemática e, consequentemente, adoção de mecanismos de garantia à privacidade, proteção e segurança[4].

Em razão da relevância dos dados em uma sociedade contemporânea, a União Europeia dispõe de alguns mecanismos direcionados à proteção de dados pessoais como: a) Diretiva 2016/680: tem como ensejo a proteção de dados direcionados às autoridades policiais

[3] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.
[4] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

e judiciárias[5]; b) Regulamento 45/2001: estabelece regras destinadas aos órgãos ou agências da União, relacionadas com o tratamento de dados (EURO-LEX, 2020); c) Diretiva 2000/31: direcionada para o Comércio Eletrônico (EURO-LEX, 2020); e d) Diretiva 95/46/CE: garante a proteção das liberdades e dos direitos fundamentais, nomeadamente do direito à vida privada[6].

Em 2018 entrou em vigor o Regulamento Geral de Proteção de Dados – GDPR, com regras direcionadas à proteção de dados pessoais e à livre circulação destes. Devido às medidas e sanções em busca da proteção desses dados, o GDPR influenciou outros países a desenvolver legislações voltadas para a proteção de dados pessoais.

Neste sentido e, de certa forma, tardiamente, pois já havia legislação protetiva desta natureza na Argentina, pioneira no aspecto de proteção de dados, Chile, Colômbia, Peru e México, o legislador brasileiro elaborou a Lei nº. 13.709, em 14 de agosto de 2018, a qual entrou em vigor em agosto de 2020, cuja norma é denominada Lei Geral de Proteção de Dados Pessoais (LGPD). Passou-se, então, a assegurar, em numerosos aspectos, a proteção de dados pessoais da pessoa natural, ao explicitar no cerne do seu texto, os princípios a serem adotados por quem realiza qualquer tipo de tratamento destes dados[7].

A LGPD representa um avanço em direção à formação de um sistema de proteção de dados pessoais no Brasil, na busca por fortalecer a confiança das pessoas nos serviços existentes na sociedade da informação, assim como incentivar a inovação progressiva destes serviços. Porém, também é de suma importância a consolidação da tutela constitucional dos dados pessoais na legislação brasileira.

As determinações trazidas pelo legislador na Lei Geral de Proteção de Dados são aplicáveis a todas as operações de tratamento de dados, realizadas por um indivíduo ou por pessoa jurídica, de direito público ou privado, seja qual for o meio utilizado para tanto, o que pode ocorrer no país de sua sede ou na nação onde estejam localizados os dados.

Em consonância com as determinações elencadas pela nova legislação, faz-se necessário que as instituições implementem mecanismos para se adequar às suas exigências e colocar-se em conformidade com a Lei Geral de Proteção de Dados Pessoais.

---

[5] EUR-LEX. Disponível em: https://eurlex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN. Acesso em: 24 jan. 2021.

[6] EUR-LEX. Disponível em: https://eurlex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN. Acesso em: 24 jan. 2021.

[7] WADE, Michael. **Digital Business Transformation**. IMD and Cisco, Working Paper, p. 1-16, 2017.

A Lei Geral de Proteção de Dados Pessoais aborda a necessária proteção de dados de pessoa natural, principalmente diante da vasta discussão que se volta à fragilidade das informações armazenadas nos diferentes bancos de dados, em função de transações realizadas com ou sem autorização dos titulares dos dados.

A instrumentalização de uma norma que regulamenta o tratamento de dados realizado por uma pessoa jurídica tende a proteger a pessoa natural de qualquer tipo de arbitrariedade, decorrente de comportamentos ilegais. Como fundamento da sua incidência tem-se o respeito à privacidade; a autodeterminação informativa; a inviolabilidade da intimidade, da honra e da imagem; os direitos humanos; o livre desenvolvimento da personalidade; a dignidade e o exercício da cidadania pelas pessoas naturais, entre outros (art. 2º).

Diante da relevância do tema, intensas têm sido as buscas por ferramentas sólidas e seguras, que atendam à proteção dos dados pessoais, a exemplo do que tem se observado com a edição da LGPD.

Em que pese ser inegável a necessidade de respeitar as determinações trazidas pela nova legislação, também é inconteste que isto requer a adoção de alguns mecanismos, em especial aqueles que capazes de levar as empresas e instituições a desenvolver a conformidade com o art. 44 e seguintes da Lei Geral de Proteção de Dados. Ressalta-se que o mencionado artigo se refere ao caráter irregular do tratamento de dados pessoais, que se configura quando não é observada a legislação ou não há segurança para o titular dos dados, além de definir regras relacionadas ao modo de tratar, o resultado, os riscos deste tratamento e, ainda, as técnicas utilizadas.

Enfim, com vistas a proteger os direitos fundamentais de liberdade, de privacidade e a livre formação da personalidade de cada indivíduo, a lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica, de direito público ou privado, e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

Os agentes de tratamento, ou qualquer outra pessoa que participe das fases do ciclo de vida dele, são obrigados a garantir a segurança da informação, a fim de proteger os dados pessoais, conforme disposto no art. 46, o qual retrata as medidas de segurança, técnicas e administrativas a serem observadas desde a fase de concepção do produto ou do serviço até a sua execução, no que tange à proteção de dados pessoais.

Para que haja um gerenciamento de segurança dos dados, deve-se observar condutas, recomendações, princípios e práticas que visem a gerir riscos e, com isto, assegurar maior segurança e resiliência. Na era digital, as notícias de vazamento de dados são cada vez mais

frequentes. Diante desse cenário, a International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) lançaram um novo padrão de privacidade, o que se tornaria ferramenta de auxílio para as organizações a cumprir leis e estruturas de privacidade internacionais[8].

Com ênfase nesta problemática, a *International Organization for Standardization* (ISO) apresenta normas que têm como objetivo estabelecer, implementar, manter e melhorar as empresas, ou seja, garantir a segurança das informações. As ISOs são normas internacionais, aptas a serem implementadas em qualquer tipo de organização, independentemente do porte ou espécie (pública ou privado)[9].

A norma ISO 27701/2019 especifica requisitos voltados para a implementação do Sistema de Gestão da Privacidade da Informação (SGPI), assim como fornece diretrizes para as funções de controlador e operador de dados pessoais. A ISO 27701 é uma extensão dos demais dispositivos e fornece orientações adicionais para a proteção e privacidade dos dados, potencialmente afetado pela sua coleta e tratamento[10].

Neste contexto, nota-se que as IEs (Instituições de Ensino) enfrentam um cenário disruptivo, moldado pelas tecnologias digitais, em que surgem novos modelos de negócios, o que altera o formato de sua evolução no decorrer do tempo, vincula as relações com os clientes, tanto internos, quanto externos, aumenta o comprometimento deles e fortalece sua experiência na organização[11].

A fusão de tecnologias exponenciais, propiciadas pela quarta revolução industrial, tem provocado uma transformação na sociedade e impactando diversos segmentos, inclusive a seara educacional. Diante destee cenário, faz-se necessário que as IES repensem seus processos, uma vez que esta área é influenciada pelas tecnologias emergentes, no tocante à mobilidade e conectividade, como observado neste momento de pandemia.

Toda esta transformação culminou na demanda por novas habilidades profissionais, no objetivo de atender a um novo mercado de trabalho, e desenhou um novo perfil de egresso.

---

[8] SPHIPMAN, Alan; WATKINS, Steve. ISSO/IEC 27701:2019 Na introduction to privacy information management. Cambridgeshire CB7 4EA Reino Unido, 2020.

[9] ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001:** 2013. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2006.

[10] PONCE, Silvana. **Panorama Geral ISO 27001:2013/ISO 27701:2020:** Sistema de Gestão da Segurança e Informação/Sistema de Gestão de Informação Privada. QMS Brasil. Disponível em: https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf. Acesso em: 12 ago. 2021.

[11] BENAVIDES, Lina Maria Castro et. al. Digital transformation in higher education institutions: a systematic literature review. **Sensors,** v.20, n. 11, 2020. Disponível em: https://www.mdpi.com/1424-8220/20/11/3291. Acesso em: 05 mar. 2021.

Nesta direção, emerge a possibilidade das IES inovarem por meio de uma visão abrangente, em questões sistêmicas e estruturais, numa nova perspectiva do seu propósito institucional, com práticas que visem a aprimorar as ações acadêmicas e administrativas[12].

Pode-se considerar a inovação como um processo que busca identificar oportunidades ou problemas, a serem solucionados a partir de uma invenção ou criação de algo novo. Para tanto, pode-se adotar técnicas, métodos, produtos, serviços e/ou tecnologias que rompam conceitos anteriormente consolidados[13]. Isto implica, segundo Benavides et al.[14], na necessidade de as universidades implementarem estratégias digitais para o enfrentamento das transformações provocadas pelos recursos tecnológicos.

Portanto, é relevante ter uma visão panorâmica da transformação digital nas Instituições de Ensino Superior, a fim de determinar as dimensões deste processo, num mundo cada vez mais tecnológico e globalizado. Frente a isto, implementar um sistema de gestão da segurança da informação tornou-se essencial para as organizações, tendo em vista a dimensão dos dados na atualidade, por conta da necessidade de proteger tais dados.

Nesta conjuntura, a ISO/IEC 27701 é um padrão de sistema de gerenciamento reconhecido internacionalmente, desenvolvida com o objetivo de auxiliar as organizações a estabelecer sistemas que visem a apoiar a conformidade com o GDPR (Regulamento Geral de Proteção de Dados), além de possuir um contexto amplo, o qual permite a aplicação numa diversidade de segmentos de negócios[15].

A lei brasileira de proteção de dados teve como parâmetro o Regulamento europeu e os controles da ISO/IEC 27701 oferecem dispositivos aptos a contribuírem para as organizações brasileiras implementarem mecanismos de conformidade com a LGPD.

A escolha por desenvolver a pesquisa em uma Instituição de Ensino Superior (IES) foi motivada pela necessidade de explorar o campo da transformação digital no contexto do ensino superior, num cenário emergente, cada vez mais competitivo e marcado por novas relações heterogêneas e complexas entre os atores, em que se nota na seara educacional o

---

[12] CHRISTENSEN; Clayton M.; EYRING, Henry J. A universidade inovadora: mudando o DNA do Ensino Superior de fora para dentro. Porto Alegre: Bookman, 2014.

[13] SEMESP. Excelência a Serviço do Ensino Superior. **Guia framework de inovação para IEs**. 2º Seminário o futuro do Ensino Superior. São Paulo. 2018. Disponível em: https://www.semesp.org.br/wpcontent/uploads/2018/08/E-book-Guia-Framework-inova%C3%A7%C3%A3o-1-1.pdf. Acesso em: 28 mar. 2021.

[14] BENAVIDES, Lina Maria Castro et. al. Digital transformation in higher education institutions: a systematic literature review. **Sensors,** v.20, n. 11, 2020. Disponível em: https://www.mdpi.com/1424-8220/20/11/3291. Acesso em: 05 mar. 2021.

[15] ISO/IEC 27701 DNV AS. **All rights reserved.Privacy Information management system**. Disponível em: https://www.dnv.com/services/iso-iec-27701-privacy-information-management-system-159186. Acesso em: 05 jan. 2021.

predomínio da utilização de tecnologias revolucionarias. Ressalta-se que, neste ambiente cada vez mais tecnológica, surge a necessidade de estudar suas implicações, bem como identificar as potencialidades e desafios da transformação digital para Instituições de Ensino Superior no Brasil.

As mudanças ocasionadas pelos avanços metodológicos de ensino e aprendizagem, assim como a concorrência neste mercado, conduzem à necessidade de fortalecer uma nova visão de negócio nas IES. Sublinha-se que a utilização das novas tecnologias favorece esta dinâmica e agrega valor ao seu domínio, além de determinar suas características distintivas no mercado.

A narrativa acima exposta, aliada à necessidade de as organizações estarem em conformidade com a LGPD, justifica os investimentos por parte das organizações, na busca por implementar ferramentas que venham a mitigar os riscos de vazamento, uso incorreto e vendas de dados pessoais, além de outros problemas encontrados nesta seara.

Isto fez com que a proteção de dados se tornasse elemento de vanguarda na segurança da informação, em virtude da expansão tecnológica ocorrida a nível mundial, como resultado dos desdobramentos da globalização, o que aumentou a relevância da informação. Esta conectividade, entretanto, gerou alguns problemas, relacionados às violações de dados organizacionais, IoT, redes sociais e a monetização dos dados pessoais[16,17].

Ressalta que o tema de proteção de dados é assunto abordado desde a década de 70, mas, foi a promulgação do *General Data Protection Regulation - GDPR*, em vigor desde 2018, o qual serviu de inspiração para vários países implementarem mecanismos de regulação e proteção de dados pessoais, inclusive no Brasil[18].

Com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais brasileira, tornou-se obrigatório às organizações, independentemente de sua natureza (pública ou privada), tamanho ou segmento, se adequar às exigências da lei, conforme exposto no artigo 1º da norma em questão. A Lei 13.709/2018 tem como objetivo a proteção de direitos

---

[16] MÄKINEN, Jenna. Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things. **Information & Communications Technology Law,** v. 24, n. 3, p. 262-277, 2015. Disponível em: https://www.researchgate.net/publication/282941950_Data_quality_sensitive_data_and_joint_controllership_as_examples_of_grey_areas_in_the_existing_data_protection_framework_for_the_Internet_of_Things. Acesso em: 19 abr. 2021.

[17] NURSE, Jason R. C.; CREESE, Sadie; ROURE, David de. Security Risk Assessment in Internet of Things Systems. **IT Professional,** v. 19, n. 5, 2017. Disponível em: https://ieeexplore.ieee.org/document/8057728. Acesso em: 19 abr. 2021.

[18] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. Lei Geral de Proteção de Dados Pessoais: comentada artigo por artigo. Salvador: JusPODIVM, 2020.

fundamentais, como a privacidade, a intimidade, a honra, o direito à imagem e à dignidade da pessoa humana, garantidos na Constituição Federal[19,20].

Insta salientar que a adequação e conformidade da UniRV com ditames da Lei 13,709/18 representará um grande diferencial competitivo, capaz de fortalecer a confiança depositada pelo titular na organização e agregar valor, ao melhorar a reputação e a imagem da instituição perante a sociedade, inclusive a nível mundial, haja vista que a Universidade trabalha com parceiros nacionais e internacionais.

Neste cenário, é de salutar importância atentar-se para a relevância de se ofertar processos e orientações que visem à proteção de dados pessoais, num sistema de gestão que envolva melhoria contínua, pois a universidade atua na formação acadêmica de discentes, docentes e servidores, com o compromisso de produzir, sistematizar e socializar conhecimentos, por meio de programas de ensino, pesquisa, extensão e serviços, em especial na formação de profissionais capazes de interagir de forma crítica, criativa, propositiva - política, técnica e social[21].

Diante de todo o exposto alhures, a pesquisa a ser desenvolvida tem como escopo primordial realizar um estudo prático, com propositura da aplicabilidade dos requisitos da ISO/IEC 27701:2019, com vistas à governança dos dados pessoais geridos pela UniRV – Universidade de Rio Verde por meio de um sistema de gestão que promova melhoria contínua através de processos orientados à proteção dos dados que culmine na conformidade da Lei Geral de Proteção de Dados Pessoais.

1.1 Tema

A proteção de dados pessoais à luz da Lei geral de proteção de dados (LGPD).

1.2 Delimitação do tema

Esta dissertação de mestrado se propõe a examinar os elementos a serem inseridos num projeto de conformidade que contemple as práticas e procedimentos mais adequados, nos

---

[19] PINHEIRO, Patrícia Peck. **LGPD:** os prós e contras de prorrogar a Lei para 2022. Disponível em: https://www.cryptoid.com.br/identidade-digital-destaques/lgpd-os-pros-e-contras-de-prorrogar-a-lei-para-2022/. Acesso em: 18 set. 2021.

[20] TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. Salvador: JusPODIVM, 2020.

[21] UNIRV. Universidade de Rio Verde. **Institucional**. Disponível em: http://www.unirv.edu.br/paginas.php?id=12. Acesso em: 18 mar. 2021.

termos da ISO 27701, com o intuito de implementar um *compliance* da LGPD, apto a mitigar os riscos envolvidos no tratamento, coleta e descarte dos dados pessoais e, com isto, viabilizar a adequação da Universidade de Rio Verde à Lei Geral de Proteção de Dados Pessoais.

1.3 Formulação do problema

Atualmente a informação se encontra presente nas diversas estruturas da sociedade, do trabalho ao lazer, no ambiente negocial, na competitividade ou na busca por destaque no mercado. Diante deste contexto, os dados se tornaram um ativo relevante para as organizações, inclusive para as instituições de ensino superior, que são ambientes voltados para a produção de conteúdo, com o objetivo de disseminar o conhecimento. Assim, surge a preocupação jurídica com a proteção destes dados, o que culminou com a edição de normas e técnicas voltadas para a proteção contra abusos no uso dos mesmos.

Em 2016 a União Europeia emitiu o Regulamento Geral sobre a Proteção de Dados, o que contribui de certa forma para o Brasil criar uma lei protetiva e se equiparar a outros países que já possuem legislações específicas a este respeito, o que gerou alterações na forma como as organizações lidam com os dados. Ao considerar este cenário, pode-se estruturar o problema da presente pesquisa da seguinte forma: sob quais condições a ISO/IEC 27701/2013 pode ser usada como ferramenta de controle e garantia de medidas técnicas e administrativas de proteção de dados, a fim de que UniRV – Universidade de Rio Verde se adequem à Lei Geral de Proteção de Dados Pessoais?

1.4 Hipótese

A Lei Geral de Proteção de Dados traz um aparato legal que representa mudanças de paradigmas, no que diz respeito à gestão de informações pessoais. A ISO 27701 é um norma de padrão internacional de certificação, que apresenta requisitos práticos a serem observados pelas instituições no intuito de estruturar um Sistema de Gestão de Privacidade da Informação (SGPI) eficaz[22].

No cenário atual, os dados são considerados como ativos particularmente valioso para as organizações, tanto para a gestão estratégica, quanto para a concorrência ou melhoria na

[22] SPHIPMAN, Alan; WATKINS, Steve. ISSO/IEC 27701:2019 Na introduction to privacy information management. Cambridgeshire CB7 4EA Reino Unido, 2020.

capacidade de tomar decisão, de modo que avoca um papel central estruturante de (re)organização da sociedade[23].

Sublinha-se que ações que asseguram e aprimoram normas e técnicas de políticas de segurança fortalece os princípios da informação, quais sejam: confidencialidade, integridade e disponibilidade, os quais se tornam essenciais para a continuidade num mercado cada vez mais competitivo, onde a tecnologia rompe fronteiras geográficas[24].

A iniciativa de realização deste estudo pauta-se na constatação da necessidade de se discutir sobre a aplicabilidade da LGPD nas IES, bem como a sua relevância, tendo em vista que a lei engloba todos os tipos e portes de empresas. É inconteste a necessidade de que as Instituições de Ensino Superior busquem ferramentas e estratégias para alcançar o *compliance* com a LGPD.

Neste contexto, a ISO 27701 possibilita a implantação de políticas de proteção da informação, a fim de proteger os dados, com práticas de processo de escalonamento de riscos, de modo a incorporar valoração aos ativos da organização, orientar quanto à análise e identificação de riscos e a implantação de controles para minimizá-los, bem como alcançar a conformidade com as exigências impostas pela LGPD[25].

Esta norma compreende requisitos que norteiam a avaliação e tratamento de riscos da informação, direcionada às necessidades da organização, em que pese a possibilidade de aplicação dela a qualquer tamanho ou natureza de empresa.

Com a vigência da Lei Geral de Proteção de Dados Pessoais no Brasil, as organizações estão obrigadas a implementar ferramentas que minimizem os riscos, a fim de evitar danos e prejuízos aos titulares dos dados. Com esta visão, verifica-se que a norma ISO 27701 fornece mecanismos de controle e diretrizes, com os quais a empresa pode alcançar a proteção da informação e, com isto, implementar um *compliance* da LGPD nas Instituições de Ensino Superior.

---

[23] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

[24] ROCHA, Camila et al. Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará,** v. 2, n. 3, p. 78-97, ago. 2019. Disponível em: http://www.revistasfap.com/ojs3/index.php/tic/article/view/285. Acesso em: 10 mar. 2021.

[25] ISO/IEC 27701, 2020. **O que é a ISO/IEC 27701/2019.** Disponível em: https://bedu.tech/wp-content/uploads/2020/10/iso-iec-27701.pdf. Acesso em: 14 jan. 2021.

1.5 Objetivos

1.5.1 Objetivo geral

Avaliar os elementos a serem abordados num projeto de conformidade de gestão de dados no âmbito da Universidade de Rio Verde, a partir das práticas da ISO 27701 para implementação de um programa *compliance* de proteção de dados à luz da LGPD.

1.5.2 Objetivos específicos

a) Discorrer sobre o espelhamento, similaridades e diferenças entre a ISO 27701 e a LGPD;

b) Elaborar uma proposta de gestão e proteção de dados baseada na ISO 27701 e em outras práticas;

c) Apontar os elementos que devem ser abordados no programa de *compliance* de gestão de dados na Universidade de Rio Verde, a fim de estar em conformidade com a legislação.

1.6 Justificativa

O presente estudo merece destaque no contexto das Instituições de Ensino Superior, tendo em vista o arsenal regulatório vigente no país e que aborda a questão da proteção de dados em especial a Lei Geral de Proteção de Dados Pessoais, Lei 13.709 de 2018, assim como o impacto para as organizações, independente da natureza ou porte.

A LGPD traz uma série de implicações, a exemplo de multas, sanções e exigências de implantação de boas práticas, com o objetivo de criar uma governança corporativa de proteção de dados pessoais. A Lei aporta os fundamentos da proteção de direitos e garantias da pessoa natural, consubstanciado no respeito à privacidade, na autodeterminação informativa, na inviolabilidade da intimidade, no fomento ao desenvolvimento econômico e tecnológico e, ainda, na livre iniciativa e respeito aos direitos humanos, entre outros[26].

[26] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 03 jan. 2021.

O direito à informação e o direito à proteção de dados pessoais são ambos direitos fundamentais previstos na Constituição Federal de 1988 e regulamentados por leis infraconstitucionais, respectivamente, Lei de Acesso à Informação (LAI – Lei nº 12.527/2011) e pela Lei Geral de Proteção de Dados

À Lei de Informação surgiu como resultado de um extenso processo de conquista de tal direito no território brasileiro. O ponto mais aclamado da Lei 12.527/2011 é, de fato, as restrições de acesso à informação governamental, nas situações em que o acesso a determinado documento implica em comprometimento da soberania, integridade do território nacional ou que afete as relações internacionais do Brasil (BORGES, 2022).

De fato, as tecnologias da informação trouxeram um novo paradigma para a relação existente entre a Administração Pública e os indivíduos, em especial no que pertine a conservação das informações e sua disponibilização, no intuito de se evitar ilícitos relacionados à utilização de dados de terceiros (OLIVEIRA, 2020).

Diante desta nova realidade, bem como da ineficiência da Lei da Informação para solucionar os problemas relacionados ao vazamento de informações e a prática de ilícitos decorrentes disto, a Lei Geral de Proteção de Dados surgiu como um reforço à busca por proteção dos direitos dos titulares de dados. Este novo regramento trouxe um arcabouço vasto de exigências técnicas e organizacionais direcionadas às entidades detentoras de dados pessoais (OLIVEIRA, 2020).

Num contexto social em que praticamente todas as atividades, econômicas ou não, se pautam em modelos que utilizam os dados pessoais para as mais diversas finalidades, estes que se tornaram insumo essencial para a tomada de decisões estratégicas, é de fundamental importância entender melhor o mercado, no intuito de continuar a fazer parte dele, se aproximar do cliente/consumidor e agregar valor à organização.

As diversas tecnologias existentes desenham um novo cenário, com a monetização dos dados. No âmbito das Instituições de Ensino Superior, é possível valer-se deste componente para a implementação de novos modelos de negócios e destacar-se como *player* no mercado educacional, de modo a promover um processo formativo eficiente, com um alcance diversificado de alunos. Isto favorece à instituição de ensino o rompimento de fronteiras, que culmina na redução dos obstáculos relacionados ao tempo e espaço. Assim, contribui para a geração de conhecimento e oportunidade de aprendizagem, que conduzem ao crescimento do país.

Entretanto, diante deste cenário, que o uso dos recursos tecnológicos propiciou, surgem novas demandas jurídicas, com o condão de resguardar direitos novos ou já existentes.

Diante de todas estas transformações, vale destacar a legislação vigente no país, no que concerne à proteção de dados pessoais, a Lei Geral de Proteção de Dados, diploma legal que impacta diretamente a vida das pessoas e das organizações, com destaque para as IES.

Ademais, sua adequação e conformidade com a Lei Geral de Proteção de Dados Pessoais, inclusive nos meios digitais trará credibilidade e, também, importará num grande diferencial competitivo, de modo a fortalecer a confiança depositada pelo titular na instituição e agregar valor à reputação e à imagem da Universidade perante a sociedade.

A Constituição Federal de 1988 traz como mandamentos os direitos à liberdade e à privacidade, de modo a erigir eles à condição de direitos fundamentais. Tal feito tem como base legal a Emenda Constitucional 115/2022 (LXXIX).

Com o advento da Emenda Constitucional 115, a proteção de dados pessoais foi elevada a um novo status, qual seja o de Direito Fundamental. A EC em questão acresceu ao texto constitucional normas que têm relação como direito fundamental à Proteção de Dados Pessoais, além de determinar a competência exclusiva da União para legislação sobre esta temática, assim como atuar na organização e fiscalização da proteção e tratamento de tais dados (SOUZA; ACHA, 2022).

Neste sentido, a fim de proteger tais direitos, promulgou-se a Lei 13.709/2018, conhecida como Lei Geral de Proteção dos Dados Pessoais, na qual o legislador trata, de forma mais minuciosa e rigorosa, tratou da questão da proteção e segurança de dados pessoais.

Demais disto, tem-se a norma ISO 27701, passível de aplicação em todos os tipos de organizações, independente do segmento, tamanho ou natureza, as quais podem ser: empreendimentos, comerciais, agências governamentais, dentre outras. Esta normatização oferece estrutura para auxiliar as organizações e demonstrar conformidade com diversos arcabouços legais de proteção e privacidade de dados pessoais, num cenário regulatório marcado por mudanças globais[27].

Milicevic e Goeken[28] trazem os padrões de segurança da informação como formato de soluções para a ampla margem de riscos, por meio de orientações de segurança da informação, com destaque para o padrão ISO 27701, como uma estrutura internacional na implementação de gestão e privacidade dos dados.

---

[27] ISO/IEC 27701, 2020. **O que é a ISO/IEC 27701/2019.** Disponível em: https://bedu.tech/wp-content/uploads/2020/10/iso-iec-27701.pdf. Acesso em: 14 jan. 2021.

[28] MILICEVIC, Daniel; GOEKEN, Matthias. **Ontology-Based Evaluation of ISO 27001.** Conference on e-Business, e-Services and e-Society - I3E 2010: Software Services for e-Worldpp 93-102. Disponível em: https://link.springer.com/content/pdf/10.1007/978-3-642-16283-1_13.pdf . Acesso em: 10 abr. 2021.

Assim, a implementação do *compliance* de conformidade, alinhado às exigências da LGPD, por meio da adoção das práticas abordadas na ISO 27701, gerará evidências documentadas correlatas ao tratamento dos dados pessoais e fornecerá credibilidade para a instituição, ao adotar mecanismos de um SGPI que trará proteção aos dados pessoais. Sublinha-se que esta prática tem se destacado tanto no contexto nacional, quanto internacionalmente, por gerar um ambiente propício para as organizações realizar o processamento das informações de forma mutualmente relevante.

Acredita-se que os resultados do presente estudo servirão de apoio para as instituições de ensino superior na busca por melhorias e compreensão da dinâmica, termos e conceitos da nova legislação. Com este desiderato, ao final do presente estudo propor-se-á um projeto de programa de *compliance*, baseada nos requisitos da ISO 27701 como forma de alcançar a conformidade com a Lei de Proteção de Dados, por meio da implementação das práticas elencadas na mencionada norma.

Por fim, salienta-se que o tema desta pesquisa está em consonância com as áreas investigadas na Linha de Pesquisa “Direito da Empresa e Regulação”, do Mestrado Profissional em Direito da Empresa e dos Negócios da Unisinos, além de servir com um delineador para a Universidade de Rio Verde adequar-se às exigências da Lei 13709/18.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo aborda um conjunto de temas relevantes para a elaboração da pesquisa, com vistas a delinear o conteúdo teórico a embasar o estudo ora proposto.

2.1 Transformação Digital

A problemática da transformação digital é muito discutida atualmente. Entretanto, a concepção de produtos, processos, negócios remontam aos anos 90 e 2000. Com o surgimento dos dispositivos inteligentes e plataformas de mídia social, no período de 2000 a 2015, ocorreu uma mudança no formato de relacionamento das organizações com seus clientes e, via de consequência, alterou os modelos de negócios[29].

A transformação digital abrange todos os segmentos da sociedade, mas também expande novas possibilidades de *networking* e permite a cooperação entre diferentes atores, os quais, por exemplo, trocam dados e, assim, iniciam processos e negócios[30].

Neste sentido, Sampaio[31] ressalta que a tecnologia não ocupa lugar apenas como ferramenta de gestão estratégia nas tomadas de decisões empresariais, mas se destaca, também, como força propulsora de competitividade, ou seja, um diferencial que explora a capacidade de reinventar novos modelos de negócios e capaz de agregar valor à indústria.

Toda esta conjuntura engloba modificações na gestão estratégica dos negócios e altera os pilares das atividades operacionais do mercado, o que afeta produtos, processos, estruturas e conceitos de gestão, do que se extrai o conceito de transformação digital[32].

Para Rogers[33], "A transformação digital não tem a ver com tecnologia – tem a ver com estratégia e novas maneiras de pensar. Transformar-se para a era digital exige que o negócio atualize sua mentalidade estratégica, muito mais que sua infraestrutura de TI".

---

[29] AURIGA. **Digital Transformation:** History, Present, and Future Trends. Retrieved June 15, 2017. Disponível em: https://auriga.com/blog/digital-transformation-history-presentand-future-trends. Acesso em: 21 mar. 2021.

[30] SCHALLMO, Daniel; WILLIAMS, Christopher; LUKE, Boardman. Digital Transformation of Business Models — Best Practice, Enablers, and Roadmap. **Ingernational Journal of Innovation Management,** v. 21, n. 1, nov. 2017. Disponível em: https://www.researchgate.net/publication/321394754_DIGITAL_TRANSFORMATION_OF_BUSINESS_MODELS_-_BEST_PRACTICE_ENABLERS_AND_ROADMAP. Acesso em: 18 mar. 2022.

[31] SAMPAIO, Rafael de. **Vantagem digital:** um guia prático para a transformação digital. Editora Alta Books, 2018. *e-book.*

[32] HESS, Thomas et al. Options for Formulating a Digital Transformation Strategy. **MIS Quarterly Executive,** v. 15, n. 2, p. 123-125, 2019. Disponível em: https://doi.org/10.1108/10878571211209314. Acesso em: 01 fev. 2021.

[33] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017. p. 12.

Na visão de Bouée, Schaible[34] e PwC[35], a transformação digital consiste no envolvimento de todos os setores da economia com seus agentes, numa nova realidade digital. Diante disto, é de fundamental importância nos diversos ramos de negócios a implantação de tecnologias baseadas na internet, de forma a transformar a vida humana em seus diferentes contextos.

Nota-se que "A transformação digital é um processo que visa melhorar uma organização, provocando alterações significativas em suas características por meio de combinações de tecnologias de informação, computação, comunicação e conectividade"[36].

Assim, o aumento na produção e no uso de dados apoiados em tecnologias digitais cada vez mais sofisticadas e especializadas proporcionou um novo formato de produzir conhecimento, apoiado em algoritmos e modelagens computacionais. Neste cenário, dados ganham valor e importância, por meio de mobilizações diversas, que envolvem negociações e interesses sociais, políticos e econômicos[37].

Os dados se manifestam com toda sua potencialidade na transformação digital, com uma dimensão que provoca a necessidade do gerenciamento das informações para implementar estratégias para o negócio.

A pandemia provocada pelo coronavírus (SARS-CoV-2), causador da Covid-19, identificado pela primeira vez em dezembro de 2019, em Wuhan, na China, provocou grande preocupação, frente à uma doença que se espalhou muito rápido e provocou inúmeras mortes a nível mundial. De acordo com a Organização Mundial da Saúde (OMS), em 18 de abril de 2021 a doença já alcançou 223 países, áreas ou territórios e chegou a 140.322.903 casos confirmados e 3.003.794 de mortes em todo o mundo[38].

A revolução digital transformou os diversos ambientes, de forma contínua e simultânea, de forma a propiciar alterações no processo produtivo e influenciar a relação empresa/consumidor, assim como levar a mudanças na gestão de informações. Em tempos de

---

[34] BOUEÉ, Charles-Edouard; SCHAIBLE, Stefan. **Die Digitale Transformation der Industrie.** Studie: Roland Berger und BDI. 2015. Disponível em: https://bdi.eu/media/presse/publikationen/information-und-telekommunikation/Digitale_Transformation.pdf. Acesso em: 12 maio 2022.

[35] PwC. **Transformação Digital - der gr o € ßte Wandel seit der Industriellen Revolution**. Frankfurt: PricewaterhouseCoopers. 2013.

[36] VIAL, Gregory. Understanding digital transformation: a review and a research agenda. **The Journal of Strategic Information Systems,** v. 28, n. 2, p. 118-144, 2019. p. 118.

[37] ALMEIDA, Bethania de Araujo et. al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva,** v. 25, p. 2487-2492, 2020. Disponível em: https://www.scielo.br/j/csc/a/T6rwdhnTNzp5vYr84w9xthB/?format=pdf&lang=pt. Acesso em: 10 mar. 2021.

[38] WHO. World Health Organization. **Coronavirus disease (COVID-19**). Disponível em: https://www.who.int/emergencIEs/diseases/novel-coronavirus-2019?gclid=Cj0KCQjwse-DBhC7ARIsAI8YcWIoKU2JK-ceoeVnZcZYV6NPO86b4XD2VZLBkQwHET_X8dNSs5mvekMaAgH5EALw_wcB. Acesso em: 18 abr. 2021.

pandemia como o atual, os dados pessoais são elementos essenciais no desenvolvimento de vacinas e rastreamento de sintomas, de forma a apoia estratégias de acompanhamento, entre outros. Esta nova realidade é crucial na busca de soluções para o momento vivido em todo o mundo[39].

Doneda[40] ressalta que, ao mesmo tempo, os governos devem implementar legislações aptas a dar proteção aos titulares dos dados, com ênfase nas liberdades individuais e coletivas, diante dos riscos inerentes ao uso destes dados para fins diferentes dos interesses de combate ao Covid-19.

Todos estes fatores influenciam a sociedade na chamada Quarta Revolução Industrial, o que acarreta desafios, oriundos das novas demandas de modelos de governança de dados e de tecnologias, correlacionando a convergência de tecnologias digitais, físicas e biológicas, em que se amplificam e constroem outras tecnologias[41].

Tecnologias como robótica, Internet das Coisas, Inteligência Artificial, nanotecnologia, veículos autônomos, impressão em 3D, nanotecnologia, Big Data, proporcionam um desenvolvimento exponencial de oportunidades nos mais variados campos: econômico, social, pesquisas científicas, novas modalidades de mercados e rompem fronteiras na vida das pessoas, das empresas, assim com afeta o papel do Estado como regulador de novas demandas e necessidades. Vale destacar que todas estas mudanças propiciadas pelas tecnologias digitais também contribuem para a formação do pensamento da sociedade contemporânea.

Enfim, a conectividade digital permeia todos os aspectos da vida humana, desde a forma que as pessoas interagem até o cenário econômico global, de modo que influencia na tomada de decisões, desde a forma de consumo à política, ou seja, conduzem a forma como as pessoas compreendem e criam fontes de valor, o que impacto no corpo, redefine o comércio global e, enfim, pode influenciar nos regimes políticos nos diversos quadrantes do planeta.

O Fórum Econômico Mundial realizou uma pesquisa denominada "*Deep Shift – Technology Tipping Points and Societal Impact*", a qual identificou 21 pontos de inflexão, oriundos das megatendências disruptivas, ou seja, momento em que algumas mudanças tecnológicas alcançarão a sociedade, num futuro hiperconectado e digital. O estudo relata seis

---

[39] ALMEIDA, Bethania de Araujo et. al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva,** v. 25, p. 2487-2492, 2020. Disponível em: https://www.scielo.br/j/csc/a/T6rwdhnTNzp5vYr84w9xthB/?format=pdf&lang=pt. Acesso em: 10 mar. 2021.

[40] DONEDA, Danilo. A proteção de dados em tempos de coronavírus. Redes Sociais como canais de distribuição de conteúdo. **Jota Info,** 2020. Disponível em https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 01 abr. 2021.

[41] SCHWAB, Klaus; DAVIS Nicholas; MIRANDA, Daniel Moreira. **Aplicando a Quarta Revolução Industrial.** Tradução de: Daniel Moreira Miranda. São Paulo: Edipro, 2018.

megatendências de *softwares* e serviços, com abrangência das pessoas e a internet, Internet das Coisas, Inteligência artificial, Big Data, Economia da partilha e a confiança distribuída e o *blockchain* que molda a sociedade e as oportunidades e riscos associados[42].

Nesta linha de pensamento, a pesquisa traz a necessidade de ajustes nos diversos pilares individuais, organizacionais, governamentais e sociais, em que todos sentirão os impactos da implementação dessas tecnologias, além de destacar que há um ambiente ainda obscuro, mas com um vislumbre de possibilidades nos próximos anos[43]. Ainda nesta perspectiva, o estudo demostra outras áreas vulneráveis a serem consideradas como proteção, privacidade e segurança[44].

Schwab[45], em uma outra reflexão, considera que a formatação das tecnologias emergentes ocorre no momento atual. Assim, faz-se necessária a contribuição dos diversos envolvidos na sociedade civil, líderes empresárias, universidades, governos, entre tantos outros, estes que contribuirão com suas opiniões no desenvolvimento das tecnologias revolucionárias, uma vez que estas mudanças acontecem numa velocidade exponencial e não linear, de forma ampla e profunda, com impactos e não linear, ou seja, em um formato transversal, nas diversas esperas da sociedade, o que culmina com a busca de mecanismos que promovam o bem comum.

Enquanto a Inteligência Artificial e o Big Data, robótica, progridem em uma velocidade tão rápida, de forma a criar a chamada computação ambiental, em que dispositivos tomarão notas e responderão às questões dos pacientes, outros dispositivos tornaram a rotina das pessoas, ao ouvir e antecipar as necessidades humanas. A impressão 3D permite a impressão de produtos em casa, o que favorece a diminuição de custos de produção, além de criar um conjunto de fatores que contribuíram para a saúde das pessoas[46].

---

[42] WEF. World Economic Forum. Deep Shift Technology Tipping Points and Societal Impact, Survey Report, Global Agenda Council on the Future of Software & Society. 2015. Disponível em: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. Acesso em: 20 jan. 2021.

[43] SILVA, Bitencourt da; KLINGENBERG, Cristina. **Estratégias para o desenvolvimento de inovações sociais voltadas a promoção de resiliência frente ao impacto gerado pelas tecnologias da quarta revolução indústria.** Disponível em: https://www.researchgate.net/publication/328190096_ESTRATEGIAS_PARA_O_DESENVOLVIMENTO_DE_INOVACOES_SOCIAIS_VOLTADAS_A_PROMOCAO_DE_RESILIENCIA_FRENTE_AO_IMPACTO_GERADO_PELAS_TECNOLOGIAS_DA_QUARTA_REVOLUCAO_INDUSTRIAL. Acesso em: 20 mar. 2021.

[44] WEF. World Economic Forum. Deep Shift Technology Tipping Points and Societal Impact, Survey Report, Global Agenda Council on the Future of Software & Society. 2015. Disponível em: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. Acesso em: 20 jan. 2021.

[45] SCHWAB, Klaus; DAVIS Nicholas; MIRANDA, Daniel Moreira. **Aplicando a Quarta Revolução Industrial.** Tradução de: Daniel Moreira Miranda. São Paulo: Edipro, 2018.

[46] WEF. World Economic Forum. **Deep Shift Technology Tipping Points and Societal Impact, Survey Report, Global Agenda Council on the Future of Software & Society.** 2015. Disponível em:

Neste contexto, pode-se citar as transformações tecnológicas que contribuem para o desenvolvimento humano, desde a "Revolução Industrial", de modo que passou a fazer parte do cotidiano das pessoas, por meio dos sistemas que convertem a escrita em áudio, como ferramenta de auxílio para pessoas com deficiência visual, aplicativos que auxiliam no desenvolvimento de pessoas com deficiência auditiva, por intermédio da tradução para a Língua Brasileira de Sinais (Libras), sistema de Big Data, que contribuem na análise da imensidão de dados gerados diariamente. Ou seja, a tecnologia está presente nos diversos aspectos da vida humana.

Diante destas mudanças, que aparentemente vão se consolidar de forma efetiva e provocar alterações estruturais, faz-se necessário aperfeiçoar e democratizar a infraestrutura digital, pois a informação, na atualidade, é considerada um bem público universal, pois remodela a inclusão digital para uma era de transformação digital[47].

As transformações propiciadas pelo ambiente digital propiciaram o nascimento de uma revolução industrial, baseada no gigantesco volume de dados criados constantemente, na computação e na automação. Desta forma, alteram o modelo de prestação de serviços, em que processos industriais são aprimorados, criados e recriados, com base em dados e escalas antes inexistentes.

Assim, a era digital acarreta um novo paradigma no formato de produção, o que envolve bens materiais, capital humano e valores. Nesta nova configuração de mercado, os dados se apresentam como um relevante fator de produção e criam valor a partir de conteúdos gerados e compartilhados por pessoas comuns, organizações, sensores e máquinas, assim como pelas informações originadas de incomensuráveis possibilidades do cruzamento, a partir do grande acervo de referências disponíveis.

Schwab, Davis e Miranda[48], destaca que a oportunidade disponibilizada pela Quarta Revolução Industrial consiste:

> em ver que a tecnologia como algo que vai além da simples ferramenta ou de uma força inevitável, encontrando maneiras de oferecer ao maior número de pessoas a capacidade de impactar

---

http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. Acesso: em 20 jan. 2021.

[47] DINIZ, Eduardo Henrique. Tecnologia em tempos de Covid-19. **Revista GV Executivo,** Conhecimento e impacto em gestão. v. 19, n. 4, p. 47, jun./ago. 2020. Disponível em: https://rae.fgv.br/sites/rae.fgv.br/files/coluna_tecnologia_0.pdf. Acesso em: 10 jan. 2021.

[48] SCHWAB, Klaus; DAVIS Nicholas; MIRANDA, Daniel Moreira. **Aplicando a Quarta Revolução Industrial.** Tradução de: Daniel Moreira Miranda. São Paulo: Edipro, 2018. p. 36.

> positivamente a sua família, organização e comunidade, influenciando e orientando os sistemas que nos rodeiam e moldam a nossa vida.

Tudo isto traz novas perspectivas e desafios para as organizações, uma vez que o progresso tecnológico proporciona formatos inovadores para a sociedade, nos seus diversos paradigmas. Assim, a transformação digital é visualizada como uma das mais importantes tendências das empresas[49]. No intuito de melhor entender a transformação digital, faz-se imprescindível aclarar que se trata de um fenômeno que une a tecnologia e a análise de dados a processos inteligentes, de forma que gera transformações nas cadeias de valor e modelos de negócios. Ressalta-se que não existe uma definição única e universal da expressão transformação digital, tampouco de interfaces nos negócios[50].

A transformação digital provocou mudanças drásticas e muito rápidas na maneira como as empresas operacionalizam suas atividades. Acrescenta Rogers[51] que, ao encarar o desafio da transformação digital, as organizações se veem obrigadas a incorporar cada vez mais processos digitais no seu funcionamento. Isto altera suas estratégias, o que requer, necessariamente, a incorporação de novas metodologias, em especial no que tange aos instrumentos de coleta e análise da informação.

Nesta dimensão, a transformação digital nas empresas está intimamente relacionada com mudança de cultura organizacional e não somente sob o foco do seu uso na execução das atividades laborais cotidianas. Entretanto, são vislumbras sobre uma nova perspectiva de tomada de decisões, análise de mercado, por meio de um novo posicionamento no mundo dos negócios[52].

Esta nova realidade dá vazão à necessidade de novos moldes de qualificações, como engenheiro de *software*, *Cloud Computing* ou Data *Analytics*, entre tantos outros que surgiram por conta da necessidade de resolução de problemas com apoio digital, da estrutura no

---

[49] HEILIG, Leonard; SCHWARZE, Silvia; STEFAN, Voss. An analysis OF digital transformation in the history and future of modern ports. **Proceedings of the 50th Hawaii International Conference on System Sciences,** 2017. Disponível em: https://www.researchgate.net/publication/312218687_An_Analysis_of_Digital_Transformation_in_the_History_and_Future_of_Modern_Ports. Acesso em: 23 abr. 2022.

[50] BERMAN, Saul J. Digital transformation: opportunitIEs to create new business models. **Strategy and Leadership,** v. 40, n. 2, 2012. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/10878571211209314/full/pdf?casa_token=GsPGR1a3DkYAAAAA:PeSHVXK4HbWNICRhYvW5Qd_y4n4SxgR8Go7vClXyg2PCUb-Gzd8Z6WM53sRoNuB2MEtLi2xx7_PpH-uv_wLb9ANflqBLzQDFCCNZWRWjlWUGnG_LnzhdEw. Acesso em: 20 mar. 2021.

[51] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.

[52] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.

diagnóstico de doenças à terapia medicamentosa, da genética ao controle de tráfego, assim como da influência das tecnologias nos processos de mercado, como resultado das transformações provocadas pelo aceleramento do ambiente digital[53].

O enorme armazenamento computacional e a capacidade de obtenção e geração de um imenso volume de dados, tanto pelas empresas, quanto por pessoas comuns, com o uso de diversas ferramentas tecnológicas existentes, criou novos anseios também para a área do direito, uma vez que nasceram novas demandas, ainda desconhecidas.

A conectividade, as mídias sociais, os robôs e as máquinas inteligentes são apenas algumas das muitas inovações tecnológicas que ocasionam a necessidade de uma nova forma de pensar o trabalho e as habilidades necessárias para desempenhar ações produtivas em um contexto cada vez mais globalizado, oriundo do avanço tecnológico.

O cenário delineado neste contexto consubstancia uma realidade de novas perspectivas e oportunidades de mercado, conjuntamente com o desenvolvimento de técnicas, algoritmos, metodologias e métodos capazes de possibilitar a análise e interpretação destes dados, de forma a transformá-los em informações relevantes, que emergem em aplicação de diversas áreas do conhecimento e fornecem subsídios, que possibilitam de agregação de valor para as organizações, num contexto de mercado com características em constantes modificações.

Assim, o dado tornou-se elemento estratégico, tanto na esfera econômica, quanto organizacional, sendo um fator de aporte para subsidiar a tomada de decisão nos ambientes estratégicos, táticos e operacionais[54].

As organizações estão cada vez mais permeadas pelas tecnologias digitais, o que transformou radicalmente a natureza e a forma de organização[55]. Neste sentido, as IES devem ter uma visão clara da aplicabilidade dos recursos tecnológicos, com o objetivo de explorar suas capacidades e remodelar as regras e papéis institucionais, de forma a criar e capturar valor para si e para seus alunos.

Neste contexto, gerenciar esses dados de forma organizada e orientada ao conhecimento é um novo desafio, a partir de um vislumbre da eficiência, de modo que gera

---

[53] WOLFANG, Hoffamann-Riem. **Teoria geral do direito digital:** transformação digital - desafios para o direito. Rio de Janeiro: Forense, 2021.

[54] LEHONG, Hung; SWANTON, Bill. A Digital Business Technology Platform Is Fundamental to Scaling Digital Business. **Gartner Research,** 2017. Disponível em: https://www.gartner.com/en/documents/3810972. Acesso em: 18 abr. 2021.

[55] YOO, Youngjin et al. **Organizing for innovation in the digital world**. Organization Science, v. 23, n. 5, p. 1398-1408, 2012. Disponível em: https://aaltodoc.aalto.fi/bitstream/handle/123456789/16540/isbn9789526062433.pdf?sequence=1&isAllowed=y. Acesso em: 26 maio 2021.

saberes, com base nos dados e transformando-os em vantagens competitivas, mensuráveis nas suas atividades.

Sob esse prisma, de alterações no formato de mercado, Weill e Woerner[56] trazem que "não estamos mais falando de 'satisfação do cliente', mas de 'experiência do cliente'", onde a concorrência potencializada pelas novas experiências dos clientes, propiciadas pelas rápidas trocas de informação, por meio do acesso aos meios digitais, afetam diretamente as marcas, produtos e serviços.

Assim, a transformação digital exige uma visão holística da estratégia de negócios. Conforme destacado por Rogers[57], as tecnologias impactam em cinco domínios: clientes, competição, dados, inovação e valor. Nesta linha de pensamento, Kane et al.[58] ressaltam a necessidade de repensar o negócio, ou seja, relacioná-lo a um formando de estratégia digital, apoiada por líderes que promovam uma cultura que permita mudanças e inovação.

Diante de todos estes fatores e frente à transformação digital, as instituições devem adaptar-se, na busca por agregar novos valores, por meio do uso das tecnologias, via entrega de resultados e de novas experiências para o cliente, de forma a usufruir das possiblidades oferecidas pelas tecnologias[59].

Frente a isto, o avanço tecnológico alterou a maneira de conectar e criar valor para os clientes, de forma que transformou a maneira de interação entre empresas/clientes, por meio de uma iteração mais direta e uma participação mais dinâmica dos consumidores, de modo que se tornou um indutor crítico do sucesso das empresas. Diante deste novo cenário, a transformação digital provoca mudanças de paradigma e cria um novo formato de visualização e modo de agir das organizações, por meio do uso das Tecnologias de Informação e Comunicação (TICs)[60].

Neste contexto, pode-se citar o exemplo da Enciclopédia Britânica, que entendeu as novas necessidades de seus clientes, emergidas da adoção de novas tecnologias, compreendeu que a organização passa por um processo de rupturas com o seu antigo modelo de negócio.

---

[56] WEILL, Peter; WOERNER Stephanie. **Qual o seu modelo digital de negócio?** São Paulo: M. Books do Brasil, 2019.

[57] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.

[58] KANE, By Gerald C. et al. **Strategy, not technology, drives digital transformation.** MIT Sloan Management Review and Deloitte University Press, 14, 2015.

[59] LORENTE, José A. A transformação Digital. **Revista Uno**, v. 24, 2016. Disponível em: https://www.revista-uno.com.br/numero-24/a-transformacao-digital/. Acesso em: 20 ago. 2018.

[60] CHEPKASOVA, Elena. Transformation in the Era of Digitization: A study of organizations implementing digital transformation projects with integrated project management and change management. 2017. Disponível em: http://www.diva-portal.se/smash/get/diva2:1071105/FULLTEXT01.pdf. Acesso em: 12 mar. 2022.

Desta forma, adotou um processo de transformação na sua estratégia, se reposicionou e criou novos valores aos seus clientes, da realidade contemporânea[61].

Diversos setores realizaram iniciativas voltadas para o abarcamento da transformação digital em suas organizações. As IES também estão permeadas por este avanço provocado pelas tecnologias da Revolução Industrial 4.0, como: IA, Big Data, blockchain, IoT, Robótica, impressora 3D, neurotecnologia, entre outras.

Todos estes acontecimentos, oriundos das ferramentas tecnológicas, demanda das instituições a atualização deste contexto de transformações, nas várias dimensões. Aplicar as abordagens destas mutações, no seu domínio educacional, encontra um vasto campo em ascensão, que permite apresentar o panorama, o que envolve os atores mediados pelos recursos digitais e o aproveitamento das prerrogativas que englobam o bem-estar dos clientes, a gestão ambiental e a dignidade da pessoa, por meio de ganho de eficiência incorporado às tecnologias[62].

Assim, empresas com capacidade de gerenciar tecnologias digitais com eficiência, podem auferir vantagens, por meio das experiências inovadoras com o cliente e, assim, aperfeiçoar as operações e novas criar linhas de negócio[63].

Por conta do volume de dados que trafegam nas redes, surgem novos desafios para as IES, relacionados à segurança da informação e à privacidade, tanto dos dados da própria instituição, quanto dos seus acadêmicos[64].

Nesta linha de pensamento, Morais et al.[65] ressalta a necessidade das Instituições de Ensino Superior implementarem ações preventivas e corretivas, bem como trabalharem a transparência na coleta, tratamento e descarte dos dados, de forma que considere, as exigências da legislação, voltadas à proteção dos dados pessoais.

Diante destas mudanças, deve-se considerar os potenciais riscos à democracia, à segurança e à privacidade, que podem ser propiciados pelo ambiente digital. Ante o exposto,

---

[61] COLLIN, Jari et al. **It Leadership in transition – the impacto f digitalization on finnish organizations.** 2015. Disponível em: https://research.aalto.fi/en/publications/it-leadership-in-transition-the-impact-of-digitalization-on-finni. Acesso em: 02 maio 2021.

[62] CARAFFINI, Josiane Piva Testolin da Silva; SOUZA, Romina Batista de Lucena de; BEHR, Ariel. Transformação digital e desempenho no setor bancário. 2018. Disponível em: http://bibliotecadigital.fgv.br/ocs/index.php/ctd/ctd2018/paper/viewFile/6965/1971.Acesso em: 23 ago. 2022.

[63] FITZGERALD, Michael et. al. **Embracing Digital Technology:** A New Strategic Imperative | Capgemini Consulting Worldwide. MIT Sloan Management Review, 1-13. Retrieved from. Disponível em: https://emergenceweb.com/blog/wp-content/uploads/2013/10/embracing-digital-technology.pdf. Acesso em: 23 mar. 2021.

[64] ELSAADANY, Amr; SOLIMAN, Mohamed. Experimental Evaluation of Internet of Things in the Educational Environment. **International Journal of Engineering Pedagogy,** v. 7, n. 3, 2017. Disponível em: https://online-journals.org/index.php/i-jep/article/view/7187. Acesso em: 12 jun. 2022.

[65] MORAIS, Isabelly Soares. **Introdução a Big Data e Internet das Coisas (IoT).** Porto Alegre: SAGAH, 2018.

um dos aspectos a ser considerado está relacionado à proteção de dados pessoais, o que assegurará a circulação de dados pessoais, de forma transparente, aos envolvidos na coleta, tratamento e descarte destes dados.

As transformações digitais trouxeram uma maior liberdade. Por outro lado, deram causa a alguns desafios e técnicas, destinadas a construir uma sociedade de vigilância, que tem como objetivo minimizar os riscos. No entanto, para isto faz-se necessárias estratégias institucionais específicas, capazes de garantir a privacidade, em uma sociedade cada vez mais tecnológica[66].

Todas estas transformações contribuem para a formação de novos direitos, até então inexistentes, e, por consequência, geram reflexos, do ponto de vista do Estado, da regulação e do direito, em diversas instâncias, tais como a responsabilidade civil dos estabelecimentos virtuais, a proteção dos dados pessoais, a confiabilidade dos consumidores, entre tantas outras, diante da conjuntura das novas tecnologias.

A revolução tecnológica alterou significativamente o comportamento humano, nas diversas conjecturas, de forma a ampliar, sobretudo, a relação de dependência social com a tecnologia, em que o processamento de dados se insere em, praticamente, todas as searas da vida humana[67].

Com lastro neste processo de transformação, em que a tecnologia ocupa lugar central nas diversas esferas da sociedade, surge a necessidade de a área jurídica se adaptar e dar respostas a novos desafios, emergidos a partir do contexto das novas tecnologias digitais, num mundo contemporâneo, com um alto nível de processamento de dados.

Sob esta perspectiva, Hoffmann-Riem[68] ressalta que a preservação dos direitos fundamentais é algo constante, de modo que é necessário utilizar a ciência do Direito como mecanismo de regulação da inovação, à vista dos valores elencados no ordenamento jurídico, especialmente, os princípios constitucionais.

Na próxima seção, foram abordadas as tecnologias emergentes da Quarta Revolução Industrial, como: Inteligência Artificial, Big Data, Robótica, Impressora 3D, Blockchain, como objeto de conhecimento dos desafios e modelagem nesta nova revolução tecnológica, a qual implica na transformação da estrutura da humanidade. A cada capítulo, acrescer-se-á

---

[66] ELER, Kalline Carvalho Gonçalves. A releitura da privacidade: do “direito de ser deixado só” ao direito à autodeterminação informativa. **Revista Internacional de Tecnologia, Ciencia y Sociedad,** v. 5, n. 2, p. 185-196, 2020.

[67] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital, desafios para o direito.** Tradução de: Italo Fuhrmann. Rio de Janeiro: Forense, 2020. p. 311-345, jan./jun. 2021.

[68] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital, desafios para o direito.** Tradução de: Italo Fuhrmann. Rio de Janeiro: Forense, 2020. p. 311-345, jan./jun. 2021.

mais uma perspectiva das linhas da transformação digitais, mediadas pelas tecnologias digitais, que terão papel de liderança na contribuição para a produtividade das organizações com eficiência, e, assim, obter crescimento econômico, social, cultural, que favoreçam o desenvolvimento de toda a sociedade.

2.2 Tecnologias Emergentes Da Quarta Revolução Industrial

Atualmente o mundo experimenta tendências transformadoras, em diversos aspectos, de forma simultânea, como: urbanização, globalização, mudanças demográficas, climáticas e o surgimento de tecnologias, cada vez mais disruptivas[69]. Ainda segundo o ponto de vista dos autores, diversas tecnologias, Inteligência Artificial, Big Data, Internet das Coisas, Blockchain, Robótica, materiais modernos, Biotecnologia, Neuroteconologia, Impressora 3D, Tecnologias espaciais, Realidade aumentada, dentre outras, compõem o complexo tecnológico da atual revolução.

Dentre todas estas tecnologias, o enfoque deste trabalho será para as tecnologias, como: Inteligência Artificial, IoT, Robótica, Impressora 3D, Neurotecnoligia, tendo em vista que a educação é fundamental para a sociedade, bem como pelo fato de ser um dos principais pilares da civilização moderna, a qual exerce papel fundamental no desenvolvimento econômico, social e político. Assim, é possível utilizar tais tecnologias como mecanismos importantes no empoderamento democrático e no avanço do bem-estar geral das sociedades[70].

Ao corroborar com o que se abordou até aqui, as transformações estão cada vez mais presentes e determinantes na sociedade, de modo que se presume novos olhares sobre a identificação e valorização da participação das organizações no mercado. As profundas mudanças no setor industrial apresentam fortes impactos ao longo de toda a cadeia de valor, as quais levam ao surgimento de novas tecnologias, criação de novos empregos e nova forma de organização de trabalho[71].

---

[69] SCHWAB, Klaus; DAVIS Nicholas; MIRANDA, Daniel Moreira. **Aplicando a Quarta Revolução Industrial.** Tradução de: Daniel Moreira Miranda. São Paulo: Edipro, 2018.

[70] ESU. Europena Students' Union. **Policy Paper on Public Responsibility, Financing and Governance of Higher Education**. Disponível em: https://web.a.ebscohost.com/ehost/detail/detail?vid=0&sid=40bf2670-879b-4163-b543-77a9a4ec6801%40sessionmgr4008&bdata=Jmxhbmc9cHQtYnImc2l0ZT1laG9zdC1saXZl#AN=ED610895&db=eric. Acesso em: 01 set. 2021.

[71] COSTA NETO, Luiz Gonzaga da; CAMPOS, Fernando Celso de. Oportunidades de aplicações de *business intelligence* no contexto da indústria 4.0: revisão sistemática da literatura 2015-2020. **Exacta Engenharia de Produção,** 2021. Disponível em: https://periodicos.uninove.br/exacta/article/view/19525. Acesso em: 23 mar. 2022.

Benesova e Tupa[72] expõem que a indústria foi afetada por mudanças tecnológicas e inovações, chamadas de revoluções, as quais não influenciam apenas a produção, mas também o mercado de trabalho, o direito, o sistema educacional, o agronegócio, a área da saúde, entre outros.

O mundo industrial foi moldado por uma série de mudanças tecnológicas fundamentais nos últimos 250 anos: vapor e ferrovia (1750-1830), eletricidade e telefone (1880-1920), informática e TI (1960-2000), era atual da Internet Industrial das Coisas (IOT) e Big Data (2010-até o presente momento)[73]. Esta era ficou conhecida como Quarta Revolução Industrial, termo cunhado por Klauw Schwab, em 2016, o que provocou alterações voltadas para a automatização total das fábricas.

Na verdade, a expressão Quarta Revolução Industrial tem origem num projeto de estratégia de alta tecnologia do governo da Alemanha, trabalhado desde 2013 para levar sua produção a uma total independência da obra humana[74].

As transformações quanto ao uso da tecnologia nas organizações possuem como fonte e característica o validar da ruptura e o desenvolvimento de ações que articulam e promovem a caracterização de fontes, que aprimoram as atividades propostas no ambiente organizacional. Conforme abordam Geissbauer, Vedso e Schrauf[75], as principais características da Indústria 4.0 são: a digitalização e integração de toda cadeia de valor, do desenvolvimento do produto à compra, por meio da manufatura, logística e serviços; a digitalização de todos os produtos e serviços oferecidos, além da criação de novos produtos e modificação da estrutura de negócios, focada na geração de receitas digitais e otimização na interação com o cliente.

A manufatura é impulsionada pela concorrência e constante necessidade de evolução e adaptação de métodos inovadores de produção. Devido à relevância desta transição para a

---

[72] BENESOVÁ, Andrea; TUPA, Juri. Requirements for Education and Qualification of People in Industry 4.0. **Procedia Manufacturing,** v. 11, p. 2195-2202, 2017. Disponível em: https://reader.elsevier.com/reader/sd/pii/S2351978917305747?token=BF8AA30CE35F49BE276E21889B18F730598F9E93441847FA0F68CA276B56BFB27C47137E20BDAA7AF54BAD195C1310CF&originRegion=us-east-1&originCreation=20210911145230. Acesso em: 11 set. 2021.

[73] TALYA, Akanksha Manik; MATTOX, Matt. **GE's Digital Industrial Transformation Playbook, General Electrics.** 2016. Disponível em: https://fhi.nl/app/uploads/sites/5/2021/02/NOVOTEK-ge-digital-industrial-transformation-playbook-whitepaper.pdf. Acesso em: 23 jan. 2022.

[74] PERASSO, Valeria. **O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas.** BBC Brasil, 2016. Disponível em: https://g1.globo.com/economia/negocios/noticia/2016/10/o-que-e-a-4a-revolucao-industrial-e-como-ela-deve-afetar-nossas-vidas.html. Acesso em: 23 jan. 2022.

[75] GEISSBAUER, Reinhard; VEDSO, Jesper; SCHRAUF, Stefan. Industry 4.0: Building the digital enterprise. 2016. PwC. Disponível em: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf>. Acesso em: 17 ago. 2022.

manutenção de uma posição e importância global, algumas iniciativas governamentais que visam a incentivar suas indústrias foram criadas[76].

Na Alemanha, houve este incentivo, ali nomeado de Indústria 4.0. No entanto, este termo passou a caracterizar não somente um auxílio do governo, mas uma ampla mudança industrial, a nível mundial. Sua principal ideia é explorar os potenciais das novas tecnologias e conceitos em ascensão, como: disponibilidade e utilização da internet e da IoT; integração de processos técnicos e de negócios; mapeamento digital e virtualização do mundo real; fábricas inteligentes, o que inclui métodos e produtos inteligentes[77].

Monahan[78], pressupõe que os avanços tecnológicos nas áreas de conectividade móvel, inteligência artificial, robótica, internet das coisas, impressão 3D, computação quântica, engenharia genética, nanotecnologia e materiais avançados, para citar alguns, o que transformou radicalmente o sistema de produção, com alterações do trabalhador do chão de fábrica para redes distribuídas de fornecedores e fabricantes, o que formata a cadeia de suprimentos atual.

Diante deste novo ambiente de mudanças global, as organizações e governos que souberem aproveitar as possibilidades oferecidas pelas tecnologias emergentes, transformarão suas atividades e criarão novos modelos de negócios, de forma a agregar fontes de valor para clientes e *stakeholders*. Este campo emerge, também, desafios, entre eles uma concorrência mais acirrada, a nível mundial, tendo em vista a inexistência de barreiras geográficas, frente a um mundo cada vez mais globalizado e conectado.

Assim, a competitividade exige cada vez mais a participação das organizações no universo, com o objetivo de propagar e salientar as diversas formas de consagrar o que, de fato, é operante e significativo, quanto à vigência e estratégias para que os negócios validam as recompensas, o que envolve e aponta para o alicerce do uso de novas tecnologias.

Estratégias baseadas em informação são utilizadas para facilitar a reengenharia de processos, com vistas à redução de custos, criação de diferenciação no produto ou serviço, e

---

[76] KOTLER, Philip; KELLER, Kevin Lane. **Administração de marketing.** 12. ed. São Paulo: Editora Pearson, 2011.

[77] ROJKO, Andreja. Industry 4.0 Concept: Background and Overview. **International Journal of Interactive Mobile Technologies,** p. 77-90. 2017. Disponível em: https://online-journals.org/index.php/i-jim/article/view/7072. Acesso em: 17 jun. 2022.

[78] MONAHAN, Sean T. **Who will lead the "Fourth Industrial Revolution?"** Disponível em: https://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=124030788&S=R&D=bth&EbscoContent=dGJyMNLr40Sep7I40dvuOLCmsEmepq9Sr6a4SrGWxWXS&ContentCustomer=dGJyMPGssk62qbNRuePfgeyx44Dt6fIA. Acesso em: 13 set. 2021.

aumento da fidelidade do cliente, de forma a alavancar novos modelos de negócio, para crescimento de receita, o que proporciona maior agilidade nas atividades propostas[79].

A digitalização se torna cada vez mais presente e consagra a possibilidade de integração e satisfação de cada atividade proponente, para o que assegura o desenvolvimento de negócios mais operante e significativo, no que diz respeito às diversas formas de estabilidade e significado do homem junto às atividades que são incorporadas[80].

Nesta linha de pensamento, Garcia e Garcia[81] ressalta que as tecnologias emergentes da Quarta Revolução Industrial representam um processo pelo qual muitas empresas passam atualmente para se adaptar à nova realidade dos negócios. Seu início ocorreu quando as companhias perceberam que precisariam mudar para se manter fortes no mercado.

Frente a este universo, a corporatividade da organização no mercado que opera é atribuída às diretrizes econômicas e sociais. Assim, os artefatos tecnológicos possuem um espectro de impacto muito mais amplo, além de compreender expressivas mudanças no âmbito social e econômico, dentre outros. A força das tecnologias digital-social, móvel, analítica e nuvem não está nas tecnologias puramente. As empresas as integram para transformar seus negócios e a maneira como funcionam[82].

As novas oportunidades são pontos de referência para o que valida e possibilita as diversas formas de apreender e conquistar, o que, de fato, é relevante e significativo, quanto à dimensão da tecnologia, em diferentes esferas de participação do homem na sociedade.

A automatização acontece por meio de sistemas ciberfísicos, que foram possíveis graças à internet das coisas e à computação na nuvem. Os sistemas ciberfísicos, que combinam máquinas com processos digitais, são capazes de tomar decisões descentralizadas e de cooperar - entre eles e com humanos - mediante a internet das coisas[83].

A possibilidade de automatizar processos, integrando estes a sistemas de internet, traz diversos benefícios, tais como: possibilidade de reduzir custos, aumentar a capacidade de

---

[79] ANDRADE, Nayara Santos; RABELO, Maria Helena Silva. Segurança da informação: um estudo sobre o processo de segurança da informação em instituições financeiras localizadas na região centro-oeste de Minas Gerais. **Revista Acadêmica Conecta FASF,** v. 2, n. 1, p. 126-144, 2017.

[80] KANE, By Gerald C. et al. **Strategy, not technology, drives digital transformation.** MIT Sloan Management Review and Deloitte University Press, 14, 2015.

[81] GARCIA, S. Gallego; GARCIA, M. García. Industry 4.0 implications in production and maintenance management: na overview. **Procedia Manufacturing,** v. 41, p. 415-422, 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S235197891931114X. Acesso em: 21 nov. 2021.

[82] KANE, By Gerald C. et al. **Strategy, not technology, drives digital transformation.** MIT Sloan Management Review and Deloitte University Press, 14, 2015. p. 4.

[83] COSTA NETO, Luiz Gonzaga da; CAMPOS, Fernando Celso de. Oportunidades de aplicações de *business intelligence* no contexto da indústria 4.0: revisão sistemática da literatura 2015-2020. **Exacta Engenharia de Produção,** 2021. Disponível em: https://periodicos.uninove.br/exacta/article/view/19525. Acesso em: 23 mar. 2022.

customização, otimização de recursos e maior agilidade no desenvolvimento de novos produtos.

Para os CIOs (*Chief Information Officer*) que buscam reduzir o custo das operações de negócios e aumentar a flexibilidade, as estratégias que exploram novas tecnologias podem ajudar a gerenciar as mudanças nas condições, ao mesmo tempo em que ganham maior eficiência[84].

A automação de processos gera mudanças, que impactam a forma de produzir e entregar produtos. A emissão de notas fiscais é um exemplo de como a transformação digital consegue facilitar tarefas e gerar transparência. As empresas melhoram o engajamento por meio da personalização. A NIKEiD, por exemplo, é uma plataforma *online* que permite que o usuário crie o seu próprio tênis. Esta experiência só é viável porque a empresa promove uma forte interação entre a produção e a área de vendas[85].

Estas mudanças são fruto das novas necessidades da sociedade, nos mais variados aspectos, o que exige celeridade na solução de suas demandas, em conjugação com a praticidade, tendo em vista que os modelos tradicionais não são mais suficientes para atender estas novas reivindicações, o que faz com que a adaptação a esta nova realidade seja uma necessidade.

Diante deste cenário, novas tecnologias são desenvolvidas ou melhoradas, com vistas a atender a esse novo universo de competitividade e exigência de segurança dos dados, com necessidades mais complexas e diversificadas, como exemplo da tecnologia *Blockchain*, cuja finalidade era proporcionar um ambiente de interoperabilidade, melhor prestação de serviços, correlacionada à necessidade de segurança e integridade dos dados.

O *Blockchain* traz uma perspectiva disruptiva, o qual foi concebido, inicialmente, como base das criptomoedas, sendo uma tecnologia de propósito amplo e de longo alcance, em diversas áreas, podendo compreender o armazenamento de informações, como a execução de protocolos[86].

---

[84] PERASSO, Valeria. **O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas.** BBC Brasil, 2016. Disponível em: https://g1.globo.com/economia/negocios/noticia/2016/10/o-que-e-a-4a-revolucao-industrial-e-como-ela-deve-afetar-nossas-vidas.html. Acesso em: 23 jan. 2022.

[85] PERASSO, Valeria. **O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas.** BBC Brasil, 2016. Disponível em: https://g1.globo.com/economia/negocios/noticia/2016/10/o-que-e-a-4a-revolucao-industrial-e-como-ela-deve-afetar-nossas-vidas.html. Acesso em: 23 jan. 2022.

[86] TRELEAVEN, Philip; BROWN, Richard Gendal; YANG, Danny. **The banking and financial-services industry has taken notice of blockchain technology's many advantages.** This special issue explores its unlikely origins, tremendous impact, implementation challenges, and enormous potential. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8048631. Acesso em: 28 ago 2021.

Davis e Le Merle[87] estabelecem que "blockchains são livros-razão abertos, distribuídos e que podem registrar transações entre duas partes de forma eficiente, verificável e permanente". Nas palavras de Rodrigues[88], *Blockchain* é um livro digital, com transações registradas de forma cronológica e seus "cabeçalhos" podem ser visualizados por todos que tiverem o acesso permitido, inseridos num mecanismo de criptografia avançado, de forma a propiciar uma maior segurança dos dados.

Seu grande patrocinador é o *Bitcoin*, mas não é só para a negociação de criptomoedas que o *blockchain* serve, uma vez que é possível utiliza-lo para armazenar dados contábeis e realizar transações bancárias e dados de contas a pagar e receber, de forma a garantir a segurança dos dados gravados. O blockchain é um dos grandes exemplos de tecnologias disruptivas no mercado[89].

Em meio à ascensão dos recursos tecnológicos, o Big Data se destaca como uma ferramenta que proporciona um novo campo de exploração, sendo que o seu grande desafio não é o fato de o volume ser elevado, mas sim a heterogeneidade dos dados, que demandam formas inovadoras de processamento de informação. Os dados se dividem em estruturados e não estruturados[90], em que, no primeiro os dados possuem uma organização para serem recuperados, como tags, linhas e colunas que identificam onde a informação se encontra precisamente. O segundo não contém todas as informações possíveis de onde o dado se encontra e são estes os que mais crescem.

Com o Big Data em sistemas IoT, grandes fluxos de dados podem ser analisados *online*, com ferramentas avançadas e trabalho em nuvem, com maior velocidade de transmissão. Estes dados gerados permitem ser armazenados em sistemas em nuvem e distribuídos para análises futuras. Os resultados destas análises podem otimizar operações e fornecer informações, a fim de aumentar a produtividade e a eficiência, bem como reduzir os custos operacionais[91].

---

[87] DAVIS, Alison; LE MERLE, Matthew C. **Blockchain competitive advantage.** Tiburon: Fifth Era Media, 2019. *e-book.* p. 97.
[88] RODRIGUES, Murilo Ramos Alambert. **Gestão Estratégica.** Rio de Janeiro: Editora FGV, 2012.
[89] BOUTER, Rick. **Accenture digital transformation re-imagine from the outside-in.** Accenture Interactive – Point of View SerIEs, dec. 2014. Disponível em: https://www.slideshare.net/rbouter/accenture-digital-transformation-reimagine-from-the-outsidein. Acesso em: 12 mar. 2022.
[90] BATIMARCHI, Susana. **A diferença entre dados estruturados e não estruturados.** 2015. Disponível em: http://docmanagement.com.br/03/06/2015/a-diferenca-entre-dados-estruturados-e-não-estruturados/. Acesso em: 10 jun. 2022.
[91] GILCHRIST, Alasdair. **Industry 4.0:** The Industrial Internet of Things. Tailândia: Apress, 2016.

Na perspectiva de Sato[92], a rápida popularização da internet, em conjunto com seu acesso por meio de dispositivos móveis, pode ser considerada como fator principal das transformações pelas quais os meios de comunicação passam. Neste sentido, vislumbra-se um cenário promissor para o surgimento e/ou aprimoramento de tecnologias, entre elas a Internet das Coisas, que tem como finalidade conectar não apenas pessoas, mas também dispositivos móveis, carros, eletrodomésticos, entre outros. Ou seja, visa a integrar todos esses dispositivos à rede, que podem ser gerenciadas por meio da web e, por sua vez, predispõe informações em tempo real[93].

Tudo isto trará reflexos no modo como as pessoas se relacionam, fazem compras, na assistência à saúde, mas também impactará a educação, uma vez que esta se encontra inserida na seara das mudanças provocadas pelas tecnologias[94].

Santos et. al.[95] define seu conceito, ao afirmar que: "a IoT pode ser entendida como a combinação de várias tecnologias, sendo complentares no sentido de viabilizar a integração dos objetos no ambiente físico ao mundo real", os quais consideram que as IES, *Internet of Things* trazem um universo amplo de possibilidades.

Diante do atual momento, caracterizado pela ocorrência da pandemia provocada pelo Covid-19, o que, de certa forma, acelerou a aplicabilidade das mais variadas tecnologias, com o fim de continuar as atividades dos diversos contextos da sociedade, o que inclui o formato de aulas *online*, em razão do isolamento social. Neste sentido, com um olhar para aplicabilidade das novas tecnologias no âmbito educacional, a Internet das Coisas deve estar na pauta dos gestores da IES, com vistas ao aprimoramento do processo ensino/aprendizagem, uma vez que a IoT terá o papel de conectar tudo e a todos. Assim, as Instituições de Ensino Superior devem analisar seus desafios, bem como as oportunidades vislumbradas[96].

Nesta perspectiva de novas tecnologias disruptivas no seio da sociedade, que provoca um novo ambiente social, econômico, político, ressalta-se a Inteligência Artificial, que

---

[92] SATO, Silvio Koiti. **Mobilidade, comunicação e consumo: expressões da telefonia celular em Angola, Brasil e Portugal.** 2015. 366f. Tese (Doutorado em Comunicação) - Universidade de São Paulo, São Paulo, 2015.

[93] SILVA, Luiz Gustavo Pereira da; LEMOS, Thiago Oliveira; RUFINO, Hugo Leonardo Pereira. **O impacto da Internet das Coisas na educação:** uma revisão. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/7770/6919. Acesso em: 15 set. 2021.

[94] SILVA, Luiz Gustavo Pereira da; LEMOS, Thiago Oliveira; RUFINO, Hugo Leonardo Pereira. **O impacto da Internet das Coisas na educação:** uma revisão. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/7770/6919. Acesso em: 15 set. 2021.

[95] SANTOS, Bruno Pereira et al. **Internet das coisas:** da teoria à prática. Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2016. Disponível em: http://www.sbrc2016.ufba.br/minicurso/minicurso-1/. Acesso em: 01 set. 2021. p. 5.

[96] SILVA, Luiz Gustavo Pereira da; LEMOS, Thiago Oliveira; RUFINO, Hugo Leonardo Pereira. **O impacto da Internet das Coisas na educação:** uma revisão. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/7770/6919. Acesso em: 15 set. 2021.

contribui para a evolução dos diversos segmentos. Na área de recursos humanos, utiliza-se a Inteligência Artificial no recrutamento de novos talentos para as empresas. Trata-se de um grande avanço, que permite selecionar os candidatos adequados para cada posição.

2.3 Dados

Na atualidade, quando se pensa em empresa e mercado, tem que considerar a competitividade, assim como a estratégia. Lobato[97] pondera que a concorrência é um fator influenciado pela globalização, inserido no mercado mundial. Assim, as organizações devem buscar mecanismos que proporcionem mudanças flexíveis e rápidas.

Segundo Porter[98]:

> A mudança tecnológica é um dos principais motores da concorrência. Ela desempenha um papel importante na mudança estrutural da indústria, bem como a criação de novas indústrias. É também um grande equalizador, corroendo a vantagem competitiva de empresas bem estabelecidas e impulsionando outros para a vanguarda. Muitas das grandes empresas de hoje surgiram a partir de mudanças tecnológicas que foram capazes de explorar. De todas as coisas que podem mudar as regras da concorrência, a mudança tecnológica está entre as mais proeminentes.

Nota-se, portanto, que as tecnologias empreenderam um novo ritmo na sociedade, as quais trouxeram mudanças para todos os segmentos da sociedade. Neste sentido, Rogers[99] enfatiza que as empresas precisam definir estratégias, a fim de se manterem competitivas, e os dados são considerados como insumo fundamental num processo de profundas mudanças nas regras de mercado, assim como no formato de relacionamento com os clientes.

Vislumbra-se que, neste cenário marcado por uma quantidade sem precedentes de transmissão de dados, tanto pelas empresas, quanto por pessoas comuns, que os movimenta por meio da utilização dos diversos recursos digitais, cabe às organizações o desafio de converter este volume de dados em informações valiosas.

---

[97] LOBATO, Diego Botelho. **Marketing digital:** estudo sobre a importância de sua aplicação emu ma imobiliária de pequeno porte. 2012. 27f. Trabalho de Conclusão de Curso (Bacharel em Administração) – Centro Universitário de Brasília, 2012.

[98] PORTER, Michel E. **Competitive advantage:** creating and sustaining superior performance, New York: The Free Press, 1998. p. 164.

[99] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.

Jesus[100] ressalta que a parte principal das tecnologias emergentes são os dados, haja vista que as empresas produzem, gerenciam e usam as informações. Assim, o planejamento para a geração de dados é fundamental, o que possibilita o desempenho das atividades no mercado, tendo em vista que estes dados estão atualmente voltados, também, para decisões estratégicas e exploradas pelas organizações, a fim de continuarem a atuar num mercado cada vez mais globalizado.

Ao demonstrar um novo olhar em relação aos dados que são gerados a todo instante, Harari[101] sustenta, em sua obra "*21 lições para o século 21"*, a importância que os dados possuem hoje e o seu impacto no futuro, ao dizer que:

> [...] se quisermos evitar a concentração de toda a riqueza e de todo o poder as mãos de uma pequena elite, a chave é regulamentar a propriedade dos dados. [...], no século XXI, os dados vão suplantar tanto a terra quanto a maquinaria como o ativo mais importante, e a política será o esforço por controlar o fluxo de dados[102].

Dessa forma, um ambiente cada vez mais globalizado, corroborado pelo desenvolvimento de novas tecnologias disruptivas, proporciona um campo competitivo e voraz, a nível mundial, entre as diversas organizações, no que sobressaem questionamentos acerca da segurança dos dados dos titulares, pois estes dizem muito sobre seus titulares, de forma que exploram e até interferem nas decisões pessoais e chegam à esfera da invasão de privacidade.

2.4 Privacidade

A noção de privacidade, em si, já faz parte das diversas épocas da sociedade. Entretanto, somente no final do século XIX o tema começou a ser abordado pelo ordenamento jurídico, para, enfim, assumir as feições atuais, num contexto do uso das tecnologias digitais, o que abarca a necessidade da proteção dos dados. A privacidade no meio digital é um fator de discussões e valores quanto ao que apreende e atribui os diversos significados e relações, para o que resguarda e mantém a inviabilidade de violações ao que é proposto no negócio.

---

[100] JESUS, Mauricio Barros de. **Modelo Corporativo para Governança e Gestão de TI da Organização.** ISACA, 2012. Disponível em: https://wiki.tce.go.gov.br/lib/exe/fetch.php/acervo_digital:cobit5.pdf. Acesso em: 27 mar. 2021

[101] HARARI, Yuval Noan. **21 lições para o século 21.** Tradução de: Paulo Geiger. São Paulo: Companhia das Letras, 2018.

[102] HARARI, Yuval Noan. **21 lições para o século 21.** Tradução de: Paulo Geiger. São Paulo: Companhia das Letras, 2018. p. 106-107.

Para Magrani[103], o direito à privacidade relaciona-se ao direito à proteção de dignidade e personalidade humana e o seu desenvolvimento, haja vista a importância elencada na Carta Magna, em seu artigo 5º, inciso X, com relação à intimidade, à vida privada e à inviolabilidade de dados.

A privacidade é defendida na Declaração Universal dos Direitos Humanos, em seu artigo XII, preceitua que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques"[104]. A Constituição Federal, art. 5º, X, define que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"[105], o que assegura, também, os Códigos Civil, Penal e de Defesa do Consumidor, além e outras leis esparsas.

Ressalta Doneda[106], em sua obra "Da privacidade à proteção de dados pessoais", que ainda resta um elo de continuidade da privacidade, abordado por Warrem e Brandeis, em que pese na contemporaneidade seus desdobramentos possuírem um sentido amplo e complexo, comparado ao isolamento ou tranquilidade. Facchini Neto e Demoliner[107] reforçam que a privacidade discutida em 1948 possuía uma dimensão diferente da atual, com possibilidades de violação dos dados infinitamente menores, comparados com a atualidade, com acesso universalizado à internet, assim como a disponibilidade das tecnologias emergentes da Quarta Revolução Industrial.

No direito norte-americano é comum a definição de privacidade como "*the right to be left alone*". No texto constitucional, por resguardar a inviolabilidade da correspondência, bem como o direito à intimidade e à vida privada[108], a privacidade é usada, também, como

---

[103] MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. Rio de Janeiro: Konrad Adenauer Stiftung, 2018.

[104] ONU. Organização Das Nações Unidas. **Declaração Universal dos Direitos Humanos.** Disponível em: https://brasil.un.org/pt-br/91601-declaracao-universal-dos-direitos-humanos. Acesso em: 15 abr. 2021.

[105] BRASIL. Constituição da República Federativa do Brasil de 1988. Emendas Constitucionais. **Diário Oficial da União,** Brasília, 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 jan. 2021.

[106] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

[107] FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo. **Revista Internacional Consinter de Direito,** a. 5, n. 9, 2019. Disponível em: https://revistaconsinter.com/revistas/ano-v-numero-ix/direitos-difusos-coletivos-e-individuais-homogeneos/direito-a-privacidade-na-era-digital-uma-releitura-do-art-xii-da-declaracao-universal-dos-direitos-humanos-dudh-na-sociedade-do-espetaculo/. Acesso em: 11 de outubro de 2021.

[108] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

sinônimo de intimidade e acabou por gerar uma dualidade na conceituação dela na doutrina. O direito à intimidade é quase sempre considerado como sinônimo do direito à privacidade.

Já no Código Civil, a questão da privacidade também foi levada em consideração, embora de forma genérica. A proteção de divulgação de escritos, da transmissão da palavra, e da exposição ou utilização da imagem das pessoas físicas ou jurídicas, poderão ser proibidas de imediato, inclusive se o intuito for apenas comercial, sem falar em prejuízo no tocante à fama, honra e respeitabilidade, questões também protegidas pelas normas citadas.

Deste modo, compreende-se que a vida privada consiste naquilo que é particular ao indivíduo, motivo pelo qual a privacidade figura como gênero no qual a intimidade atua como espécie. A importância do direito à privacidade é tão vasta que serve de pilar para a proteção do direito de personalidade[109].

Sob outro prisma, ressalta-se que o direito à proteção de dados pauta-se em um direito de regulamentação econômica, como destaca Dohmann[110], tendo em vista que muitas possibilidades auferidas pelo tratamento automatizado de dados oferece um grande potencial econômico, entendimento também sustentado por Rogers[111].

A privacidade, bem como a proteção de dados, muitas vezes se apresenta como uma regulamentação do próprio mercado:

> em que as propriedades particulares das informações, como bens comunitários (*common goods*, nos termos da teoria econômica) e bens de experiência (*experience goods*). Além disso, normalmente o valor das informações não deriva delas mesmas, e sim das decisões subsequentes. A partir destas, porém, não se pode perceber em que informações elas estão baseadas[112].

Portanto, a proteção de dados é absolutamente necessária e a atuação jurídica torna-se essencial para que as informações não sejam repassadas, de modo a desequilibrar a confiabilidade da organização, seja para os clientes externos, seja para a concorrência ou para a própria atividade que a organização exerce.

---

[109] MARTINS NETO, João dos Passos; PINHEIRO, Denise. Liberdade de informar e direito à memória: uma crítica à ideia do direito ao esquecimento. **Revista Novos Estudos Jurídicos Eletrônica,** v. 19 - n. 3 - set-dez 2014.

[110] DOHMANN, Indra Spiecker Genannt. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. In: BIONI, Bruno (Coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021. p. 9-32.

[111] ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.

[112] DOHMANN, Indra Spiecker Genannt. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. In: BIONI, Bruno (Coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021. p. 9-32. p. 30.

A comercialização dos dados coletados pelos sites para outros fins, para empresas comerciais ou de prestação de serviços não coligadas à empresa que os coletou, merece maior atuação do Direito, em defesa dos usuários e de sua privacidade. Ou seja, a utilização cada vez maior dos recursos tecnológicos impacta a noção de proteção e privacidade, sendo necessárias novas formas de atuação do Estado, assim como do Poder Judiciário frente a esse manancial de transformações provocadas pelas tecnologias.

Neste sentido, caso ocorra alguma violação, esta é caracterizada como violação de privacidade disposto no art. 5º, inciso LXXIX da Constituição Federal, que implica na não observância aos direitos e garantias fundamentais da pessoa. Assim, em resposta a esta necessidade, surgiu, então, a Lei Geral de Proteção de Dados (LGPD).

O Art. 6º destaca que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior, de forma incompatível com essas finalidades;

b) adequação: o tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

c) necessidade: o tratamento de dados pessoais deve ser limitado 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;

d) 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;

e) 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;

f) 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;

g) 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;

h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

j) 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.

Em virtude da vigência de tais princípios, a privacidade se torna um elo de formação e construção, quanto ao que assegura, e possibilita referenciar as medidas que são envolvidas neste interagir das organizações e das atividades nelas desenvolvidas.

Em leitura panorâmica, Facchini Neto e Demolier[113] explana que a personalidade da pessoa na sociedade atual, inclusive no mundo virtual, converte-se em dados, com destaque para a necessidade de fornecer dados no dia a dia. Neste sentido, a privacidade se encontra interligada aos dados gerados pela organização.

Assim, faz-se necessária a implantação de mecanismos que forneçam subsídios para que os titulares possam, de alguma forma, ter o controle de seus dados, fornecendo-os quando imprescindível e de forma consciente.

2.5 Compliance aplicado à proteção de dados

Tendo em vista, o nível de desenvolvimento tecnológico, a urgência de propiciar um ambiente de maior segurança jurídica às relações, assim como, estabelecer uma legislação compatível com a de outros países no contexto de proteção de dados, considerando também o direito à privacidade, o Brasil promulgou a Lei 13.705/2018, conhecida como Lei Geral de Proteção de Dados Pessoas. Diante desse cenário, as organizações, sejam públicas ou privadas, de todos os portes devem implementar mecanismos para se adequarem às novas regras impostas pela legislação vigente.

Neste capítulo abordar-se-á o "*compliance*", como mecanismo de mitigação dos riscos, por meio de padrões de segurança que as organizações devem seguir, termos de uso e políticas de privacidade, como a aplicabilidade das melhores práticas a serem adotadas. Ao final, propor-se-á um modelo integrado para um projeto de conformidade com a Lei Geral de

[113] FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo. **Revista Internacional Consinter de Direito,** a. 5, n. 9, 2019. Disponível em: https://revistaconsinter.com/revistas/ano-v-numero-ix/direitos-difusos-coletivos-e-individuais-homogeneos/direito-a-privacidade-na-era-digital-uma-releitura-do-art-xii-da-declaracao-universal-dos-direitos-humanos-dudh-na-sociedade-do-espetaculo/. Acesso em: 11 de outubro de 2021.

Proteção de Dados, que contenha uma alternativa para as IES se adequarem à Lei Geral de Proteção de Dados Pessoais (LGPD).

Sob esta perspectiva, compreender o termo *compliance*, assim como conseguir vislumbrar suas aplicações práticas, é indispensável para as organizações entrarem em conformidade com as leis, padrões éticos e regulamentos[114].

No que tange ao *compliance*, tem-se que:

> O termo compliance origina-se do verbo inglês to comply, que significa cumprir, executar, obedecer, observar, satisfazer o que lhe foi imposto. Compliance é o dever de cumprir, de estar em conformidade e fazer cumprir leis, diretrizes, regulamentos internos e externos, buscando mitigar o risco atrelado à reputação e o risco legal/regulatório[115].

Nas palavras de Biegelman e Biegelman[116], *compliance* refere-se a um "estado de estar de acordo". Nesta visão, as transformações ocorridas na contemporaneidade, com destaque para o avanço dos recursos tecnológicos propiciados pela Quarta Revolução Industrial, provocaram novas demandas, sendo necessária a criação de mecanismos que forneçam às organizações meios de funcionarem em conformidade com o regramento atual da proteção de dados.

Num ambiente em que as ferramentas digitais se tornaram condicionantes, tanto da vida das pessoas, quanto do desenvolvimento das funções nas organizações, sendo determinantes para que várias atividades sejam executadas, preservar e garantir os direitos fundamentais de privacidade e proteção dos dados tornou-se um processo desafiador para as organizações.

Em virtude da vigência da Lei Geral de Proteção de Dados, as organizações são obrigadas a cumprir seus dispositivos. Neste sentido, o *compliance* se constitui num conjunto de práticas, que objetivam assegurar a adesão da organização à legislação, a um código de conduta, políticas e princípios, Isto pode ser tratado como sinônimo de conformidade em qualquer segmento, seja jurídico, administrativo ou tecnológico, ou seja, pode estar relacionado com diferentes assuntos, que almejam a plenitude na sua eficiência[117].

---

[114] SILVA, Daniel C.; COVAC, José R. **Manual de Compliance**. São Paulo: Editora de Cultura, 2015.
[115] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi. **Manual de compliance:** preservando a boa governança e a integridade das organizações. São Paulo, Atlas, 2010. p. 2.
[116] BIEGELMAN, Martin. T; BIEGELMAN, Daniel R. Building a World-**Class Compliance Program:** Best Practices and Strategies for Success. Editora: John Wiley & Sons, 2008.
[117] LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital.** São Paulo: Almedina, 2021.

Segundo Blum e López[118], o processo de implementação de um programa de *compliance* tem como finalidade proporcionar a prevenção e resolução dos efeitos das condutas lesivas, negligentes, ou mesmo não intencionais. Ou seja, traduz-se em um conjunto de ações, por meio de medidas práticas, de forma a evitar a violação de normativas e buscar a redução das ameaças e vulnerabilidades que provoquem violação de dados.

A Lei Geral de Proteção de Dados Pessoais elenca, em seu artigo 6º, além da boa-fé, princípios norteadores das condutas a serem adotadas pelas organizações que, de alguma forma, coletam, usam e armazenam dados, de forma a alcançar o *compliance*. Neste sentido, o gestor da organização exerce papel fundamental para qualquer ação: da inovação à estratégia, da adoção das melhores práticas de gestão à acreditação dos processos[119].

Entretanto, a implementação destas práticas recomendadas para o *compliance*, não é uma tarefa simples, pois demanda tempo, assim como recursos financeiros, o que exige o comprometimento da alta gestão, para tratar as questões da conformidade com a nova legislação, e deste modo, alcançar um resultado eficaz.

As transformações nos diversos pilares da sociedade, econômico, social, político, dentre outros, impõem a existência de empresas confiáveis, de modo que a gestão deve ter um olhar voltado para a implementação de códigos de ética, de conduta, padrões de integridade. Neste contexto, a implantação de programa de *compliance* se destaca como um fator importante na observância de regras e condutas que visam à conformidade com a lei.

2.5.1 Gestão de Compliance

Pinheiro[120] alerta que a implementação de um conjunto de ações que formata um programa de *Compliance* não é uma tarefa fácil, haja vista que os modelos de negócios, na atualidade, estão globalizados, em que os dados pessoais circulam pela internet de forma internacionalizada. Com a velocidade na transmissão das informações sensíveis, tornou-se imprescindível a adoção de um comportamento, por parte das organizações, proativo e

---

[118] BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. **Cadernos Jurídicas,** a. 21, n. 53, p. 171-177, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_7_cadernos_juridicos_epm.pdf?d=637250348268501368. Acesso em: 22 jan. 2022.

[119] SANTOS, Renato Almeida dos et al. Compliance and leadership: the susceptibility of leaders to the risk of corruption in organizations. **Einstein**¸ v. 10, n. 1, p. 1-10, jan.;mar. 2012.

[120] PINHEIRO, Patrícia Peck. **LGPD:** os prós e contras de prorrogar a Lei para 2022. Disponível em: https://www.cryptoid.com.br/identidade-digital-destaques/lgpd-os-pros-e-contras-de-prorrogar-a-lei-para-2022/. Acesso em: 18 set. 2021.

preventivo, caracterizado pelas melhores práticas e planejamento estratégico[121]. Neste contexto, verifica-se que nunca foi tão importante preocupar-se com a proteção dos dados pessoais.

Todavia, como pontuam Frazão, Olivia e Abílio[122], a importância de dar maior atenção à questão da proteção de dados se contrapõe ao crescimento contínuo do interesse por dados pessoais, vistos como forma de melhorar o desempenho das organizações e aprimorar suas atividades, fato que revela a necessidade veemente de inovadores mecanismos de tutela da segurança dos dados.

De acordo com Espinoza[123], são inúmeros os setores e organizações que enfrentam dificuldades no que concerne à aplicação do *compliance* na prática da proteção de dados e, mais especificamente, quanto à observância dos princípios do *compliance* em tecnologias características.

Às organizações são impostas adaptações, para que suas atividades estejam de acordo com as regulamentações nacionais e internacionais, o que implica em ajustes nas suas rotinas. Porém, isto não significa, necessariamente, que elas terão que limitar suas atividades com vistas à conformidade com a regulação. Ademais, a instabilidade regulatória observada no Brasil com relação à proteção de dados e segurança da informação torna esta tarefa um pouco mais complexa[124].

Ao tratar da gestão de *compliance*, Frazão, Oliva e Abílio[125] destacam três fatores que favorecem o fortalecimento dos mecanismos de *compliance* no contexto da proteção de dados, quais sejam: o amplo escopo de incidência da LGPD, o que requer adaptação não somente das atividades relacionadas à coleta e tratamento dos dados, mas também de todas as operações que impliquem em repasse (direta ou indiretamente) ou utilização, de modo que até as mais simples atividades deverão fazer parte do programa de *compliance*.

---

[121] ANAHP. Associação Nacional de Hospitais Privados. **Manual de melhores práticas LGPD.** 2020. Disponível em: https://www.anahp.com.br/pdf/manual-melhores-praticas-lgpd.pdf. Acesso em: 14 set. 2021.

[122] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 677-715.

[123] ESPINOZA, Javier. EU admits it has been hard to implement GDPR. **Finacial Times,** 23 jun. 2020. Disponível em: https://www.ft.com/content/66668ba9-706a-483d-b24a-18cfbca142bf. Acesso em: 17 maio 2021.

[124] ANAHP. Associação Nacional de Hospitais Privados. **Manual de melhores práticas LGPD.** 2020. Disponível em: https://www.anahp.com.br/pdf/manual-melhores-praticas-lgpd.pdf. Acesso em: 14 set. 2021.

[125] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 677-715.

O segundo fator destacado pelos autores acima tem relação com o objetivo da proteção de dados, que não é tornar inviável a coleta de dados para conhecimento do seu público alvo ou para favorecer o aprimoramento das atividades da organização, em que pese o dever de respeito às pessoas físicas a quem estes dados pertencem.

Já o terceiro, e último, fator, refere-se à necessidade de tornar tangíveis certos ditames da LGPD, de modo a possibilitar a adoção de comportamentos considerados consonantes com o que dita o regramento legal[126].

Para corroborar com o raciocínio supra, cita-se Reis[127], o qual pondera que há, ainda, um quarto elemento fundamental na gestão de *compliance* em matéria de proteção de dados, qual seja o comprometimento da alta administração da organização, a qual deve estar empenhada em adotar práticas de gestão que conduzam à efetivação do *compliance*.

A autora mencionada destaca a autonomia e independência do setor de *compliance*, os treinamentos periódicos e a criação de uma cultura corporativa ética e de respeito ao regramento, como fatores de extrema importância para o sucesso da gestão de *compliance* em proteção de dados.

A este respeito, o IBGC[128] defende que:

> O comprometimento e o apoio da administração, explicitados de forma inequívoca desde o início, são condições indispensáveis e permanentes para a criação e o funcionamento de um sistema de *compliance*, buscando fomentar uma cultura ética e uma conduta de respeito aos valores e à legislação. Os administradores da organização e demais gestores, por ocuparem uma função de destaque em relação aos colaboradores, precisam dar exemplos positivos.

Um programa de *compliance* se apresenta como um sistema de alta complexidade e que requer organização, posto ser formado por uma série de componentes. Por assim ser, tal programa requer uma estrutura múltipla, formada por pessoas, processos, sistemas eletrônicos, documentos, ações e ideais. Neste contexto, é imprescindível que haja a nomeação de um gestor, que será o responsável pela área de *compliance* da organização, ao

---

[126] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 677-715.

[127] REIS, Beatriz de Felippe. A cultura de compliance em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista de Direito do Trabalho,** v. 214, p. 323-340, nov./dez. 2020. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/180571. Acesso em: 13 set. 2021.

[128] IBGC. Instituto Brasileiro De Governança Corporativa. **Compliance à luz da governança corporativa.** São Paulo: IBGC, 2017. p. 32.

qual deverá conferir-se autoridade e recursos e autonomia suficientes para assegurar a eficácia do programa[129].

Nesta conjuntura, Reis[130] evidencia, ainda, que a gestão de *compliance* requer o monitoramento constante dos controles e processos, com vistas a atualizar e adequar o programa de *compliance* adotado pela organização. Esta supervisão constante favorece a identificação de conflitos e medidas corretivas necessárias.

Xavier et al.[131] ponderam que a confiabilidade e eficácia de um programa de *compliance* são mensuradas por meio de um processo de avaliação constante de sua execução, consistente em monitoramento e auditorias, com o fito de identificar os pontos onde, porventura, algum (ns) pilar (es) do programa não está (ão) funcionamento de acordo com aquilo que foi planejado.

Ressalta-se que o monitoramento é de fundamental importância para assegurar a efetividade e contínuo aperfeiçoamento do programa de *compliance*, em razão de favorecer a avaliação da adequação e do cumprimento das políticas e procedimentos instituídos, com vistas a identificar e avaliar possíveis desvios no planejamento efetuado pela gestão[132].

Sublinha-se que o *compliance* de dados apresenta como particularidade o fato de que sempre requer atualizações, haja vista a constante evolução da sociedade e das tecnologias utilizadas na proteção dos dados[133].

Na temática gestão de *compliance* em proteção de dados pessoais, se destaca a pessoa do gestor de *compliance*, o qual, segundo Xavier et al.[134], precisa reunir habilidades para

---

[129] SIBILLE, Daniel; SERPA, Alexandre; FARIA, Felipe. **Os pilares do programa de compliance:** uma breve discussão. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Os-pilares-do-programa-de-compliance.pdf. Acesso em: 12 mar. 2022.

[130] REIS, Beatriz de Felippe. A cultura de compliance em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista de Direito do Trabalho,** v. 214, p. 323-340, nov./dez. 2020. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/180571. Acesso em: 13 set. 2021.

[131] XAVIER, Deiverson Felipe Souza et al. **Compliance uma ferramenta estratégica para a segurança das informações nas organizações**. In: SIMPÓSIO Internacional de gestão de projetos, inovação e sustentabilidade, 6, São Paulo, nov. 2017. Disponível em: http://www.singep.org.br/6singep/resultado/429.pdf. Acesso em: 14 set. 2021.

[132] IBGC. Instituto Brasileiro De Governança Corporativa. **Compliance à luz da governança corporativa.** São Paulo: IBGC, 2017.

[133] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). **A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 677-715.

[134] XAVIER, Deiverson Felipe Souza et al. **Compliance uma ferramenta estratégica para a segurança das informações nas organizações**. In: SIMPÓSIO Internacional de gestão de projetos, inovação e sustentabilidade, 6, São Paulo, nov. 2017. Disponível em: http://www.singep.org.br/6singep/resultado/429.pdf. Acesso em: 14 set. 2021.

coordenar, conhecimento acerca do regramento legal aplicável ao ramo do qual a organização na qual ele está inserido faz parte, assim como sobre o código de ética da sua empresa e, principalmente, ter profundo conhecimento acerca do programa de *compliance* adotado pela organização, sem o que não será possível a gestão do *compliance* alcançar êxito da execução do programa adotado.

2.6 Arcabouço legal

Em razão das transformações ocorridas na sociedade, a nível mundial, nos últimos anos, com destaque para as mudanças nas dinâmicas ocasionadas pelo fenômeno da globalização e, via de consequência, a incorporação das novas tecnologias nas relações sociais de um modo geral, os dados pessoais se tornaram bem mais vulneráveis e merecedores de uma atenção especial por parte do legislador, inclusive no âmbito da sociedade brasileira.

No Brasil, todos os textos constitucionais que já vigoraram referem-se ao direito à inviolabilidade do domicílio e ao direito à confidencialidade das comunicações. Todavia, somente na constituição de 1988 contemplou-se o direito à privacidade e proteção das pessoas privadas[135].

Além da previsão no texto constitucional, como salientam Souza e Acha (2022), tem-se, ainda, a Lei Geral de Proteção de Dados (Lei 13.709/2018) que disciplina mais especificamente a questão da proteção, disponibilização e tratamento de dados pessoais por entidades que os detêm. Posteriormente, a Emenda Constitucional 115/202. inseriu três novos dispositivos à Carta Magna, cujas normas destacam a proteção de dados nos dias atuais. Os acréscimos feitos pela EC 112 foram:

> Art. 1º O *caput* do art. 5º da Constituição Federalpassa a vigorar acrescido do seguinte inciso LXXIX: "Art. 5º LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.
> Art. 2º O *caput* do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI: "Art. 21 XXVI-organizar e fiscalizar a proteção e o tratamento de dados pessoais, nostermos da lei."
> Art. 3º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX: "Art. 22. XXX-proteção e tratamento de dados pessoais (BRASIL, 2022).

[135] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

Nota-se, portanto, que, em que pese as Constituições Federais anteriores à em vigor fazem menção ao direito à privacidade, em suas diversas variações, apenas na Carta Magna de 1988 o legislador, de fato, debruçou-se sobre esta problemática, o que pode se justificar pelo aumento da necessidade de se resguardar alguns direitos dos cidadãos, agora mais vulneráveis em razão da evolução da sociedade rumo à digitalização das relações em geral.

O Brasil avançou bastante nos últimos anos no quesito transparência pública. Para corroborar com isto, destaca-se o compromisso de 2011 com a *Open Government Partnership* (OGP). Tal parceria requer que os países participantes se comprometam com os denominados planos de ação, que englobam as recomendações e atos do país, com vistas a melhorar a transparência, viabilizar a prestação de contas e fomentar a responsabilidade, engajamento cívico e inovação. Como resultado dos compromissos assumidos, este país editou leis, portarias e decretos que visam a embasar a publicação de informações e aumentar o volume de dados disponibilizados à sociedade[136].

Como elucida Doneda[137], a autonomia da legislação protecionista de dados pessoais parece ser uma tendência já bem ancorada nos ordenamentos jurídicos de vários países, em particular porque a proteção de dados tem sido qualificada como um direito fundamental da pessoa.

Sobressai, assim, a preocupação do legislador, a nível mundial, com a proteção de dados e a busca incessante por mecanismos que possam efetivar a segurança dos cidadãos. Neste tocante, em especial com relação aos seus dados pessoais e os malefícios que a exposição indevida deles podem acarretar para a vida do indivíduo que tem tais direitos violados.

No cenário internacional, semelhantemente ao que aconteceu no Brasil, percebe-se que, com a modernidade do século XX, as preocupações com o direito à privacidade se avolumaram bastante. Exemplo disto é que a Constituição norte-americana de 1788 não fazia referência clara à inviolabilidade do domicilio, tampouco ao direito à privacidade[138]. No entanto, com a Quarta e Quinta Emendas, bem como com a Declaração Universal dos Direitos

---

[136] CAROSSI, Daniel Fernando. **Dados abertos:** categorias e temas prioritários a serem disponibilizados pelas instituições federais de ensino superior (IFES) aos cidadãos. 2016. 139f. Dissertação (Mestrado em Sistemas de Informação) – Universidade Federal de Pernambuco, Recife, 2016.

[137] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law,** v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 13 jan. 2021.

[138] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

Humanos, este direito passou a ser considerado importante, vale citar, aqui, o artigo 12 da Declaração de 1948[139].

Neste contexto, a segurança dos dados e a privacidade se tornaram essenciais para o desenvolvimento da sociedade. Por assim ser, chamou a atenção do legislador pátrio, que elaborou normas esparsas e, principalmente, uma lei específica para dirimir as questões relativas à proteção de dados pessoais, denominada de Lei Geral de Proteção de Dados, sobre a qual explanar-se-á mais detalhadamente doravante, no intuito de se ter uma melhor compreensão sobre o assunto.

Como pontua Pessoa[140] "a segurança da informação tornou-se indispensável para qualquer empresa, organização, instituição, seja pública ou privada, em decorrência do crescente números de utilização dos sistemas operacionais que envolvem o tratamento de dados pessoais".

A despeito do objetivo das leis protetivas de dados, Shores e Oliveira[141] ponderou que elas objetivam à harmonização entre os interesses legítimos dos indivíduos titulares de dados, com aqueles eleitos pelas empresas como prioridade, pois, "a lei não tem como fim frear o desenvolvimento tecnológico, mas tão somente compatibilizar direitos e expectativas, de forma a fomentar a inovação e viabilizar o tratamento legítimo dos dados".

Tonou-se muito mais comum a mercantilização dos próprios dados, seu tratamento, análise e agregação. No entanto, o que se observa é que o crescimento do volume e da qualidade das bases de dados, associado ao aumento da capacidade de processamento e análise de tais informações, culminou por se tornar um fator de risco para a privacidade dos cidadãos e, via de consequência, gerador de uma série de problemas[142].

Nota-se a inegável necessidade da existência de uma regulação que organiza o funcionamento de bancos de dados pessoais se conduz, portanto, num caminho de aceitação

---

[139] Artigo 12°. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei (BRASIL, 1948).

[140] PESSOA, Larissa Rocha de Paula. **Os desafios da governança de dados e a realidade cultural brasileira.** 2021. 152f. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2021. p. 125.

[141] SHORES, Robert Daniel; OLIVEIRA, André. **Conhecendo a lei geral de proteção de dados do Brasil – LGPD.** Disponível em: https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf. Acesso em: 11 jan. 2022. p. 2.

[142] MACHADO, Matheus Fogaça. **Medidas de proteção de dados pessoais no planejamento e operação de SMART grid utilizando computação em nuvem:** estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil. 2019. 117f. Dissertação (Mestrado em Planejamento e Governança Pública) - Universidade Tecnológica Federal do Paraná, Curitiba, 2019.

sem o endeusamento de seus potenciais nem o menosprezo da sua afetação à dignidade humana"[143].

Sublinha-se que, a despeito da imposição constitucional de publicidade nos atos da Administração, a legislação vigente no Brasil já contemplava a exigência de transparência, por exemplo na gestão fiscal (arts. 48, 48-A e 49 da Lei Complementar nº 101/2000)[144].

Observa-se, pela singela observação do arcabouço legal brasileiro atinente à proteção de dados, em diversas esferas, que a necessidade de se lidar, pelo aspecto normativo, com a questão da exposição de dados pessoas e suas consequências, não é uma constatação recente.

Como abordam Lugati e Almeida[145] "as regulamentações sobre proteção de dados passam por diversas fases até chegar ao momento atual quando o direito à proteção de dados adquire o enfoque como um direito fundamental e passa a ter legislações específicas e completas como a LGPD".

No mesmo sentido, ao explanar acerca do arcabouço legal brasileiro atinente à proteção de dados, Doneda[146] pontua que as normas que abordam a proteção de dados pessoais podem ser classificadas em quatro etapas, consoante consignado por Viktor Mayer-Scönberger. A primeira contempla as leis que tratam da criação dos bancos de dados, na década de 70, assim como dos limites impostos ao Estado, no que concerne ao uso e controle das informações. A princípio, o legislador voltou-se mais para as questões relacionadas com a evolução da tecnologia e o processamento dos dados.

Como comentam Lugati e Almeida[147], "a primeira geração de leis se insere no contexto do Estado Moderno, onde o Estado se utilizava de grandes bancos de dados, pois o

---

[143] BRASIL. Ministério Público Federal. **Sistema brasileiro de proteção e acesso a dados pessoais:** análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília: MPF, 2019. p.15.

[144] BRASIL. Ministério Público Federal. **Sistema brasileiro de proteção e acesso a dados pessoais:** análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília: MPF, 2019. 85p.

[145] LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre a proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito,** v. 12, n. 2, 2020. Disponível em: https://webcache.googleusercontent.com/search?q=cache:IErV4URFlxwJ:https://periodicos.ufv.br/revistadir/article/download/10597/5880/48773+&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 2 fev. 2022. p. 4.

[146] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law,** v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 13 jan. 2021.

[147] LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre a proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito,** v. 12, n. 2, 2020. Disponível em: https://webcache.googleusercontent.com/search?q=cache:IErV4URFlxwJ:https://periodicos.ufv.br/revistadir/article/download/10597/5880/48773+&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 2 fev. 2022. p. 4-5.

controle da população se dava por meio de obtenções massivas de informações sobre os indivíduos".

De modo bastante elucidativo, Gasiola[148] explica que a primeira geração perdurou até que fosse implementada a *Bundesdatenschutzgesetz*, denominação dada à lei federal da República Federativa da Alemanha, que versa acerca da proteção de dados pessoais, em 1977. Diversas normas que disciplinam a questão da proteção de dados foram criadas na Alemanha naquela época. O autor aclara que esta geração e leis acabou por se tornar ultrapassada, em razão da evolução tecnológica, o que culminou com o tratamento dos dados indo além do domínio governamental.

Na segunda etapa, já no final da década de 70, o foco esteve na privacidade das pessoas e no acesso de terceiros aos dados a elas pertencentes, com destaque para o controle, no objetivo de conferir aos cidadãos maneiras de tutelar seus direitos individuais[149].

Consoante explana Bioni[150], a partir desta segunda fase, facultou-se ao usuário, por intermédio de consentimento expresso, fazer parte do processo de tratamento de dados, de forma a participar da coleta, uso e compartilhamento de seus dados pessoais.

Ainda de acordo com Doneda[151], na terceira fase o foco esteve no princípio de liberdade, de forma que o titular dos dados ganhou certa autodeterminação, no que diz respeito à coleta e tratamento dos seus dados, assim como à forma como isto ocorria.

De acordo com Lugati e Almeida[152]:

> A terceira geração de leis se preocupa mais com a tutela do direito à privacidade, indo além da liberdade de ceder ou não os dados, mas sim em garantir a efetividade deste direito.
> Contudo, essa geração só abarcou uma parcela de indivíduos e isso fez com que a terceira geração se tornasse insuficiente, caminhando assim para a quarta geração, que prevalece até hoje.

---

148 GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha.** 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-daprotecao- de-dados-na-alemanha-29052019. Acesso em: 2 fev. 2022.

149 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law,** v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 13 jan. 2021.

150 BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

151 DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law,** v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 13 jan. 2021.

152 LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre a proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito,** v. 12, n. 2, 2020. Disponível em: https://webcache.googleusercontent.com/search?q=cache:IErV4URFlxwJ:https://periodicos.ufv.br/revistadir/article/download/10597/5880/48773+&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 2 fev. 2022. p. 5.

Por fim, na quarta e última etapa, o legislador voltou-se mais para a aplicação de técnicas que visam a efetivar o controle da desigualdade verificada entre o cidadão titular dos dados pessoais e a entidade que os coleta e processa.

Observa-se, assim, que foi longo o caminho percorrido pela legislação até chegar ao arcabouço legislativo à disposição da sociedade nos dias atuais, de onde se observa uma progressão protecionista, que levou aos ditames observados na LGPD em vigor no Brasil.

A respeito disto, Calabrich[153] comenta que "o processo legislativo que culminou na aprovação do RGPD é fruto de uma preocupação cada vez mais candente, mas que já vinha sendo debatida há anos nas cortes europeias".

Ademais, de acordo com a explanação de Panek[154], o crescimento vertiginoso da utilização e exposição dos dados culminou numa situação em que: "não é surpresa a inclinação dos ordenamentos jurídicos na criação de normas autônomas para a proteção da matéria, levando ao desenvolvimento de um direito fundamental à proteção de dados".

Os progressos observados na humanidade têm relação diretamente proporcional ao volume de informações compartilhadas. Como consequência direta disto, o direito ao acesso se expandiu até possibilitar o alcance a vários conteúdos, independentemente do local onde o sujeito se encontra. Como resultado disto, houve um avanço considerável da inteligência, do marketing, da publicidade e dos dados pessoais, de modo a se tornar uma mercadoria interessante para se trabalhar no mercado[155].

Finkelstein e Finkelstein[156] corroboram a assertiva acima, ao afirmarem que "É notório que desde o advento da internet, a coleta de dados invadiu sobremaneira a privacidade das pessoas. Novas normas se faziam necessárias à proteção da privacidade na sociedade da informação".

Antes da entrada em vigor da legislação brasileira específica para a proteção de dados pessoais, qual seja a LGPD, houve outras normas que, de alguma forma, também buscaram disciplinar esta questão, de modo a dar solução às demandas que surgiam. Entrementes, à

---

[153] CALABRICH. Bruno Freire de Carvalho. O conceito de tratamento de dados pessoais e o acordo Lindqvist, do Tribunal de Justiça da União Europeia. **Revista Tribunal Regional Federal da 1ª Região,** a. 31, n. 2, 2019. Disponível em: https://rtrf1.emnuvens.com.br/trf1/article/view/103/92. Acesso em: 28 dez. 2021. p. 1.

[154] PANEK, Lin Cristina Tung. **Lei geral de proteção de dados nº 13.709/2018:** uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019. 35f. Monografia (Curso de Direito) - Universidade Federal do Paraná, Curitiba, 2019. p. 17

[155] SCHIRMER, Dara Luana; THAINES, Aleteia Hummes. A implementação da Lei Geral de Proteção de Dados nas rotinas dos profissionais da área contábil: percepções dos contabilistas associados à associação dos contabilistas do Vale do Paranhana/RS. **Revista Eletrônica de Ciências Contábeis,** v. 10, n. 1, p. 31-56, 2021. Disponível em: https://seer.faccat.br/index.php/contabeis/article/view/1956. Acesso em: 15 jun. 2022.

[156] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

medida que evoluíam as relações sociais e seus conflitos, a legislação passou a carecer de ajustes, a fim de conseguir acompanhar as mudanças, o que culminou com a edição da LGPD. Ademais, o avanço tecnológico e as alterações no ambiente informacional gerou um cenário bastante propício para a prática de crimes cibernéticos, de onde surgiu a necessidade da criação de leis que visem ao combate de tais práticas criminosas[157].

Na visão de Mattos Filho e Quiroga Junior[158], a LGPD:

> É uma lei que estabelece regras detalhadas para a coleta, uso, tratamento e armazenamento de dados pessoais e afetará todos os setores da economia, inclusive as relações entre clientes e fornecedores de produtos e serviços, empregado e empregador, relações comerciais transnacionais e nacionais, além de outras relações nas quais dados pessoais sejam coletados, tanto no ambiente digital quanto fora dele.

No tocante às diretrizes introduzidas na legislação por intermédio da Lei de Acesso à Informação, alguns atos normativos infralegais foram editados, com o fim de disciplinar o tema, dentre os quais merecem destaque, no âmbito federal, o Decreto nº 7.724/2012, que regulamenta referido diploma legal; o Decreto nº 8.777/2016, que institui a Política de Dados Abertos do Poder Executivo Federal; e a Instrução Normativa nº 4/2012, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, a qual definiu Infraestrutura Nacional de Dados Abertos.

De mais a mais, existem atos normativos que, no intuito de alcançar a regulamentação do controle social de políticas públicas, de forma indireta, tratam da transparência governamental, como é o caso do Decreto nº 8.243/2014, por meio do qual criou-se a Política Nacional de Participação Social e o Sistema Nacional de Participação Social[159].

O Decreto nº 8.777, de 11 de maio de 2016, estabeleceu a Política de Dados Abertos do Poder Executivo federal, ao determinar que as instituições da Administração Pública Federal (APF) criem Planos de Dados Abertos, no intuito de colocar à disposição da sociedade dados de interesse público. No texto do primeiro inciso do artigo Art. 1º, a norma em comento impõe às instituições da APF o dever de "promover a publicação de dados

---

[157] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.

[158] MATTOS FILHO, Veiga; QUIROGA JUNIOR, Marrey. **Guia para a Lei Geral de Proteção de Dados.** ago. 2018. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Acesso em: 12 jan. 2021. p. 2.

[159] BRASIL. Ministério Público Federal. **Sistema brasileiro de proteção e acesso a dados pessoais:** análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília: MPF, 2019. 85p.

contidos em bases de dados de órgãos e entidades da administração pública federal direta, autárquica e fundacional sob a forma de dados abertos"[160].

Frente a esta nova realidade fática, tornou-se indispensável que se adotem tecnologias e dados abertos, no intuito de favorecer a disseminação e publicação de informações públicas junto à sociedade[161].

No ano de 2011, ao entrar em vigor a Lei de Acesso à Informação - LAI (Lei 12.527) restou regulamentado o direito previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no § 2º do art. 216 da Constituição Federal, que há muito carecia de regulamentação. A norma infraconstitucional em comento alterou a Lei 8.112, de 1990, e revogou a Lei 11.111, de 2005, bem como dispositivos da Lei 8.159, de 1991[162].

Para complementar a explanação acima, Carossi[163] comentou que, ao entrar em vigor a Lei nº 12.527 de 2011, o legislador impôs às instituições públicas federais, estatuais e municipais a obrigação de disponibilizar informações públicas de modo ativo à sociedade.

Um dos principais objetivos da Lei de Acesso à Informação é aumentar o nível de democratização e transparência da coisa pública, de forma que permita à sociedade o acesso às informações em poder dos órgãos públicos, que versem sobre temas de interesse coletivo ou particular. Ademais, a norma em questão deixa evidente a definição de "Governo Aberto", com vistas a colocar ao dispor da sociedade informações para consulta de forma livre sociedade[164].

A LAI se destaca como um marco para a transparência no âmbito do Brasil, em virtude de estabelecer a obrigação de as instituições públicas procederem à divulgação das informações de forma ativa, independentemente de haver ou não solicitação por parte da sociedade. Quaisquer informações, assim como os dados processados ou não, que façam parte

---

[160] BRASIL. Decreto n. 8.777, de 11 de maio de 2016. Institui a Política de Dados Abertos do Poder Executivo Federal. **Diário Oficial da União,** Brasília, 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm. Acesso em: 8 fev. 2022.

[161] CAROSSI, Daniel Fernando. **Dados abertos:** categorias e temas prioritários a serem disponibilizados pelas instituições federais de ensino superior (IFES) aos cidadãos. 2016. 139f. Dissertação (Mestrado em Sistemas de Informação) – Universidade Federal de Pernambuco, Recife, 2016.

[162] BORGES, Cyonil. **Resumo da lei de acesso à informação – concurso público.** 2012. Disponível em: https://www.tecconcursos.com.br/blog/resumo-da-lei-de-acesso-a-informacao-lei-125272011/. Acesso em: 11 jan. 2022.

[163] CAROSSI, Daniel Fernando. **Dados abertos:** categorias e temas prioritários a serem disponibilizados pelas instituições federais de ensino superior (IFES) aos cidadãos. 2016. 139f. Dissertação (Mestrado em Sistemas de Informação) – Universidade Federal de Pernambuco, Recife, 2016.

[164] CAROSSI, Daniel Fernando. **Dados abertos:** categorias e temas prioritários a serem disponibilizados pelas instituições federais de ensino superior (IFES) aos cidadãos. 2016. 139f. Dissertação (Mestrado em Sistemas de Informação) – Universidade Federal de Pernambuco, Recife, 2016.

de um meio ou formato, disponibilizados, produzidos ou custodiados pela administração pública devem ser divulgados[165].

Com o passar dos anos, foram vários os fatores políticos e econômicos que levaram à criação de três Projetos de Leis principais, quais sejam: 4.060/2012, 330/2013 e 5.276/2016, normas estas de suma importância para a elaboração do Projeto de Lei nº 53/2018, aprovado pelo Congresso Nacional e sancionado pela Presidência da República no dia 14 de agosto de 2018[166].

A inquietação com relação à proteção aos dados se mostra muito mais intensa atualmente, pelo fato de que, para utilizar praticamente todos os produtos ou serviços os usuários precisam se identificar e proceder a uma autenticação, por intermédio da comunicação de seus dados pessoais. Seja nas relações *online*, seja em estabelecimentos físicos, nota-se que os dados agora constroem um perfil cada vez mais cheio de detalhes acerca das vidas dos indivíduos[167].

Cruz[168] elaborou um quadro bastante interessante sobre as legislações concernentes à proteção de dados que precederam à LGPD, onde ilustra uma linha do tempo, como se vê da figura 1:

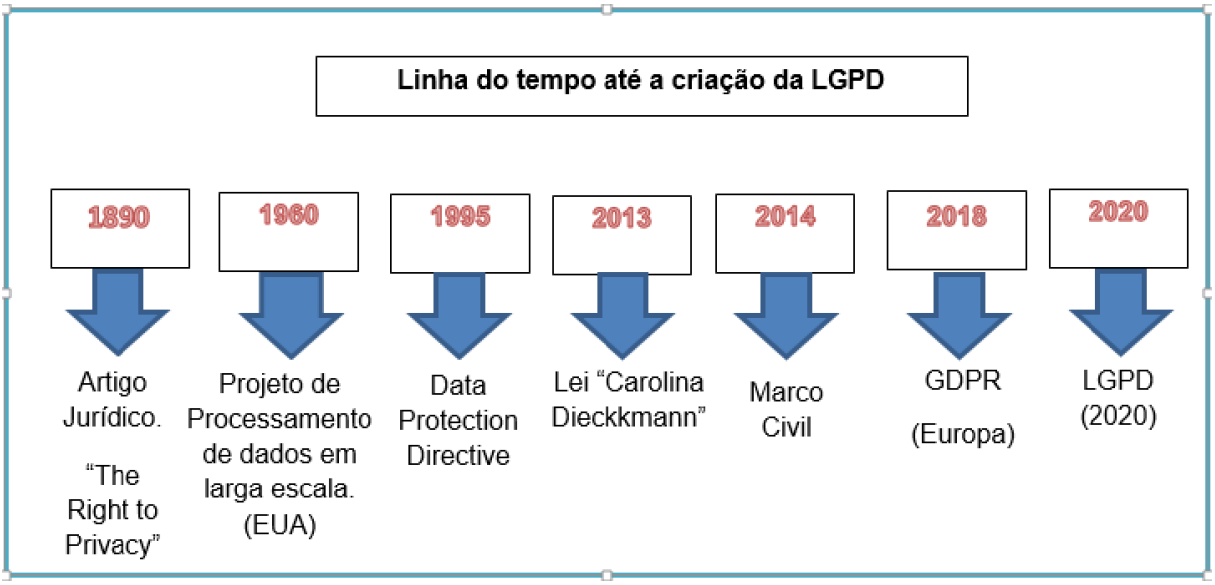
---

[165] CAROSSI, Daniel Fernando. **Dados abertos:** categorias e temas prioritários a serem disponibilizados pelas instituições federais de ensino superior (IFES) aos cidadãos. 2016. 139f. Dissertação (Mestrado em Sistemas de Informação) – Universidade Federal de Pernambuco, Recife, 2016.

[166] SHORES, Robert Daniel; OLIVEIRA, André. **Conhecendo a lei geral de proteção de dados do Brasil – LGPD.** Disponível em: https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf. Acesso em: 11 jan. 2022.

[167] MACHADO, Matheus Fogaça. **Medidas de proteção de dados pessoais no planejamento e operação de SMART grid utilizando computação em nuvem:** estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil. 2019. 117f. Dissertação (Mestrado em Planejamento e Governança Pública) - Universidade Tecnológica Federal do Paraná, Curitiba, 2019.

[168] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.



Fonte: Cruz[169].

Figura 1. Linha do tempo até a criação a LGPD.

Na opinião externada por Shores e Oliveira[170], a Lei Geral de Proteção de Dados é de suma importância para a harmonização de todas as normas vigentes no Brasil que versam sobre a proteção de dados (Código de Defesa do Consumidor, a Lei de Acesso à Informação, a Lei do Cadastro Positivo, a Resolução BACEN 4.658/2018, entre outras). Além disto, a legislação especial tem o potencial de elevar o Brasil ao patamar daquelas nações que garantem segurança jurídica ideal à proteção de dados pessoais, o que reflete significativamente na questão da transferência internacional de dados.

Insta pontuar que os dados permanecem figurando como um dos recursos de maior valor a nível mundial. Por outro lado, a utilização de dados influencia as pessoas e favorece a geração de lucro, o que ocasionou o surgimento de diversas questões éticas, as quais levaram vários países a elaborar novas legislações, que disciplinem a questão do direito à privacidade[171].

[169] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.

[170] SHORES, Robert Daniel; OLIVEIRA, André. **Conhecendo a lei geral de proteção de dados do Brasil – LGPD.** Disponível em: https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf. Acesso em: 11 jan. 2022

[171] GOMES, Heloisa dos Santos. **Lei geral de proteção de dados (LGPD):** uma análise dos impactos da lei na cultura e tratamento de dados no Brasil. 2019. 28f. Monografia (Curso de Tecnologia em Análise e Desenvolvimento de Sistemas) - Universidade do Sul de Santa Catarina, Florianópolis, 2019.

Ao explanarem sobre o surgimento da LGPD, Finkelstein e Finkelstein[172] comentam que:

> Em 2010 houve uma consulta pública executada pelo Ministério da Justiça sobre os limites de privacidade e uso de dados no Brasil, que contou com 2.500 contribuições. Posteriormente a discussão se alastrou, principalmente com a disseminação de casos como o *Wikileaks*, as revelações de espionagem por Edward Snowden e o escândalo da *Cambridge Analytica* com suas possíveis implicações no controle dos processos eleitorais democráticos. A consulta pública foi fonte para um texto maduro que gerou em 2016 o PL 5276/2016, aprovado sob unanimidade na Câmara dos Deputados. Ainda neste ano, as movimentações políticas de impeachment tiraram o foco da PL. Em 2017 o tema foi retomado pela Comissão de Assuntos Econômicos do Senado, e pressionado com ênfase no caráter de urgência, dada a vantagem econômica que o texto poderia proporcionar ao Brasil.

A evolução digital, nos moldes observados na atualidade, fez com que se formasse um mundo no qual a publicidade direcionada aparece a todo momento na tela dos aparelhos celulares e computadores das pessoas, de modo que, como consequência, a informação pessoal ganha cada vez mais valor na condição de produto e moeda de troca. Esta realidade fez com que fosse inevitável a criação de uma norma específica sobre a proteção de dados e apta a assegurar o desenvolvimento social saudável, seja no mundo virtual, seja fora dele[173].

Como discorrido em linhas volvidas, o arcabouço legal concernente à proteção de dados não teve início recentemente, tampouco é limitado a uma ou duas normas. Todavia, todas as legislações editadas com objetivos relacionados com este fim conduziram à elaboração da Lei Geral de Proteção de Dados, que é mais completa e disciplina uma quantidade maior de pontos relacionados com a temática, consoante demonstrar-se-á doravante.

2.6.1 LGPD

Consoante a doutrina pesquisada, em especial Machado, Santos e Paranhos[174], a Lei Geral de Proteção de Dados brasileira foi fortemente influenciada pela legislação europeia, com enfoque para a norma denominada *General Data Protection Regulation*.

---

[172] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022. p. 293-294.

[173] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

[174] MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos; PARANHOS, Mario Cosac Oliveira. **LGPD e GDPR:** uma análise comparativa entre as legislações. 2018. Disponível em:

Diante disto, antes de tratar especificamente da norma brasileira, é interessante fazer alguns apontamentos quanto à GDPR, a fim de compreender o motivo pelo qual foi utilizada como inspiração para a legislação brasileira.

2.6.1.1 Principais pontos da GDPR

Há décadas existe uma significativa discussão acerca da ingerência de terceiros e do Estado na vida privada das pessoas e de sua autonomia informacional, o que constantemente faz parte da pauta das discussões da Comunidade Europeia e da União Europeia há muitos anos[175].

Monteiro[176] argumenta que a Lei Geral de Proteção de Dados teve como principal inspiração a GDPR, tendo como finalidade precípua não apenas a regulação dos dados pessoais, mas, ainda, levar ao desenvolvimento econômico e tecnológico, a fim de criar-se um mecanismo apto a salvaguardar e implementar regras relativas ao tratamento dos dados pessoais. Um dos objetivos da legislação, portanto, é gerar um equilíbrio entre o ambiente de negócios e aa sociedade.

A norma inspiradora da LGPD, ou seja, o GDPR, foi elaborada em resposta à necessidade de se modernizar a legislação, ao introduzir novas tecnologias às rotinas das empresariais. A GDPR teve como intuito principal reforçar e unificar as determinações quanto à proteção de dados pessoais na União Europeia, por intermédio de uma adequação dos princípios à sociedade informatizada, com destaque para o progressivo crescimento da coleta e tratamento de dados pessoais físicos ou digitais, no ambiente da internet ou não[177].

No mesmo sentido:

> A Lei geral de proteção de dados – LGPD foi criada sob a influência do Regulamento Geral sobre a Proteção de Dados - GDPR, que consiste em um regulamento do direito europeu de proteção de dados pessoais dentro da união europeia. Em virtude dos crescentes episódios de manipulação indevida e vazamento

---

https://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acesso em: 12 jan. 2021.

[175] POLIDO, Fabrício B. Pasquot et al. **Instituto de Referência em internet e sociedade:** GDPR e suas repercussões no direito brasileiro. 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-IRIS-1.pdf. Acesso em: 12 jan. 2021.

[176] MONTEIRO, Renato Leite. **Existe um direito à explicação na lei geral de proteção de dados do Brasil.** 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 19 jan. 2022.

[177] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

> de dados no mundo virtual, fez-se necessária a criação de normas que pudessem regulamentar o acesso a esses dados de forma a assegurar a privacidade dos usuários[178].

Vê-se, assim que o legislador brasileiro, diante da inegável necessidade de se criar uma legislação específica e mais completa para disciplinar a questão da proteção de dados, buscou inspiração no arcabouço legal de outras nações.

Miragem[179], também comentou que, dentre as diversas influências à LGPD, se destacam sobremaneira as normas extraídas do modelo europeu de proteção de dados, principalmente aquelas encartadas no Regulamento Geral de Proteção de Dados (Regulamento 2016/679), a qual substituiu a Diretiva 46/95/CE, acerca do tratamento de dados pessoais, e a Convenção 108, do Conselho da Europa, de 1981, que abordava a proteção das pessoas no que tange ao tratamento automatizado de dados pessoais. Entrementes, não se pode ignorar a influência de outros sistemas jurídicos, internacionais e das normas brasileiras.

Ao comentar sobre a legislação europeia de proteção de dados, Machado, Santos e Paranhos[180] sustentaram que o ponto principal é o caráter de evolução da Diretiva Europeia do ano de 1995, o que conduz à constatação de que a legislação protetora dos danos já existia no legislativo europeu há cerca de 25 anos. Este fato demonstra que a Europa se destaca como uma cultura com uma evolução maior no que diz respeito à proteção de dados.

A legislação europeia de 1995 se tornou cada vez mais forte com o passar das décadas. Isto implica dizer que o país considera que contar com uma lei de proteção significa que a nação assegura a proteção mínima de informações, por intermédio de princípios como transparência, finalidade, uso necessário e outros[181].

De acordo com a explanação de Polido et al.[182], a abrangência da GDPR, assim como a ambição legislativa e a maturidade conceitual revelam que se trata de um autêntico

---

[178] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021. p. 11.

[179] MIRAGEM, Bruno. A lei geral de proteção de dados (Lei 13.709/2018) e o direito de consumidor. **Revista dos Tribunais,** v. 1009, nov. 2019. Disponível: https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 20 jan. 2022.

[180] MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos; PARANHOS, Mario Cosac Oliveira. **LGPD e GDPR:** uma análise comparativa entre as legislações. 2018. Disponível em: https://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acesso em: 12 jan. 2021.

[181] VENTURA, Ivan. **A relação entre a lei de proteção de dados e o ingresso do Brasil no OCDE.** mar. 2019. Disponível em: https://www.consumidormoderno.com.br/2019/03/20/relacao-lgpd-desejo-brasil-ocde/. Acesso em: 03 fev. 2022.

[182] POLIDO, Fabrício B. Pasquot et al. **Instituto de Referência em internet e sociedade:** GDPR e suas repercussões no direito brasileiro. 2018. Disponível em: https://irisbh.com.br/wp-

regulamento-modelo, apto a espelhar outras iniciativas nacionais, regionais e intracomunitárias, na busca por padrões normativos uniformes na proteção de dados pessoais.

> Não seria exagero afirmar que o GDPR nasce como 'monstro normativo'2, um Leviatã a induzir condutas de conformidade ('compliance') por parte de agentes nas esferas pública e privada no campo da proteção de dados pessoais e especialmente identificáveis nos ambientes informacional e digital[183].

Não pairam dúvidas, portanto, de que a GDPR inovou bastante a legislação mundial em termos de proteção de dados e trouxe parâmetros bastante interessantes a serem observados por outros países dando a elaboração de suas normas protetivas especiais.

Finkelstein e Finkelstein[184] comentam que o Regulamento Geral de Proteção de Dados Pessoais Europeu trouxe consigo novo entendimento sobre a proteção de dados pessoais, de modo que expandiu sua abrangência para além do próprio território europeu. Implica, então, num modo sistemático de proteção das pessoas singulares, em relação ao tratamento de dados pessoais e à livre circulação destes. Ressalta-se que o GDPR tem caráter imperativo em todos os seus elementos e aplicação direta em todos os Estados-Membros.

A GDPR é composta por normas que visam a orientar as empresas para que elas consigam ofertar seus produtos ou serviços e, ainda assim, assegurar a privacidade e *compliance*. Ademais, tem o condão de favorecer as condições para que que não apenas os sistemas de tratamento dos dados, a exemplo de bancos de dados, sejam desenvolvidos considerando todos os princípios da GDPR[185].

Ao procederem uma análise comparativa entre a LGPD e a GDPR, Finkelstein e Finkelstein[186] pontuam que os objetivos apresentados pela GDPR são condizentes com os da Lei nacional, com vistas a, também, garantir direitos fundamentais de pessoas naturais, por meio da proteção de dados. A legislação alienígena que serviu de parâmetro para a LGPD é

---

content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-IRIS-1.pdf. Acesso em: 12 jan. 2021.

[183] POLIDO, Fabrício B. Pasquot et al. **Instituto de Referência em internet e sociedade:** GDPR e suas repercussões no direito brasileiro. 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-IRIS-1.pdf. Acesso em: 12 jan. 2021. p. 4.

[184] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

[185] LANGEN, Talita da Silva Carlos. **Lei geral de proteção de dados:** diagnóstico do grau de conformidade de micro e pequenas empresas. 2020. 137f. Dissertação (Mestrado em Administração de Micro e Pequenas Empresas) - Centro Universitário Campo Limpo Paulista, Campo Limpo Paulista, 2020.

[186] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

bastante concisa e minuciosa, no que tange aos seus conceitos. Para exemplificar, cita-se o fato de que a GDPR classifica os tipos de dados em pessoais e pessoais sensíveis, além de abordar a existência de dados genéticos, biométricos e os relativos à saúde.

A legislação modelo prevê sanção para o descumprimento dos preceitos da GDPR, o que chega a 20 milhões de euros ou a 4% do faturamento anual da empresa que infringiu a norma. Semelhantemente, a norma brasileira, introduziu a regulação estatal sobre uma realidade peculiar da contemporaneidade. A ética autorregulada observada nos operadores das redes digitais e nas empresas de marketing da era digital atingiu um novo patamar e precisa se ajustar à nova realidade[187].

2.6.1.2 Lei Geral de Proteção de Dados Brasileira

Consoante comentou-se alhures, o Brasil não foi pioneiro a elaborar uma lei que trate especificamente da proteção de dados pessoais, pois, ao entrar a LGPD em vigor neste país, diversas outras nações já contavam com uma legislação exclusiva para este fim[188].

Um programa de segurança de dados se faz de suma importância para se assegurar que os dados não sejam violados nas empresas, posto que elas fornecem e tratam dados pessoais diariamente. Para corroborando com tal firmação, destaca-se que existem diversos relatos de empresas em vários países que tiveram seus dados expostos, situação também verificada no Brasil[189].

A temática da proteção de dados se tornou foco quando o Brasil revelou seu interesse em ingressar na OCDE – Organização para a Cooperação e Desenvolvimento Econômico, conhecido como “clube de países ricos”. Assim ocorreu porque a criação de lei específica para este fim implica em segurança dos dados, que é um dos requisitos para o ingresso no mencionado grupo[190].

---

[187] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

[188] PANEK, Lin Cristina Tung. **Lei geral de proteção de dados nº 13.709/2018:** uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019. 35f. Monografia (Curso de Direito) - Universidade Federal do Paraná, Curitiba, 2019.

[189] SCHIRMER, Dara Luana; THAINES, Aleteia Hummes. A implementação da Lei Geral de Proteção de Dados nas rotinas dos profissionais da área contábil: percepções dos contabilistas associados à associação dos contabilistas do Vale do Paranhana/RS. **Revista Eletrônica de Ciências Contábeis,** v. 10, n. 1, p. 31-56, 2021. Disponível em: https://seer.faccat.br/index.php/contabeis/article/view/1956. Acesso em: 15 jun. 2022.

[190] GOMES, Heloisa dos Santos. **Lei geral de proteção de dados (LGPD):** uma análise dos impactos da lei na cultura e tratamento de dados no Brasil. 2019. 28f. Monografia (Curso de Tecnologia em Análise e Desenvolvimento de Sistemas) - Universidade do Sul de Santa Catarina, Florianópolis, 2019.

Consoante explana Cruz[191], no Brasil o marco inicial da proteção de dados foi a entrada em vigor da Lei 12.965, no ano de 2014, por meio da qual o legislador trouxe regras sobre o uso da internet no país. Contudo, esta norma não foi suficiente para abranger o volume e a diversidade de demandas envolvendo uso de dados pessoais que surgiram.

Assim é porque a Lei nº 12.965/14 tem artigos que tratam especificamente da proteção à confidencialidade e inviolabilidade da vida privada digital e o tráfego de informações via Internet. Ademais a norma conhecida como marco civil da internet também garante que a guarda e disponibilização de registros de conexão e de acesso a aplicações a internet respeitem a intimidade, honra e imagem das pessoas. Para ilustrar, o texto do art. 7º, exige o consentimento expresso do usuário para coleta, uso, armazenamento e tratamento de dados pessoais[192].

Sublinha-se que, enquanto a Lei nº 12.965/14 possibilita somente o tratamento de dados pessoais, por meio do consentimento do titular dos dados, a LGPD arrola as hipóteses para o tratamento de dados, no que se insere o consentimento, o interesse legítimo do controlador ou de terceiros, a necessidade de cumprir o contrato ou de obrigação legal ou regulatória[193].

Blum e López[194] comentam que, inicialmente os artigos 6º, III, e 31, §1º, da Lei de Acesso à Informação estabeleceram que, via de regra, deve existir previsão legal ou consentimento do titular dos dados. Posteriormente, a Lei Geral de Proteção de Dados veio para complementar esta disposição.

> A Lei Geral de Proteção de Dados surge no ordenamento jurídico brasileiro dentro da perspectiva de fortalecimento das relações democráticas com os cidadãos, construídas a partir da Constituição Federal, notadamente com a Lei do *Habeas Corpus* e a Lei do Acesso à Informação. Em uma sociedade de informação, saber é poder. A transparência sobre o tratamento dos dados pessoais sobre os quais se sabe implica necessariamente o compartilhamento do poder detido, pois comprova pela clareza a legalidade das ações realizadas pelo Poder Público. Nessa perspectiva, a

---

[191] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.

[192] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

[193] MATTOS FILHO, Veiga; QUIROGA JUNIOR, Marrey. **Guia para a Lei Geral de Proteção de Dados.** ago. 2018. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Acesso em: 12 jan. 2021.

[194] BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. **Cadernos Jurídicas,** a. 21, n. 53, p. 171-177, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_7_cadernos_juridicos_epm.pdf?d=637250348268501368. Acesso em: 22 jan. 2022.

> Lei Geral de Proteção de Dados é um passo à frente em nossas relações democráticas[195].

A Lei nº13.709, de 14 de agosto de 2018, ficou conhecida popularmente como Lei Geral de Proteção de Dados ou LGPD, cuja norma legal objetiva, principalmente, garantir a segurança de dados pessoais, bem como alterar substancialmente a Lei nº 12.965/2014, chamada de Marco Civil da Internet[196].

Gomes[197] pondera que o foco da LGPD é, precisamente, ter-se uma legislação específica sobre a segurança e privacidade de dados, bem como para regulamentar e fiscalizar a forma como as empresas coletam, armazenam e utilizam os dados coletados.

A LGPD traz os parâmetros para o tratamento de dados pessoais, com ênfase para os meios digitais, por pessoa natural ou pessoa jurídica de direito público ou privado. O intuito principal desta norma é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[198].

Ou seja, a legislação especial visa a possibilitar que o cidadão tenha um controle maior sobre o tratamento que é dado às suas informações pessoais. Isto implica dizer que a Lei buscar dar aos cidadãos, consumidores e titulares uma maior confiabilidade na coleta, uso e privacidade de seus dados[199].

No âmbito da sociedade atual, a proteção de dados ganhou bastante relevância, especialmente porque o compartilhamento de informações ocorre de modo instantâneo, em que são repassadas e utilizadas desprovido do necessário cuidado. A Lei Geral de Proteção de Dados Pessoais se apresenta como um mecanismo que visa a padronizar e garantir que os dados fornecidos sejam tratados de forma segura e transparente[200].

---

[195] BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. **Cadernos Jurídicas,** a. 21, n. 53, p. 171-177, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_7_cadernos_juridicos_epm.pdf?d=637250348268501368. Acesso em: 22 jan. 2022. p. 177.

[196] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.

[197] GOMES, Heloisa dos Santos. **Lei geral de proteção de dados (LGPD):** uma análise dos impactos da lei na cultura e tratamento de dados no Brasil. 2019. 28f. Monografia (Curso de Tecnologia em Análise e Desenvolvimento de Sistemas) - Universidade do Sul de Santa Catarina, Florianópolis, 2019.

[198] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 03 jan. 2021.

[199] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.

[200] SCHIRMER, Dara Luana; THAINES, Aleteia Hummes. A implementação da Lei Geral de Proteção de Dados nas rotinas dos profissionais da área contábil: percepções dos contabilistas associados à associação dos

Consoante Finkelstein e Finkelstein[201], a criação de uma norma legal específica sobre a privacidade de dados virtuais acabou por se tornar uma condição para que o Brasil consiga fazer parte, como país-membro, da Organização para Cooperação e Desenvolvimento Socioeconômico, o que ensejou um maior empenho na elaboração da norma e enfatizou a importância econômica dela.

Sobre o ensejo da criação da LGPD, Ventura[202] explicou que:

> Países que desejam ingressar na OCDE precisam cumprir requisitos técnicos e até político-diplomáticos. Há também uma longa jornada legislativa. É preciso aprovar nada menos que 245 instrumentos legais (leis ou princípios) que endossem os princípios defendidos pela Organização, sendo que um deles é justamente a proteção de dados pessoais. Na América do Sul, países como o Chile (membro da Organização desde 2010), Colômbia (o pedido já foi aceito, mas o ingresso depende da aprovação do pleito no congresso colombiano).

A LGPD conta com 65 artigos, divididos em 10 capítulos. O texto desta lei entrou em vigor em setembro de 2020 (com exceção da atuação da Autoridade Nacional de Proteção de Dados).

A Lei no 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais cria determinações e salvaguardas ao uso de dados pessoais no país e, com este objetivo, traz disposições sobre a proteção de privacidade e prevê a realização de processo sistemático para a avaliação de riscos à privacidade[203].

Ao tratar das principais garantias que a LGPD traz, Shores e Oliveira[204] criaram um quadro que elucida com bastante clareza o assunto, consoante se vê da figura 2:

---

contabilistas do Vale do Paranhana/RS. **Revista Eletrônica de Ciências Contábeis,** v. 10, n. 1, p. 31-56, 2021. Disponível em: https://seer.faccat.br/index.php/contabeis/article/view/1956. Acesso em: 15 jun. 2022.

[201] FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

[202] VENTURA, Ivan. **A relação entre a lei de proteção de dados e o ingresso do Brasil no OCDE.** mar. 2019. Disponível em: https://www.consumidormoderno.com.br/2019/03/20/relacao-lgpd-desejo-brasil-ocde/. Acesso em: 03 fev. 2022. s./p.

[203] MACHADO, Matheus Fogaça. **Medidas de proteção de dados pessoais no planejamento e operação de SMART grid utilizando computação em nuvem:** estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil. 2019. 117f. Dissertação (Mestrado em Planejamento e Governança Pública) - Universidade Tecnológica Federal do Paraná, Curitiba, 2019.

[204] SHORES, Robert Daniel; OLIVEIRA, André. **Conhecendo a lei geral de proteção de dados do Brasil – LGPD.** Disponível em: https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf. Acesso em: 11 jan. 2022.

Fonte: Shores e Oliveira[205].

Figura 2. Garantias da LGPD.

Para Schirmer e Thaines[206], a garantia dos direitos dos titulares é composta pelos princípios que a LGPD determina, este que, de acordo com a Lei n. 13.709, são os seguintes: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Mattos Filho e Quiroga Junior[207] comentam que os princípios que a LGPD estabelece trazem novas diretrizes e limites relacionados com os dados pessoais e forma de tratamento deles. Assim, é de fundamental importância a adoção, por parte dos agentes de tratamento, de

[205] SHORES, Robert Daniel; OLIVEIRA, André. **Conhecendo a lei geral de proteção de dados do Brasil – LGPD.** Disponível em: https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf. Acesso em: 11 jan. 2022.

[206] SCHIRMER, Dara Luana; THAINES, Aleteia Hummes. A implementação da Lei Geral de Proteção de Dados nas rotinas dos profissionais da área contábil: percepções dos contabilistas associados à associação dos contabilistas do Vale do Paranhana/RS. **Revista Eletrônica de Ciências Contábeis,** v. 10, n. 1, p. 31-56, 2021. Disponível em: https://seer.faccat.br/index.php/contabeis/article/view/1956. Acesso em: 15 jun. 2022.

[207] MATTOS FILHO, Veiga; QUIROGA JUNIOR, Marrey. **Guia para a Lei Geral de Proteção de Dados.** ago. 2018. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Acesso em: 12 jan. 2021.

medidas efetivas, demonstráveis, a fim de que as operações de tratamento sejam condizentes com os princípios previstos na legislação em questão.

Pormenorizando os princípios da Lei Geral de proteção, tem-se o seguinte:

• Princípio da Finalidade: realizar o tratamento para fins legítimos, específicos, explícitos e informados ao seu titular, sem possibilitar o tratamento posterior de modo incompatível com tais objetivos[208]. Isto significa que, tanto a coleta, quanto o tratamento dos dados, devem expressar clareza e dar ao seu titular informações suficientes para que possa consentir com este processamento. Assim sendo, é vedado qualquer tratamento divergente do acordado;

• Princípio da Adequação: refere-se ao contexto no qual se deu o consentimento do titular para o tratamento dos dados. Ou seja, tem relação com a compatibilidade do tratamento e a finalidade informada ao titular;

• Princípio da Necessidade: concerne à limitação do tratamento e da coleta dos dados ao mínimo necessário, de acordo com a finalidade. Por conta disto, proíbe-se a coleta de dados excessivos e de modo não condizente com a finalidade;

• Princípio do Livre Acesso: assegura aos titulares a facilidade e gratuidade na consulta sobre como os seus dados são tratados, além de ter acesso à informações quanto ao tempo e a finalidade do uso destes dados;

• Princípio da Qualidade dos Dados: traz definições referentes à fidelidade dos dados, transparência acerca da atualização e importância, conforme a necessidade e a finalidade para os quais coletaram os dados;

• Princípio da transparência: assegura clareza nas informações, além de precisão e facilidade de acesso pelos titulares dos dados;

• Princípio da segurança: estipula que os dados devem ser armazenados de modo seguro, com o uso de técnicas variadas, a fim de evitar o acesso indevido dos dados pessoais;

• Princípio da Prevenção: tem a ver com a adoção de medidas que visem a prevenir danos ocasionados pelo tratamento de dados pessoais;

• Princípio da não discriminação: traz limites ao tratamento de dados pessoais, de forma que impede seja feito para fins discriminatórios, ilícitos ou abusivos;

---

[208] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 03 jan. 2021.

• Princípio da responsabilização e prestação de contas: as empresas devem comprovar a adoção de medidas eficazes para cumprir todas as regras de proteção dos dados pessoais e comprovar a eficácia destas medidas adotadas.

A LGPD traz em seu bojo a previsão de elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), definida pelo legislador: "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco"[209].

De acordo com Santini et al.[210], no texto da LGPD é interessante destacar o teor do artigo 3°, que determina que a legislação em comento deve ser aplicada para quaisquer tratamentos de dados realizados por pessoa, natural ou jurídica, de direito público ou privado, seja qual for o meio, no país de sua sede ou no que estejam localizados os dados. Isto significa que a legislação tem ampla aplicação, pois atinge qualquer pessoa ou empresa que, porventura, proceda ao tratamento de dados.

Salienta-se que esta legislação tem reflexos, também, no setor econômico, pois influencia diretamente na forma de realizar os controles internos de uma empresa[211]. A LGPD é aplicável, ainda, no âmbito educacional, nos casos de utilização de quaisquer dados sensíveis ou pessoais dos alunos, familiares e responsáveis legais, bem como no que diz respeito aos profissionais da escola (professores, gestores e outros funcionários). Ressalta-se a necessidade de tratamento especial aos dados de crianças (até os 12 anos, consoante previsão do Estatuto da Criança e do Adolescente), cujo armazenamento requer consentimento dos pais ou do representante legal[212].

Quanto à abrangência da LGPD, de acordo com Mattos Filho e Quiroga Junior[213], a norma:

---

[209] BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 03 jan. 2021.

[210] SANTINI, Barbara et al. A eficácia da Lei Geral de Proteção de Dados (LGPD). In: SALDANHA, Paloma Mendes (Org.). **O que estão fazendo com meus dados?** A importância da Lei Geral de Proteção de Dados. Recife: SerifaFina, 2019. p. 19-30.

[211] SANTINI, Barbara et al. A eficácia da Lei Geral de Proteção de Dados (LGPD). In: SALDANHA, Paloma Mendes (Org.). **O que estão fazendo com meus dados?** A importância da Lei Geral de Proteção de Dados. Recife: SerifaFina, 2019. p. 19-30.

[212] CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.

[213] MATTOS FILHO, Veiga; QUIROGA JUNIOR, Marrey. **Guia para a Lei Geral de Proteção de Dados.** ago. 2018. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Acesso em: 12 jan. 2021. p. 9.

> Aplica-se independentemente do meio e/ou forma de tratamento dos dados; ou seja, impõe regras ao tratamento de dados realizado dentro ou fora da internet, utilizando ou não meios digitais.
> Aplica-se a operações de tratamento que ocorrem no território brasileiro, mas também a operações de tratamento que ocorrem fora do país, quando:
> * os dados pessoais forem coletados no Brasil;
> * os dados sejam relacionados a indivíduos localizados no território brasileiro;
> * tiver por objetivo a oferta de produtos e/ou serviços ao público brasileiro.

Percebe-se, assim, que o legislador teve o desejo de ampliar o máximo possível a abrangência de lei protetiva, no afã de garantir maior segurança para os dados pessoas, em virtude de sua importância na sociedade atual.

No entanto, Brasil[214] faz uma crítica severa à LGPD, ao afirmar que "O texto final da Lei nº 13.444/2017 é merecedor de algumas críticas, notadamente em razão de ter se omitido diante da necessidade de criação de normas para a proteção dos dados pessoais que integrarão a Base de Dados da Identificação Civil Nacional -BDICN".

2.7 Normas

O trabalho de adequação às leis gerais de proteção de dado requer grande esforço, além de demandar tempo, investimento em pessoas, alteração na forma como os processos são realizados e aquisição de ferramentas de segurança da informação. Há casos, ainda, que requerem a contratação de serviços especializados de consultoria e de segurança da informação, a exemplo dos testes de vulnerabilidade e análise de código[215].

Mattos Filho e Quiroga Junior[216] comentam que a LGPD não revoga ou obsta a aplicação de normas setoriais, as quais, de igual forma, servem para regulamentar dados pessoais, de modo que, em que pese a vigência da LGPD, permanece a obrigatoriedade de sua obediência.

2.7.1 Normas de gestão

---

[214] BRASIL. Ministério Público Federal. **Sistema brasileiro de proteção e acesso a dados pessoais:** análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília: MPF, 2019. p. 36.
[215] NAKAMURA, Emilio Tissato; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. **Metodologia de avaliação de riscos e medidas de segurança na proteção de dados.** Disponível em: https://sbseg2019.ime.usp.br/anais/197877.pdf. Acesso em: 14 dez. 2021.
[216] MATTOS FILHO, Veiga; QUIROGA JUNIOR, Marrey. **Guia para a Lei Geral de Proteção de Dados.** ago. 2018. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Acesso em: 12 jan. 2021.

No cotidiano das empresas, aplicar as determinações trazidas pela LGPD não é uma tarefa simplória, bem como exige a observância de outros parâmetros, além daqueles trazidos pela citada lei. Para tanto, faz-se necessário que as empresas lancem mão das chamadas normas de gestão. Diante disto:

> É necessário um alinhamento da organização e estrutura geral da gestão com a segurança da informação, isso significa que a segurança da informação precisa ser considerada nas etapas dos projetos de processos, sistemas de informação e controle, de uma forma sistêmica e não isolada, pois um incidente em determinado ponto pode repercutir em outro, observando-se as necessidades da empresa[217].

Neste contexto, a ISO (*The International Organization for Standardization*) e a IEC (*The International Electrotechnical Commission*) desenvolveu uma família de normas, que trazem diretrizes relacionadas à introdução, implementação e manutenção do SGSI, a serem aplicadas numa organização. Ademais, estas recomendações servem como um tipo de base comum no desenvolvimento de práticas e técnicas relacionadas à segurança organizacional, além de estabelecer a confiança nos relacionamentos intra e inter empresariais[218].

Como destaca Giovanini[219], diferentemente do que se observa com relação à LGPD, "as normas ISO têm caráter de atendimento voluntário, ficando a critério de cada empresa adequar-se ou não a seus requisitos".

Esta família de ISOs é composta por um conjunto de normas que especificam os requisitos indispensáveis a um sistema de gestão de segurança da informação, com vistas à gestão dos riscos, métricas e diretrizes de orientação para a implantação de um sistema de gestão de segurança da informação[220].

---

[217] PESSOA, Larissa Rocha de Paula. **Os desafios da governança de dados e a realidade cultural brasileira.** 2021. 152f. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2021. p. 121.
[218] CORREIA, Carlos Manuel Rosa. **Plano de implementação da norma ISSO /IEC 27001 no INEM.** 2016. 110f. Dissertação (Mestrado em Gestão de Informação) – Instituto Superior de Estatística e Gestão de Informação, Lisboa, 2016.
[219] GIOVANINI, Wagner. **Entenda a diferença entre a LGPD e a ISO 27.701.** 2021. Disponível em: https://www.compliancetotal.com.br/conteudos/detalhe/302/entenda-a-diferenca-entre-a-lgpd-e-a-iso-27-701. Acesso em: 9 fev. 2022. s./p.
[220] CORREIA, Carlos Manuel Rosa. **Plano de implementação da norma ISSO /IEC 27001 no INEM.** 2016. 110f. Dissertação (Mestrado em Gestão de Informação) – Instituto Superior de Estatística e Gestão de Informação, Lisboa, 2016.

Salienta-se que as Normas de Sistemas de Gestão ISO, inclusive aquelas específicas para determinado setor, são elaboradas com o objetivo de serem implementadas de modo separado ou como um Sistema de Gestão combinado[221].

De acordo com a explanação de Freire et al.[222]:

> A Associação Brasileira de Normas Técnicas – ABNT é uma entidade sem fins lucrativos que possui muita credibilidade, sendo ela a única representante do país reconhecida pelo CONMETRO no ano de 1992, sendo membro e participado ativamente da construção da ISO (*International Organization for Standardization*), da COPANT (Comissão Panamericana de Normas Técnicas) e da AMN (Associação Mercosul de Normalização).

Define-se normalização como a atividade que constitui, no que diz respeito aos problemas existentes ou passíveis de ocorrerem, prescrições que visem à utilização comum e recorrente, com o objetivo de se obter um grau ótimo de ordem, num determinado contexto. Isto induz à constatação de que o objetivo geral da associação é otimizar os serviços e solucionar problemas que afetam os diversos setores[223].

Dentre as normas relacionadas a um Sistema de Gestão de Segurança da Informação (SGSI), as mais conhecidas são: a ISO 27001, que traz um modelo a ser seguido no estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoramento do SGSI (Sistema de Gestão de Segurança da Informação); e a ISO 27002, que expressa os objetivos de controles de segurança, os quais devem ser implementados pelos responsáveis pelo SGSI, conforme a aplicabilidade e resultados da análise de riscos, bem como os requisitos de segurança identificados no contexto específico[224].

> A informação é fundamental no apoio às estratégias e processos de tomada de decisão, bem como no controle das operações empresariais. Sua utilização representa uma intervenção no processo de gestão, podendo, inclusive, provocar mudança organizacional, à medida que afeta os diversos elementos que compõem o sistema de gestão. Esse recurso vital da organização, quando devidamente

---

[221] ABNT. Associação Brasileira de Normas Técnicas. **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. 2019. Disponível em: https://www.normas.com.br/autorizar/visualizacao-nbr/11548. Acesso em: 7 fev. 2022.

[222] FREIRE, Gianfrancesco Ranieri D.A. et al. **Gestão da informação e do conhecimento, segurança da informação e normalização:** diferentes perspectivas para unidades de informação. 2012. Disponível em: https://brapci.inf.br/index.php/res/download/86511. Acesso em: 22 jan. 2022. p. 38.

[223] ABNT. Associação Brasileira de Normas Técnicas. **Normalização.** 2011. Disponível em: http://pwt.net.br/site/o-que-e-normatizacao-segundo-a-abnt/. Acesso em: 7 fev. 2022.

[224] NAKAMURA, Emilio Tissato; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. **Metodologia de avaliação de riscos e medidas de segurança na proteção de dados.** Disponível em: https://sbseg2019.ime.usp.br/anais/197877.pdf. Acesso em: 14 dez. 2021.

> estruturado, integra as funções das várias unidades da empresa, por meio dos diversos sistemas organizacionais[225].

O principal objetivo destas normas é ajudar as organizações a manter os seus ativos de informação, de forma segura, tais como, informações financeiras, propriedade intelectual, dados pessoais dos colaboradores, dos clientes, dos utentes ou informação que foi confiada a terceiras entidades[226].

De acordo com Pessoa[227], as normas de gestão se destacam por fornecer "*standards* internacionais capazes de atender o dispositivo legal e concretizar o princípio da segurança da informação, ou seja, complementam a Lei Geral de Proteção de Dados Pessoais no que diz respeito à segurança e sigilo dos dados".

Em virtude do progresso representado pelo advento de Novas Tecnologias da Informação e Comunicação (NTICs), surgiram, para a gestão da informação, outras ferramentas, utilizadas para desenvolver seus processos de modo mais eficaz, de forma que as empresas passaram a utilizar novos sistemas de informação, com o intuito de tornar mais fácil o acesso aos dados[228].

Silvieri[229] pondera que o Sistema de Gestão de Segurança da Informação, que tem por base a ABNT NBR ISO/IEC 27001, foi criado com o intuito de possibilitar a adição de requisitos específicos para os setores, sem precisar desenvolver um novo Sistema de Gestão.

Em virtude dos objetivos propostos para o presente estudo, optou-se por abordar, especificamente, a ISOs 27000/2019 e 27701/2019, das quais tratar-se-á nos itens que seguem.

---

[225] BEUREN, Ilse Maria. **Gestão da informação:** um recurso estratégico no processo de gestão empresarial. 2. ed. São Paulo: Atlas, 2000. p. 43.

[226] CORREIA, Carlos Manuel Rosa. **Plano de implementação da norma ISSO /IEC 27001 no INEM.** 2016. 110f. Dissertação (Mestrado em Gestão de Informação) – Instituto Superior de Estatística e Gestão de Informação, Lisboa, 2016.

[227] PESSOA, Larissa Rocha de Paula. **Os desafios da governança de dados e a realidade cultural brasileira.** 2021. 152f. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2021. p. 120.

[228] FREIRE, Gianfrancesco Ranieri D.A. et al. **Gestão da informação e do conhecimento, segurança da informação e normalização:** diferentes perspectivas para unidades de informação. 2012. Disponível em: https://brapci.inf.br/index.php/res/download/86511. Acesso em: 22 jan. 2022.

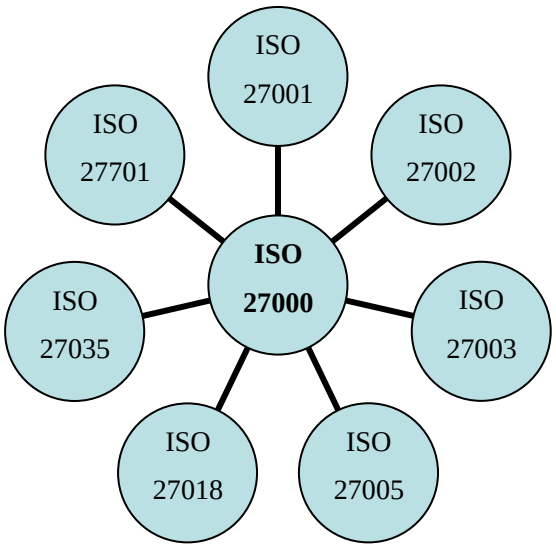
[229] SIVIERI, Edson Vicente. **Estruturação do departamento de segurança da informação para atender a gestão de dados em conformidade à lei geral de proteção de privacidade de dados (LGPD)**. 2021. 37f. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/20088/1/TCC_Edson_Sivieri.pdf. Acesso em: 11 dez. 2021.

2.7.2 ISO 27000:2019

As normas ISO/IEC 27000 expressam padrões de segurança da informação, publicados em conjunto, pela *International Organization for Standardization* e pela *International Electrotechnical Commission*[230].

Trata-se de recomendações de práticas consideradas mais adequadas, acerca do gerenciamento da segurança da informação, o que envolve a gestão dos riscos, por intermédio de controles, no contexto de um Sistema de Gestão de Segurança da Informação (SGSI). Estas normas apresentam uma estrutura bastante parecida com os sistemas de gestão, a fim de assegurar a qualidade (série ISO 9000), de proteção ambiental (série ISO 14000) e outros sistemas de gerenciamento.

A família ISO 27000 possui uma série de normas, que fornecem uma estrutura de apoio para proteção e privacidade de dados. A figura 3 apresenta algumas destas normas, relevantes num contexto de necessidade de adquação no tratamento dos dados pessoais no país, sendo imprescindível para todos os segmentos, em consônancia com a LGPD.



Fonte: Elaborada pela autora.

Figura 3. Família ISO 27000.

A ISO 27000 traz principios e aborda o vocabúlario da segurança da informação. A norma 27001 está relacionada aos requisitos para desevolver, implementar, operar de foma

[230] AZEVEDO, Gleyson. **Gestão de segurança da informação I.** Disponível em: https://free-content.direcaoconcursos.com.br/demo/curso-8913.pdf. Acesso em: 25 jan. 2022.

contínua, um SGSI (Sistema de Gestão de Segurança da Informação); a 27002 específica códigos de boas práticas, com direcionamento de aplicação dos controles da ISO 27001; a ISO 27005 aborda a gestão dos riscos à segurança da informação; a 27018 adota mecanismos para a proteção dos dados em nuvem; e a norma 27035 trata da gestão de incidentes de segurança da informação e oferece requistos a serem aplicados como suporte, para atender a lei de proteção de dados. Ressalta que a ISO 27701 também trata da questão da violação de dados.

Em síntese a família de normas ISO/IEC 27000, inclui normas para:

> a) definir os requisitos para um SGSI;
> b) prestar apoio direto, orientação e / ou interpretação detalhada para o processo global de estabelecer, implementar, manter e melhorar um SGSI;
> c) fornecedor orientações setoriais e específicas para SGSI;
> d) endereçar diretrizes para realizar auditoria e avaliação de conformidade para SGSI[231].

O modo como se estabelece e implementa o SGSI de uma empresa depende completamente de suas necessidades, objetivos, requisitos de segurança, processos organizacionais adotados, tamanho e estrutura. O SGSI se apresenta como instrumento utilizado para preservar a confidencialidade, integridade e disponibilidade da informação, o que se dá por intermédio da aplicação de um processo de gestão de riscos e garantia às partes interessadas de que estes são devidamente gerenciados[232].

As empresas que adotam os princípios de segurança da informação previstos na ISO 27000 conseguem implementar, otimizar, revisar e fazer análises precisas em relação à gestão da TI. Esta característica ganha ainda mais importância ao considerar que a área de TI ganhou uma importância estratégica nos negócios[233].

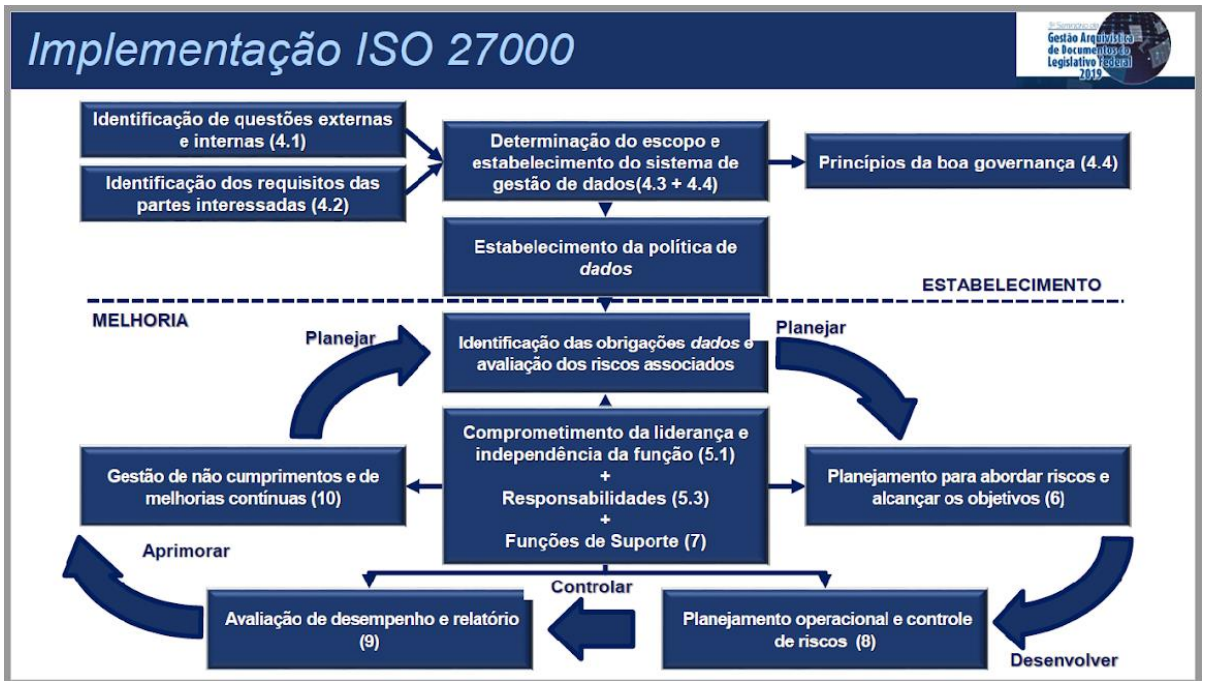
No objetivo de tornar mais claro o processo de implementação da ISO 27000, insere-se ao presente estudo a figura 4, que estampa as etapas de implantação mencionada norma:

---

[231] CORREIA, Carlos Manuel Rosa. **Plano de implementação da norma ISSO /IEC 27001 no INEM.** 2016. 110f. Dissertação (Mestrado em Gestão de Informação) – Instituto Superior de Estatística e Gestão de Informação, Lisboa, 2016. p. 5.

[232] AZEVEDO, Gleyson. **Gestão de segurança da informação I.** Disponível em: https://free-content.direcaoconcursos.com.br/demo/curso-8913.pdf. Acesso em: 25 jan. 2022.

[233] KALENDAE. **Saiba como a ISO 27000 pode ser útil na sua empresa.** Disponível em: https://kalendae.com.br/blog/iso-27000/>. Acesso em: 12 jan. 2021.



Fonte: Luz[234].

Figura 4. Implementação ISO 27000.

O autor supramencionado traz, na figura 4, os passos para a implementação da ISO, do que se extrai tratar-se de um processo bem fundamentado e que envolve a participação de vários setores da organização, a começar pela liderança, de forma que não se mostra possível trabalhar a ISO restrita a um segmento da empresa.

A este respeito, Nakamura, Formigoni Filho e Ide[235] aclaram que:

> Muitas empresas têm adotado a ISO 27000 como *framework* para a segurança da informação, porém a sua implementação, de forma isolada, não garante o integral atendimento às leis gerais de proteção de dados. Fundamentalmente, a família de normas 27000 trata de proteção de informações do ponto de vista da entidade que está implementando o SGSI e não do ponto de vista dos direitos dos indivíduos. É claro que ao proteger as informações da organização, as informações das pessoas também estarão protegidas, porém alguns direitos estabelecidos na legislação não estão contemplados na norma, como por exemplo o direito de ter informações removidas e o consentimento do dono das informações.

Insta destacar que os preceitos encontrados na ISO 27000 funcionam como normas que disciplinam a segurança dos dados. Em meio aos princípios mais importantes desta estão a disponibilidade, a integridade, a confidencialidade e a autenticidade[236].

---

[234] LUZ, Charlley. **Lei geral de proteção de dados.** 2019. Disponível em: https://www12.senado.leg.br/institucional/arquivo/apresentacoes/slide-7a. Acesso em: 21 jan. 2022.

[235] NAKAMURA, Emilio Tissato; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. **Metodologia de avaliação de riscos e medidas de segurança na proteção de dados.** Disponível em: https://sbseg2019.ime.usp.br/anais/197877.pdf. Acesso em: 14 dez. 2021. p. 4.

2.7.3 ISO 27701:2019

A ISO 27701 se apresenta como uma extensão da ISO/IEC 27001, a qual determina que a empresa tem o dever de buscar atender a todos os requisitos e controles da norma base, com vistas à garantia da privacidade de dados pessoais e aos controles adicionais[237].

A respeito, Pessoa[238] comenta que:

> Trata-se de uma verdadeira ampliação aos requisitos previstos na ABNT NBR ISO/IEC 27001:2013, referente à proteção da privacidade dos titulares de dados pessoais, com requisitos e diretrizes, incluindo, expressamente os conceitos de *privacy by design* e o *privacy by default* para "assegurar que processos e sistemas sejam projetados de forma que a coleta e o tratamento de DP (incluindo o uso, divulgação, retenção, transmissão e descarte) estejam limitados ao que é necessário para o propósito identificado".

A norma ISO 27701 traz os requisitos e diretrizes relacionadas ao estabelecimento, implantação, manutenção e melhoria constante de um Sistema de Gestão de Privacidade da Informação, além de fornecer orientações destinadas aos controladores e operadores de dados pessoais. Vale sublinhar que a ISSO 27701 "é aplicável a todos os tipos e tamanhos de organizações, tanto públicas quanto privadas, organizações controladoras e operadoras de dados pessoais e tem relação com as normas técnicas que lhe dão suporte para a implementação da conformidade"[239].

A finalidade da ISO 27701 é ajudar as empresas a demonstrar às agências, órgãos públicos, investidores e sociedade seu empenho para adotar controles eficientes e considerados como as melhores práticas internacionais em proteção de dados[240].

De acordo com a ABNT[241], a ISO 27701 foi editada no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-021), pela Comissão de Estudo de

---

[236] KALENDAE. **Saiba como a ISO 27000 pode ser útil na sua empresa.** Disponível em: https://kalendae.com.br/blog/iso-27000/>. Acesso em: 12 jan. 2021.
[237] FUNDAÇÃO VANZOLINI. **ISO/IEC 27701:** gestão de segurança da informação e privacidade. Disponível em: https://vanzolini.org.br/produto/iso-iec-27701/. Acesso em: 6 fev. 2022.
[238] PESSOA, Larissa Rocha de Paula. **Os desafios da governança de dados e a realidade cultural brasileira.** 2021. 152f. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2021. p. 125.
[239] KOHAN, Sarah. **Entenda a importância da gestão de privacidade da norma ISO 27701.** jun. 2021. Disponível em: https://vanzolini.org.br/produto/entenda-a-importancia-da-gestao-de-privacidade-da-norma-iso-27701/. Acesso em: 12 jan. 2021. p. 1.
[240] MILAGRE, José. **O que é ISO 27701 e como entender a aplicação da norma para gestão da norma para gestão da privacidade da informação em 5 passos.** Disponível em: https://josemilagre.jusbrasil.com.br/artigos/791257034/o-que-e-iso-27701-e-como-entender-a-aplicacao-da-norma-para-gestao-da-privacidade-da-informacao-em-5-passos#:~:text=Deste%20modo%2C%20a%20ISO%2027701,internacionais%20em%20prote%C3%A7%C3%A3o%20de%20dados. Acesso em: 4 jan. 2021.

Técnicas de Segurança (CE-021:000.027) e o projeto que culminou com a edição da ISO em questão circulou em Consulta Nacional, por meio do Edital nº 10, de 04.10.2019 a 07.11.2019.

Como extrai-se da Fundação Vanzolini[242]:

> A norma ISO/IEC 27701 é uma extensão da norma de segurança da informação, a ISO/IEC 27001, para privacidade. A preocupação com a segurança e proteção de dados pessoais vem sendo tema de debates há anos em fóruns globais que envolvem governos, empresas, entidades de classe e sociedade. Em 2018, a União Europeia criou a lei para proteção de dados GDPR (General Data Protection Regulation), que influenciou a lei brasileira. Em seguida, os países do bloco encomendaram para ISO (Organização Internacional de Normalização ou International Organization for Standardization) a criação de uma norma para atender a essa legislação, que resultou na ISO/IEC 27701.

Quanto ao seu campo de aplicabilidade, a norma ISO/IEC 27701 é passível de ser implementada em todo tipo de empresa, seja qual for seu porte ou segmento, onde visa a garantir a segurança da informação e a privacidade de dados pessoais de clientes, fornecedores, funcionários, parceiros e gestores[243].

Destaca-se que a necessidade de segurança e os objetivos comuns às empresas nos tempos modernos apontam para a imprescindibilidade da adoção de um processo organizacional e estruturado de gestão de segurança da informação, que deve ter como parâmetro o requisito da segurança. Frente a isto, é de suma importância implementar um sistema de gestão de segurança da informação pautado nas normas de gestão[244]. Portanto, é realmente imprescindível um programa de compliance para que as empresas consigam garantir a segurança dos dados das pessoas nelas envolvidas.

Por fim, é inconteste que uma política de compliance é capaz de proteger a organização de "danos à reputação, dela e de seus funcionários; do risco regulatório; da ação de órgãos de controle e as correspondentes sanções administrativas, judiciais e os danos de imagem de divulgação dessas sanções"[245].

---

[241] ABNT. Associação Brasileira de Normas Técnicas. **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. 2019. Disponível em: https://www.normas.com.br/autorizar/visualizacao-nbr/11548. Acesso em: 7 fev. 2022.

[242] FUNDAÇÃO VANZOLINI. **ISO/IEC 27701:** gestão de segurança da informação e privacidade. Disponível em: https://vanzolini.org.br/produto/iso-iec-27701/. Acesso em: 6 fev. 2022. s./p.

[243] FUNDAÇÃO VANZOLINI. **ISO/IEC 27701:** gestão de segurança da informação e privacidade. Disponível em: https://vanzolini.org.br/produto/iso-iec-27701/. Acesso em: 6 fev. 2022. s./p.

[244] PESSOA, Larissa Rocha de Paula. **Os desafios da governança de dados e a realidade cultural brasileira.** 2021. 152f. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2021.

[245] SILVA, Kátia Rejane da; LARANJA, Patricia Colona; OLIVEIRA, Adriana Carla Silva de. A importância do *compliance* no plano de gestão do centro de biociências da Universidade Federal do Rio Grande Norte. In:

Em similar sentido, Silva, Lopes e Moura[246] concluiram que, com a colocação em prática de um modelo adequado de compliance, é possível às instituições de ensino aperfeiçoar suas práticas e alcançar um diferencial competitivo, representado pela segurança ofertada quanto aos dados pessoas de seus usuários.

No âmbito específico da UniRV, objeto de avaliação neste estudo, nota-se uma grande preocupação em adotar normas e padrões de comportamento que se adequem ao disposto na legislação que disciplina a proteção dos dados pessoais, em especial porque isto implica em mitigar os riscos atrelados à reputação da instituição.

GUIMARÃES, Patrícia et al. (Org.). **Compliance:** estudos interdisciplinares aplicados na gestão de instituições de ensino superior públicas. Natal, RN: EDUFRN, 2018. p. 27-54. p. 51.

[246] SILVA, Aline Gama da; LOPES, Paloma de Lavor; MOURA, Renan Gomes de; BARBOSA, Marcus Vinicíus. Mecanismos de compliance em instituições de ensino superior. **Revista Valore,** 4. ed. p. 317-330. 2019. Disponível em: https://revistavalore.emnuvens.com.br/valore/article/download/373/274. Acesso em: 02 fev. 2022.

3 METODOLOGIA

Neste capítulo apresenta-se a caracterização da pesquisa proposta e os procedimentos empregados para o desenvolvimento da pesquisa. Assim, no texto abaixo apresentar-se-á a abordagem metodológica, com as etapas que serão adotadas e, por fim, os dados que coletar-se-á para servir como base para o desdobramento do projeto, por meio das práticas da ISO 27701/2019 e fechamento do estudo.

A metodologia utilizada é uma análise comparativa da norma ISO 27701: 2019 e a Lei Geral de Proteção de Dados Pessoais, com base na literatura sobre o assunto, na busca de um direcionamento para a aplicabilidade da Lei e as práticas da norma. Os métodos adotados no estudo incluíram uma revisão bibliográfica sobre a relevância da lei no contexto de proteção de dados pessoais, tanto numa visão econômica em que o país busca preservar suas relações comerciais, bem como a garantia dos direitos dos titulares dos dados com uma clara consonância com a Declaração Universal dos Direitos Humanos no livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais disposto em seu artigo 1º.

A pesquisa contou com três etapas, que foram: identificação do problema, organização documental da pesquisa (referencial teórico) e o desenvolvimento da aplicabilidade da pesquisa, por meio da propositura de um modelo de projeto, a partir das práticas da ISO 27701, para implementação de um programa compliance de proteção de dados à luz da LGPD na Universidade de Rio Verde.

Na etapa de identificação do problema, buscou-se explicar o interesse do desenvolvimento da pesquisa, que teve como base a promulgação da legislação brasileira de proteção de dados pessoais – LGPD (Art. 1º) e a necessidade de que todos os segmentos organizacionais se adequem ao arcabouço legal, inclusive as Instituições de Ensino Superior.

Assim, as IES precisam desenvolver mecanismos para atender aos requisitos da Lei. Entretanto, a aplicabilidade da norma legal por parte das organizações não é uma tarefa tão simples, pois é uma legislação nova, que traz em seu bojo apenas diretrizes para adequação, de modo que fica a parte técnica, atinente à conformidade, a critério das organizações, que devem definir o que realmente precisam fazer para se tornarem compatíveis, além do custo para esta conformidade.

Diante deste cenário, o presente estudo tem como foco a análise da ISO 27701/2019, na condição de definidora de boas práticas de governança da privacidade dos dados por parte das IES.

Na segunda etapa, desenvolveu-se a revisão da literatura, por meio de pesquisas bibliográficas, a fim de buscar material pertinente ao assunto em estudo nas bases de dados EBSCOHost, e Periódicos Capes, Google Acadêmico, RT online, livros e artigos. A busca por material literário visou ao entendimento das diretrizes e processos indicados pela norma ISO 27701, bem como à criação de registros documentais, o que culminou por envolver outras normas da família ISO, a exemplo da 27001, que trata da segurança das informações e a 27002.

Neste estudo utilizou-se as seguintes palavras-chave e operadores Booleanos: Data Protection, ISO 27701 AND GDPR, LGPD AND Higher Education Institutions, Challenges, LGPD, Data, Economic Development AND Data Protection.

A terceira etapa contempla a aplicabilidade da pesquisa, por meio da proposta de um projeto de *compliance,* fundamentado nas cláusulas e subclausulas da ISO 27701/2019, para a gestão dos dados tratados pela Universidade de Rio Verde, a fim de alcançar a conformidade com a legislação em vigor.

Sublinha-se que a proposta a ser apresentada como produto do presente estudo será elaborada com base no ciclo PDCA (*Plan-Do-Check-Act*), este que, consoante explica Alves[247] é formado pelas seguintes etapas: Planejar (PLAN), Executar (DO), Verificar, (CHECK) e Agir (ACTION). Trata-se de uma ferramenta de gestão que tem como objetivo a melhoria e o controle dos processos rotineiros. A escolha por esta ferramenta justifica-se pela constatação de que as normas ISO e os sistemas de gestão costumam adotar o PDCA como estrutura de base, a fim de garantir a interligação entre as normas a serem utilizadas.

3.1 Caso (UniRV)

Com a necessidade de fazer adequações na instituição de ensino Universidade de Rio Verde - UniRV e integrá-la a uma ordem superior, neste particular às exigências da Lei Geral de Proteção de Dados – (LGPD), buscou-se reunir elementos para embasar um projeto de compliance, tendo como base as práticas da ISO 27701 para a governança dos dados tratados pela UniRV.

A Universidade onde fora realizada o estudo é uma Fundação Pública de Direito Público Municipal. Foi criada pela Prefeitura Municipal de Rio Verde – GO por meio da Lei Municipal nº. 1.221/1973, modificada pela Lei Municipal nº. 1.313/1974 para Fundação do

[247] ALVES, Érika Andrade Castro. O PDCA como ferramenta de gestão da rotina. 2015. Disponível em: https://www.inovarse.org/sites/default/files/T_15_017M_7.pdf. Acesso em: 15 jun. 2022.

Ensino Superior de Rio Verde – FESURV e posteriormente modificada pelas Leis Municipais nº. 4.541/2003 e 4.802/2004 para FESURV – Universidade de Rio Verde.

Por se tratar de uma fundação pública municipal integra a Administração Pública Indireta nos termos do art. 4º inciso II, alínea "d", do Decreto-Lei nº. 200/1967. Logo, todos os Campus da Universidade de Rio Verde possuem a mesma natureza jurídica.

Além do câmpus administrativo, instalado em uma área de 62 alqueires e mais um câmpus em Rio Verde (Centro de Negócios), a UniRV também está presente nas cidades de Aparecida de Goiânia, Caiapônia, Goianésia e Formosa. Hoje são mais de 8100 acadêmicos frequentando um dos 34 cursos de graduação oferecidos em quatro grandes áreas: Ciências Humanas e Sociais; Ciências Exatas e Engenharias; Ciências Biológicas e da Saúde e Ciências Agrárias, 11 cursos de curta duração e 15 cursos de pós-graduação[248].

Na área de Pós-Graduação, destaca-se o mestrado em Produção Vegetal, implantado em 2004, devidamente recomendado pela Capes/MEC e o recentemente implantado mestrado em Direito no Agronegócio[249].

Com uma longa e expressiva trajetória na educação superior, a UniRV construiu uma história diferenciada das demais, a qual se destaca como uma conquista para região Sudoeste e, nos últimos anos, cresceu de forma representativa. Em virtude da consciência da sua importância para a formação do cidadão, bem como do seu compromisso para com a responsabilidade social, a universidade em questão procura não perder de vista a sua missão.

Neste intuito, laborou-se no sentido de identificar o problema e a motivação para execução da pesquisa, os quais se relacionaram com objetivo geral deste estudo, para, assim, propor elementos a serem utilizados na elaboração de um projeto de conformidade com a lei protetiva de dados, com vistas ao *Compliance* com a LGPD, tendo como parâmetro as etapas da metodologia, as quais foram descritas em linhas volvidas.

Outrossim, diante do arcabouço legal de proteção de dados e por se tratar de um departamento essencial para o desenvolvimento das atividades da Instituição, é de fundamental importância que todos os envolvidos na gestão de dados estejam conscientes de sua responsabilidade perante os titulares destes dados, bem como criem uma cultura organizacional de proteção de dados.

---

[248] UNIRV. Universidade de Rio Verde. **Institucional**. Disponível em: http://www.unirv.edu.br/paginas.php?id=12. Acesso em: 18 mar. 2021.

[249] UNIRV. Universidade de Rio Verde. **Institucional**. Disponível em: http://www.unirv.edu.br/paginas.php?id=12. Acesso em: 18 mar. 2021.

Com o intuito de trazer maior clareza acerca da relação existente e necessária entre os preceitos trazidos pela LGPD e as normas práticas apresentadas pela ISO 27701, na sequência, trar-se-á um quadro comparativo e elucidativo a respeito.

4 COMPARATIVO ENTRE A ISO 27701: 2019 e a LGPG

A expansão dos negócios possibilitada pela globalização e pela contínua conectividade via Internet, corroborada, ainda, pelas novas tecnologias, possibilitou um crescimento exponencial do volume e variedade de dados armazenados, processados e transmitidos nas organizações, de modo a gerar um volume e uma variedade de dados muito grande. Contudo, muitas vezes o seu titular não sabe o motivo do uso de seus dados, tampouco quem os utiliza.

A nova dinâmica mundial, que tem os dados como matéria-prima, é essencial para o desenvolvimento da economia, na esfera internacional. Frente a isto, equilibrar a utilização destes dados, sob a ótica dos seus titulares, tornou-se fundamental.

Diante deste cenário, as empresas, a nível global, se esforçam para encontrar um ponto de equilíbrio entre a privacidade dos dados e o aproveitamento das oportunidades comerciais auferidas por estes dados[250]. Assim, governos de vários países criaram ou aperfeiçoaram legislações já existentes, com o intuito de definir como as organizações podem coletar, armazenar e tratar os dados relativos aos cidadãos, em um ecossistema que ofereça segurança aos titulares e, concomitantemente, dê condições para as organizações continuarem a tratar os dados.

Frente a esta problemática, no afã de acarretar segurança e proteção aos dados pessoais no país, o Brasil criou a Lei 13.709/18, que já se encontra em vigência. A norma em comento tem como fundamento o desenvolvimento econômico e tecnológico e a inovação, bem como a livre iniciativa e a livre concorrência.

Entrementes, a implementação de um sistema de conformidade com os diversos arcabouços legais que tratam da proteção e privacidade de dados se apresenta como um grande desafio para indivíduos e organizações, que operam em um ambiente dinâmico e global, caracterizado pela utilização dos recursos tecnológicos da Quarta Revolução Industrial[251].

A ISO/IEC 27701:2019 tem o condão de servir de suporte às organizações, a fim de ajudarem-nas a entrar em conformidade com o GDPR. Destaca-se que a aplicação da ISO

---

[250] PR NEWSWIRE. **Building Trust with Data Security - Why Explorium got** ISO/**IEC** 27701 **certification.** Disponível em: https://web.p.ebscohost.com/ehost/detail/detail?vid=7&sid=ef79619a-4613-4b4e-9e9a-d43b065e4c22%40redis&bdata=JkF1dGhUeXBlPWlwLHNoaWImbGFuZz1wdC1iciZzaXRlPWVob3N0LWxpdmU%3d#AN=202104280000PR.NEWS.USPR.UN55136&db=bwh. Acesso em: 05 mar. 2022.

[251] ANWAR, Memoona Javeria; GILL, Asif Qumer. **Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model.** Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020. Acesso em: 28 jan. 2022.

27701, por meio dos seus controles, fornece às organizações meios para implementar ferramentas de conformidade com a LGPD.

Assim, faz-se necessário desenvolver um comparativo entre os dispositivos elencados na LGPD e os controles dispostos na ISO 27701, com o objetivo de averiguar em que patamar a norma atende às exigências da Lei Geral de Proteção de Dados Pessoais.

Por ter como base um padrão internacional, a certificação ISO se mostra importante em um cenário de transformações, em que a proteção dos dados dos titulares tornou-se obrigatória. Demais disto, é valiosa para clientes, parceiros, autoridade de proteção de dados, gestores, dentre outros, por facilitar a comunicação, transparência e conformidade[252].

O objetivo da correlação entre a ISO e a nora legal é garantir a conformidade da Universidade de Rio Verde com os preceitos da LGPD, no intuito de que a instituição conquiste uma posição de respeito aos direitos dos titulares dos dados pessoais geridos por ela, bem como consiga se destacar no mercado da educação superior como uma instituição que respeita e cumpre a legislação de proteção de dados pessoais, por intermédio da governança e das boas práticas.

A ISO 27701 abarca 29 dos 65 artigos contidos na Lei 13.709/18, os quais são destacados na Quadro 1, ou seja, traz normas que abrangem 44,61% dos comandos da LGPD. Entretanto, carece identificar se o conteúdo da ISO 27701 oferece subsídios capazes de, efetivamente, gerar a conformidade com a LGPD. Assim, o próximo passo é evidenciar um comparativo dos controles da norma com os dispositivos contidos na LGPD.

Estar em conformidade com a Lei representa uma tarefa complexa para as organizações. Todavia, diante deste desafio, a adoção da ISO 27701/2019 se apresenta como um caminho de inovação quanto à privacidade, a fim de garantir que as organizações, independentemente do porte e natureza, estejam preparadas para atender às exigências do mecanismo legal. A lei protetiva arrola obrigações impostas aos controladores e responsáveis pelo tratamento dos dados pessoais, a fim de agregar segurança jurídica, no que tange às relações comerciais. Já a norma ISO 27701 é uma ferramenta de gestão, apta a contribuir para que as organizações alcancem a conformidade com a legislação, por meio de suas cláusulas e subcláusulas.

Sublinha-se que a norma ISO/IEC 27701:2019 traz uma abordagem sobre proteção de dados que difere, em alguns aspectos, da Lei Geral de Proteção de Dados Pessoais. A ISO

---

[252] ANWAR, Memoona Javeria; GILL, Asif Qumer. **Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model.** Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020. Acesso em: 28 jan. 2022.

27701 é uma extensão da ISO 27001, com foco na segurança da informação. A LGPD, por sua vez, trata da segurança da informação como um requisito para a efetivação da proteção de dados, ou seja, com uma visão na privacidade dos dados dos titulares.

A Lei brasileira, promove uma abordagem baseada em riscos amplos e direcionada aos direitos fundamentais de liberdade e de privacidade, assim como ao livre desenvolvimento da personalidade da pessoa natural, elencados na Carta Magna. Por outro lado, a ISO/IEC 27701:2019 traz orientações que visam a descobrir e reduzir os riscos inerentes à segurança da informação.

Merece destaque também, outro aspecto em relação a LGPD e a ISO 27701, que é o fato de que a lei traz um escopo mais amplo e abrange diferentes tipos de dados, em meios físicos (registros em papel) ou digitais, o que abarca os dados estruturados ou não estruturados. Por outro lado, a ISO/IEC 27701:2019 tem como alicerce dados estruturados em ativos de Tecnologia da Informação.

A LGPD determina que os dispositivos de certificação carecem de aprovação pela autoridade supervisora, no caso a Autoridade Nacional de Proteção de Dados – ANPD, esta que cumula a função de fiscalizadora da observância da lei e de seu cumprimento. Já os padrões da ISO têm proteção embasado nos direitos autorais. Em relação à violação de dados, a lei brasileira não estabelece um tempo específico para a comunicação de tal ocorrência, mas diz que dever ser em tempo razoável, assim também a ISO 27701 não trabalha um lapso temporal determinado.

A norma ISO se pauta na confidencialidade, integridade e disponibilidade, com base na segurança das informações, enquanto a LGPD traz à baila a probabilidade da ocorrência do risco e seu impacto. Ressalta que a ISO/IEC 27701 é um padrão, assim sua adesão é opcional, enquanto a lei brasileira é obrigatória para todas as organizações que processam dados. Entrementes, é inegável que a adesão à ISO traz benefícios, por ajudar as organizações a se adequarem aos ditames da lei, ao oferecer mecanismos práticos para a promoção da proteção e privacidade dos dados. Na busca por conformidade com a LGPD, as organizações que optam pela adoção da ISO 27701 fortalecem a sua maturidade e demonstra uma abordagem proativa de proteção e privacidade dos dados.

Diante desta necessidade de as organizações buscarem a conformidade e na busca por clarificar um pouco mais a relação entre os dispositivos da normativa e os da Lei protetiva, traz-se as correlações apontadas no Quadro 1.

Lei Geral de Proteção de Dados Pessoais – LGPD	ISO/IEC 27701
Um arcabouço legal	Uma ferramenta de gestão
Pautada na proteção de dados pessoais	Foco na privacidade
Baseada em direitos com uma visão ampla de riscos voltados para os direitos e liberdades dos titulares dos dados	Traz uma abordagem em risco para garantir a privacidade dos dados
Elencada em princípios e requisitos obrigatórios	Cláusulas opcionais
Documentação disponível e acesso fácil	A documentação é privada e protegida por direitos autorais estritos
Base na probabilidade e gravidade dos riscos	Pautada na confidencialidade, integridade e disponibilidade
Notificação de violação de dados em tempo razoável	Notificação de violação em 72 horas

Fonte: Elaborada pela autora.

Quadro 1. Comparativo entre ISO/IEC 27701:2019 e a LGPD

Vê-se, portanto, que a legislação protetiva traz a imposição de várias condutas direcionadas às organizações que lidam dados pessoais, mas, na prática, apenas os ditames da norma legal não suficientes para colocar em prática seus mandamentos. Neste contexto, exsurge a necessidade de as organizações buscarem mecanismos de efetivar a proteção, no que se encaixam perfeitamente a ISO 27701.

4.1 Elementos da LGPD abordados pela ISO/IEC 27701:2019

A Lei Geral de Proteção de Dados traz uma série de determinações a serem observadas no tocante à gestão de dados pessoais, cujos regulamentos têm caráter obrigatório, consoante já amplamente explanado em linhas volvidas. Todavia, a aplicação prática de todos os mandamentos constante da LGPD requer mecanismos de gestão dos dados.

Neste contexto, desponta a necessidade de utilização de uma metodologia de aplicação prática dos ditames da legislação em comento, de onde surge a necessidade de utilização de uma normatização, como as ISOS.

Frente a isto, a ISO 27701 traz os mecanismos a serem adotados pelas instituições, com vistas a ter a implantação de um sistema de gestão da segurança da informação que leve ao alcance do compliance com os ditames da LGPD. Como a ISO relata na sua parte introdutória, ela "foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão da999 Segurança da Informação – SGSI". Ainda, "pode ser usada para avaliar a conformidade"[253].

Com explicam Anwar e Gill[254] (2020, p.1):

> A proteção dos ativos de informação requer uma abordagem interdisciplinar e capacidades multifuncionais. Nos últimos tempos, a segurança da informação e a conformidade com a privacidade continuam sendo uma tarefa complicada devido ao aumento das restrições regulatórias, mudanças nas legislações e conscientização do público. O recém-publicado padrão de segurança e privacidade da informação ISO/IEC 27701:2019 fornece suporte para organizações que desejam implementar sistemas para dar suporte à conformidade com os requisitos globais de privacidade de dados.

No bojo deste estudo já se falou vastamente sobre o conteúdo, objetivo e importância das ISOs, em especial da 27701. Contudo, como a explanação que se pretende realizar aqui tem como objetivo propor moldes para a gestão de dados no órgão, entendeu-se por bem pormenorizar esta relação existente entre os preceitos jurídicos encontrados na LGPD e as normas constantes da ISO 27701.

É de suma importância realizar-se, ainda que brevemente, a correlação entre as determinações constantes da LGPD e as normas trazidas pela ISO 27701, estas que têm o condão de fornecer "as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI)" e, ainda, "fornece as diretrizes para os controladores de DADO PESSOAL e operadores de DADO PESSOAL que têm responsabilidade e responsabilização com o tratamento de DADO PESSOAL"[255].

O Quadro 2, traz uma análise dos aspectos correlacionados entre a norma ISO 27701/2019 e a LGPD, que podem oferecer base para o *compliance* de proteção de dados:

---

[253] ISO/IEC 27701 DNV AS. **All rights reserved.Privacy Information management system**. Disponível em: https://www.dnv.com/services/iso-iec-27701-privacy-information-management-system-159186. Acesso em: 05 jan. 2021.

[254] ANWAR, Memoona Javeria; GILL, Asif Qumer. **Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model.** Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020. Acesso em: 28 jan. 2022. p. 1.

[255] ISO/IEC 27701 DNV AS. **All rights reserved.Privacy Information management system**. Disponível em: https://www.dnv.com/services/iso-iec-27701-privacy-information-management-system-159186. Acesso em: 05 jan. 2021.

Artigos da LGPD	Descrição dos requisitos da LGPD	Controles ISO 27701	Descrição dos Controles da ISO 27701
Art. 5º X Art. 6º, VII Art. 46 Art. 47 Art. 49	Tratamento dos dados, da segurança e do sigilo de dados, boas práticas e governança de dados	6.5.2.1 6.5.2.2 6.5.3.1 6.5.3.2 6.5.3.3 7.2.3 7.2.4	Classificação das informações Rótulos e tratamento de dados Gerenciamento de mídias removíveis Descarte de mídias Transferência física de mídias Quando o consentimento deve ser obtido Obtendo e registrando o consentimento
Art. 4º, § 3º Art. 5º, XVII Art. 10 III Art. 32 Art. 38	Tratamento de dados pelo poder público	7.2.5	Avaliação de impacto de privacidade
Art. 6º, VII Art. 46 Art. 47 Art. 49	Tratamento dos dados, da segurança e do sigilo de dados, boas práticas e governança de dados	6.3.2.1	Política para uso de dispositivo móvel
Art. 6º, § 1º, III, V	Tratamento de dados – princípios	6.15.1.3	Proteção de registros

	Necessidade Qualidade dos dados Adequação	7.4.1 7.4.3 7.4.4	Limites de coleta Precisão e qualidade Objetivos de minimização de DP
Art. 6º, I, II, III, IV, V, VI, VII, VIII, IX, X Art. 7º, I, II, III, IV, V, VI, VII, VIII, IX, X Art. 37 Art. 41 Art. 46	Atividades de tratamento de dados pessoais - Controlador e Operador	8.3.1 8.4.3 8.5.1	Obrigações para os titulares de DP Controles de transmissão de DP Notificação de solicitações de divulgação de DP
Art. 7º, § 5º, II Art. 8º, § 4º Art. 11 – II 'a' Art. 23 Art. 26, IV Art. 34, I	Dos requisitos para o tratamento de Dados Pessoais; Consentimento; Tratamento de dados sensíveis; Tratamento de dados pelo poder público; Compartilhamento de dados; Proteção de dados do país estrangeiro	7.2.2 7.2.7 7.5.1	Identificação de bases legais Controlador conjunto de DP Identificando as bases de transferência de DP entre jurisdições
Art. 9º, I, II, III, IV, V, VI, VIII Art. 14, § 6º	Acesso às informações pelo titular; Tratamento de dados pessoais de crianças e adolescentes	7.2.1 7.3.1 7.3.2 7.3.3 7.3.6	Identificação e documentação do propósito Determinando e cumprindo as obrigações para os titulares de DP Determinado as informações para os titulares de DP Fornecendo informações aos titulares de DP

		8.2.3	Acesso, correção e/ou exclusão Uso de marcketing e propaganda
Art. 8º, § 5º Art. 9º, § 2º	Consentimento; Tratamento de dados pessoais de crianças e adolescentes	7.3.4 7.3.5	Fornecendo mecanismos para modificar ou cancelar o consentimento Fornecendo mecanismos pra negar o consentimento ao tratamento de DP
Art. 10, I, II Art. 18	Legitimo interesse	8.2.1	Acordos com o cliente
Art. 12 § 3º Art. 32 Art. 46 § 1º Art. 49 Art. 50 Art. 51	Dados anonimizados; Segurança e sigilo dos dados; Das boas práticas de governança; Adoção de padrões técnicos	6.15.1.1	Identificação da legislação aplicável e de requisitos contratuais
Art. 15 I, II, III, IV Art. 16 I, II, III, IV Art. 37 Art. 46	Do término do tratamento de dados; Da segurança e do sigilo dos dados;	8.4.2	Retorno, transferência ou descarte de DP
Art.16 Art. 37	Eliminação de dados; Do controlador e do operador	8.5.3 8.2.6	Registros de DP divulgados para terceiros Registros relativos ao tratamento de DP

Art. 18 § 6º, II Direito do titular de obter informações a respeito dos dados		7.3.7 7.3.8 7.3.9 7.3.10	Obrigação dos controladores de DP para informar aos terceiros Fornecendo cópia de DP tratato Tratamento de solicitações Tomada de decisão automatizada
Art. 23	Tratamento de dados pessoais pelo Poder Público	8.2.2	Propósitos da organização
Art. 33 I, II, III, IV, V, VI, VII, VIII, IX Art. 34, I, II, III, IV, V, VI	Da transferência internacional de dados; Nível de proteção de dados de país estrangeiro	8.5.1 8.5.2	Bases para transferência de DP entre jurisdições Países e organizações internacionais para os quais DP podem ser transferidos
Art. 38 Art.50, §1º	Das boas práticas e governança	5.4.1.2 5.4.1.3	Avaliação de riscos de segurança da informação Tratamento de riscos de segurança da informação
Art. 38	Relatório de impacto	6.2.1.1	Políticas para segurança da informação
Art. 41	Do encarregado pelo tratamento de dados pessoais;	8.5.6 6.3.1.1	Divulgação de subcontratos usados para tratar DP Responsabilidades e papéis da segurança da informação
Art. 39 Art. 41	Operador dever realizar o tratamento conforme orientação do controlador; Do encarregado pelo tratamento de dados	8.5.7 8.5.8	Contratação de um subcontratado para tratar DP Mudança de subcontratado para tratar DP

	pessoais		
Art. 42	Da responsabilidade e do tratamento de dados pessoais	8.3.1	Obrigações para os titulares de DP
Art. 44 Art. 45	Transferência de dados pessoais; Violação do direito do titular no âmbito do Direito do Consumidor	8.2.4 8.2.5	Violando instruções Obrigações do cliente
Art. 46 Art. 47 Art. 49	Da segurança e do sigilo dos dados	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	Registro e cancelamento de usuário Provisionamento para acesso de usuário Procedimentos seguros de entrada no sistema (log-on) Políticas para 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 de operadores de DP Políticas e procedimentos para transferência de informações Acordos de confidencialidade e não divulgação Serviços de aplicação em redes públicas

		6.13.1.1 8.4.1	Proteção dos dados para teste Identificando segurança da informação nos acordos com fornecedores Responsabilidades e procedimentos Arquivos temporários

Fonte: Elaborada pela autora.

Quadro 2. Aspectos correlacionados entre a norma ISO 27701/2019 e a LGPD

De uma análise detida da lei protetiva, vê-se, inicialmente, que, no que tange à segurança no tratamento de dados pessoas, a Lei Geral de Proteção de Dados, no seu art. 5º, X define tratamento dos dados. No art. 6º, arrola os princípios a serem observados no tratamento, com destaque para o inciso VII, que trata da segurança na gestão dos dados. O texto dos arts. 46 e 47 menciona a obrigatoriedade de utilização de medidas técnicas e administrativas de segurança, determinação complementada pela disposição encartada no art. 49, onde impõe que no tratamento dos Dados Pessoais os sistemas devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais. Por fim, no art. 50º §1º encontram-se os requisitos a serem observados no momento de estabelecer regras de boas práticas, abordando, na sequência (§2º I) a implementação o programa de governança em privacidade.

Em contrapartida, no tocante à segurança, sigilo, boas práticas e governança de dados pessoais, a ISO traz, no item 6.3.2.1 que é interessante a organização assegurar o uso de dispositivos móveis que não conduza a um comprometimento de dados pessoais. Em seus itens 6.5.2.1e 6.5.2.2, a ISO diz que o sistema de classificação da informação deve considerar explicitamente os dados pessoais, como parte de todo o sistema, a fim de entender qual dado pessoal a organização trata, onde é armazenado e os sistemas pelos quais ele pode fluir.

Ademais, o ISO orienta, também, que é preciso que a organização assegure que as pessoas estejam conscientes da definição de dado pessoal e saibam como reconhecer uma informação como tal.

No item 6.5.3.1 a norma orienta sobre o uso de mídias removíveis para o armazenamento, cujas mídias devem permitir a criptografa, e as mídias não criptografadas sejam usadas somente quando for inevitável, e em situações onde a mídia e/ou os dispositivos não criptografados forem usados. A norma trata, também, da necessidade de implementação de procedimentos e controles compensatórios (por exemplo, embalagens invioláveis) para tratar os riscos.

Vale aqui ressaltar que:

> A ISO/IEC 27701:2019 promove uma abordagem totalmente baseada em riscos para identificar e reduzir os riscos de segurança da informação aplicáveis ao gerenciamento e armazenamento de PII de ativos de TI. No entanto, o GDPR ocasionalmente se baseia em uma abordagem baseada em risco para abordar riscos mais amplos sobre os direitos e liberdades dos titulares de dados[1].

[1] ANWAR, Memoona Javeria; GILL, Asif Qumer. **Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model.** Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020. Acesso em: 28 jan. 2022. p. 5.

No item 6.5.3.2, orienta sobre o descarte seguro de mídias removíveis armazenadas. Por fim, orienta sobre a necessidade de um sistema para registrar as entradas e saídas das mídias físicas quando mídias físicas são usadas para transferência da informação, bem como que medidas adicionais, como criptografa, sejam implementadas para assegurar que os dados somente possam ser acessados no ponto de destino e não durante o transporte e, por fim, que a organização submeta a mídia física contendo dado pessoal a um procedimento de autorização antes de deixar as suas instalações e que assegure que o dado pessoal não seja acessível para qualquer outra pessoa que não aquelas autorizadas (item 6.5.3.3).

Quanto ao consentimento para o tratamento de dados pessoais, a LGPD traz as regras a serem observadas, nos arts. 7º e 8º, e suas exceções, no art. 11. A este respeito, a ISO 27701 diz que, para estar em *compliance* com a legislação correlata ao tratamento de dados, a organização deve se atentam para as regras atinentes ao consentimento dos titulares, para o que precisa desenvolver uma base para cada atividade do tratamento (item 7.2.2), com a determinação clara das responsabilidades e respectivos papéis, o que deve ser devidamente documentado (item 7.2.7). Ainda, precisa identificar e documentar as bases relevantes para o tratamento dos dados, de forma a desenvolver o *compliance* com respeito a estes requisitos (item 7.5.1).

No tocante à revogação do consentimento para o tratamento dos dados, em virtude de mudanças na finalidade para o tratamento que são incompatíveis com o consentimento original, a lei faculta ao seu titular a revogação do consentimento (art. 8º, § 5 º da LGPD), enquanto que a ISO diz que o mecanismo usado para cancelamento depende do sistema, mas deve guardar relação com os mecanismos usados para a obtenção do consentimento, sempre que possível (ex.: se o consentimento foi dado pelo e-mail, a revogação também pode ser por este canal). Com relação à modificação do consentimento, ela pode ser por meio de imposição de restrições ao controlador para excluir o dado em alguns casos (itens 7.3.4 e 7.3.5).

Quanto ao tratamento de dados pelo Poder Público, a temática é tratada na LGPD nos arts. 4º, § 3º, 5º, XVII, 10º, III, 32 e 38. Já a ISO traz que a organização deve implementar um sistema de avaliação de impacto de privacidade, quando do planejamento de novos tratamentos ou mudanças nele, bem como para a avaliação dos riscos (item 7.2.5), além de abordar a finalidade do tratamento de dados pelos entes públicos e as regras correlatas. Nos arts. 23 e 27 a LGPD trata da transferência de dados do poder público para instituições privadas, inclusive países estrangeiros.

No que concerne aos princípios, necessidade e qualidade do tratamento de dados, disciplinados no art. 6º, §1º, III e V, encontra-se uma correlação nos itens 6.15.1.3, 7.4.1,

7.4.3 e 7.4.4 da ISO 27701, em que a norma trata da retenção de cópias de seus procedimentos e políticas de privacidade associados, por um período definido na programação da organização, inclusive retendo versões anteriores dos documentos, bem como que a coleta dos dados tenha uma limitação relevante, proporcional e necessário, com inclusão da coleta indireta. A ISO também propõe a utilização do princípio de *Privacyby Default*.

Sobre a minimização da imprecisão dos dados pessoais, a ISO orienta a implementar políticas, procedimentos e/ou mecanismos para este fim, o que deve fazer parte da informação documentada e ser aplicado ao longo do ciclo de vida do dado (item 7.4.3). Com relação aos dados anonimizados, indica a documentação de quaisquer mecanismos projetados para implementar os objetivos da anonimização, em um tempo hábil (7.4.4).

Quanto aos papeis do controlador e do operador, mencionados na LGPD, nos artigos 5º, IX, 6º, 7º, 37, 41 e 46, como agentes de tratamentos de dados, a ISO, em análise, no item 8.3.1, indica que devem submeter os dados a uma rede de transmissão e a controles apropriados, projetados para assegurar que os dados alcancem os destinos pretendidos, frente à necessidade de que a transmissão seja controlada, por meio de processos apropriados e sem comprometimento para os devidos destinatários (item 8.4.3). No item 8.5.4, aborda a necessidade de notificar as partes sobre quaisquer solicitações legalmente obrigatórias para a divulgação de dado pessoal, dentro de um prazo acordado e em consonância com um procedimento previamente ajustado.

Com relação ao acesso às informações por parte do titular, pais ou responsável legal por crianças ou adolescentes, e a responsabilização por falhas neste sentido, a fim de cumprir o princípio do livre acesso, a LGPD traz, nos artigos 9º, art. 14, § 6º, as regras a serem observadas, Já a ISO em comento aduz que a organizar deve fazer um documento que declare ao titular, de forma clara, o propósito do tratamento dos dados, o que possibilitará que o consentimento e as escolhas sejam dados adequadamente (item 7.2.1, 7.3.1 e 7.3.2), em cujo documento o controlador deve ser identificado claramente, sendo que a informação, sempre que possível, serão fornecidas no momento da coleta dos dados e permanecerão acessíveis ao titular (item 7.3.3). A ISO aborda, inclusive, o procedimento a ser adotado para a pessoa exercitar seu direito de negar o consentimento (item 7.3.5), bem como para corrigir e excluir ele (item 7.3.6). Ademais, no item 8.2.3 a ISO fala da necessidade de consentimento expresso do titular para a utilização dos dados pessoas para fins de marketing.

Quanto ao legítimo interesse do controlador como fundamento para o tratamento de dados (art. 10, I e II da LGPD) e o direito de o titular obter informações relacionadas aos seus

dados (art. 18 da LGPD), a ISO, no item 8.2.1, orienta que o contrato relativo ao tratamento de dados deve contemplar estes aspectos.

No que diz respeito à anonimação dos dados (art. 12, §3 da LGPD), a possibilidade de a autoridade nacional solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas (art.32 da LGPD), a previsão de adoção de medidas técnicas e administrativas de segurança, por meio de padrões mínimos, regras de obas práticas e governança e adoção de padrões técnicos (arts. 46, 49, 50 e 51 da LGPD), a ISO, no item 6.15.6.1.1, destaca a importância da identificação da legislação aplicável e requisitos contratuais, com a verificação das sanções legais que podem resultar das obrigações contratuais, o que pode servir de base para o contrato com o titular dos dados.

As hipóteses de término do tratamento de dados, a eliminação dos dados e as situações em que é possível sua conservação, abordadas nos arts. 15 e 16 da LGPD, assim como a obrigatoriedade da manutenção do tratamento pelo prazo previsto no contrato, e a necessidade de medidas de segurança contra o acesso indevido ou fatores acidentais passíveis de gerar a destruição, perda ou alteração dos dados (arts. 37 e 46 da LGPD), encontram correlação na ISO, que sugere a implementação de uma política de descarte dos dados pessoais, disponível para o cliente quando solicitado, que englobe a relação antes (item 8.4.2) e, depois do descarte, determina que mantenha os registros necessários para apoiar a demonstração do *compliance* (item 8.2.6). Também orienta quanto à documentação da divulgação de dados para terceiros (ex.: em investigações judiciais ou auditorias) (item 8.5.3).

Sobre o dever de informar aos agentes com os quais compartilhou dados sobre a correção, a eliminação, a anonimização ou o bloqueio dos dados (art. 18, § 6º da LGPD), a ISO 27701 traz os passos apropriados, com base na tecnologia disponível, para informar sobre qualquer modificação ou cancelamento do consentimento (item 7.3.7). A ISO orienta, também, sobre a necessidade de fornecimento de uma cópia do dado tratado em um formato estruturado e usado normalmente, acessível ao titular (itens 738, 7.3.9 e 7.3.10).

Quanto ao tratamento de dados pessoais pelas pessoas jurídicas de direito privado (art. 23 da LGPD), a ISO orienta que o contrato entre a organização e o cliente deve incluir as informações relacionadas a este tratamento, mas não pode ser limitado a ele, além de conter o objetivo e o tempo de duração do serviço (item 8.2.2).

No que tange à transferência internacional de dados pessoais, bem como à avaliação do nível de proteção de dados do país estrangeiro (arts. 33 e 34 da LGPD), a ISO prevê seja documentado o *compliance* como a base para transferência, bem como informe o titular sobre

a transferência (item 8.5.1). Ademais, a norma técnica diz que deve especificar e documentar os países e as organizações internacionais para os quais os dados possam, possivelmente, ser transferidos (item 8.5.2).

No art. 38, a LGPD prevê a elaboração de relatório de impacto à proteção de dados pessoais, pelo controlador e, no art. 50, § 1º, estabelece regras de boas práticas destinadas ao controlador e ao operador. Estes aspectos também são contemplados pela ISO, onde sugere que a organização aplique o processo de avaliação de riscos de segurança da informação para identificar os riscos associados à perda de confidencialidade, integridade e disponibilidade, dentro do escopo do SGPI (itens 5.4.1.2 e 5.4.1.3). A norma sugere, ainda, que a organização produza uma declaração quanto ao apoio e comprometimento para alcançar *compliance* com as regulamentações e legislações de proteção de dados (6.2.1.1).

A LGPD, no seu art. 18, diz que o controlador deve fornecer ao titular uma série de informações relacionadas ao tratamento de seus dados, o que também é abordado pela ISO, ao sugerir que organização forneça ao cliente meios para estar em *compliance* com suas obrigações relativas aos titulares de dados pessoais.

Sobre as possíveis irregularidades no tratamento de dados pessoais (art. 44 da LGPD) e as hipóteses de violação do direito do titular no âmbito das relações de consumo (art. 45 da LGPD), a ISO diz que a organização deve informar ao titular dos dados se ela permite e contribui para a realização de auditorias por parte do cliente ou outro auditor obrigatório, ou de outra maneira acordada (itens 8.2.4 e 8.2.5).

No art. 48 da LGPD o legislador incumbe o controlador de comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança. Sobre esta possibilidade, a ISO diz que convém que os procedimentos a que se refere este trecho da lei incluam notificações relevantes de registros (item 6.13.1.5).

A LGPD aborda a questão do acesso não autorizado e situações acidentais ou ilícitas de destruição, perda, alteração dos dados (art. 46), a obrigação de as pessoas que intervenham em uma das fases do tratamento garantir a segurança da informação, em relação aos dados pessoais, mesmo após o seu término (art 47), bem como a obrigatoriedade de que os sistemas utilizados para o tratamento de dados pessoais sejam estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e nas demais normas regulamentares (art. 49).

Nota-se que os aspectos apontados no parágrafo anterior também são contemplados pela ISO 27701, a qual prevê a adoção de procedimentos para registro e cancelamento de usuários que administrem ou operem sistemas e serviços (item 6.6.2.1); a manutenção de um

registro preciso e atualizado dos perfis dos usuários criados para os usuários que tenham sido autorizados a acessar o sistema (item 6.6.2.2); o fornecimento de procedimentos seguros de entrada para quaisquer contas de usuários sob o controle do cliente (item 6.6.4.2), de informações para o cliente em relação às circunstâncias em que ela usa a criptografia para proteger os dados pessoais (item 6.7.1.1). Ademais, traz que a organização deve assegurar que, quando um espaço de armazenamento é realocado, qualquer dado pessoal previamente guardado naquele espaço de armazenamento não seja acessível (item 6.8.2.7).

No item 6.8.2.9 a norma técnica aborda a necessidade de restringir a criação de material físico que inclua dado pessoal ao mínimo necessário para atender ao propósito do tratamento identificado. Além disto, traz a necessidade de que a organização tenha uma política que considere os requisitos para cópia de segurança, recuperação e restauração de dado pessoal (que pode ser parte de uma política de cópias de segurança das informações globais), bem como quaisquer requisitos adicionais para sua eliminação (item , 6.9.3.1), bem como fala da implementação de um processo para analisar criticamente os registros de eventos (logs)usando processos contínuos de alerta e monitoramento automatizados, ou também manualmente, onde convém que tal análise crítica seja desempenhada em uma periodicidade especificada e documentada, visando identificar irregularidades e propor esforços de remediação (item 6.9.4.1).

Já no item 6.9.4.2, a norma trata da implantação de procedimentos, preferencialmente automatizado, para assegurar que as informações de eventos sejam excluídas ou anonimizadas como especificado na programação de retenção, assim como para assegurar que regras relativas ao tratamento de dados valham em todo o sistema e fora dele (item 6.10.2.1).

A ISO aborda a necessidade de assegurar que os dados pessoais transmitidos por redes de transmissão de dados não confiáveis estejam criptografados para a transmissão (item 6.11.1.2), não sejam usados para propósitos de testes, sendo usado um dado falso ou sintético (item 6.11.3.1), ou, quando inevitável o uso dos dados reais, sejam implementadas medidas técnicas e organizacionais equivalentes àquelas usadas no ambiente de produção, para minimizar os riscos (item 6.11.3.1), além de falar de uma avaliação de riscos, a fim de informar a seleção de controles apropriados de mitigação (item 6.12.1.2).

Quanto às violações às regras do tratamento de dados, a ISO, no item 6.13.1.1, diz que devem estabelecer responsabilidades e procedimentos para a identificação e registro delas, assim como procedimentos relativos à notificação dos envolvidos e a divulgação para as autoridades, levando em conta a regulamentação e/ou legislação aplicadas (item 6.12.1.2).

Sobre a obrigação de confidencialidade dos dados pessoais tratados, no item 6.10.2.4 da ISO, ressalta que a organização deve assegurar que os indivíduos que operam sob o controle dos dados pessoais estejam sujeitos a um acordo obrigatório de confidencialidade, parte de um contrato ou, de forma separada, além de prever verificações periódicas, de modo que arquivos temporários não usados sejam removidos dentro do período de tempo identificado (item 8.4.1).

4.2 Aspectos da norma ISO/IEC 27701:2019 que abrangem além dos requisitos da LGPD e que constam na legislação mas não faz parte da ISO

A ISO orienta a organização a divulgar para o cliente qualquer subcontrato para tratar os dados pessoais, antes do uso, com a inclusão no instrumento de informações sobre os nomes dos subcontratantes, a pertinência, nomes para os países os subcontratantes poderem transferir os dados, sendo necessária a autorização escrita do titular, por meio da inserção adequada de cláusula contratual neste sentido. No caso de subcontratação também é obrigatória a informação ao titular de quaisquer alterações antes mesmo de os dados serem tratados pelo novo contratante (itens 8.5.6, 8.5.7 e 8.5.8). A norma também aconselha que a organização designe um ponto de contato para ser usado pelo cliente, em relação ao tratamento dos dados pessoais (item 6.3.1.1).

Em contrapartida, ao analisar detidamente a Lei Geral de Proteção de Dados, observa-se que ela restou inerte com relação à possibilidade de celebrar subcontratos para tratamento de dados.

Outro ponto que a ISO aborda, mas a Lei não faz menção, é a questão da necessidade de conscientização sobre as medidas adotadas para o tratamento dos dados pessoais e para a segurança destes dados, o que se vê do item 6.4.2.2 da norma técnica.

Por outro lado, há aspectos em que, em que pese a legislação de proteção de dados abordar, a ISO não faz menção a nenhum procedimento a ser utilizado quanto a estes tópicos, como se vê com relação à reparação dos danos causados pelo controlador ou o operador (art. 42).

Portanto, em que pese seja inegável que a ISO 27701 é interessante para gerenciar o *compliance* /conformidade legal com a LGPD, não se pode esquecer que a norma técnica não alcança alguns aspectos da legislação, assim como que em outros pontos a ISO vai além dos aspectos abrangidos pela LGPD.

5 MODELO INTEGRADO DE CONFORMIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS NA UNIRV

Após vastamente discorrido sobre a nova Lei Geral de Proteção de Dados, sua necessidade, obrigatoriedade e importância, assim como sobre as ISO que trata da proteção de dados e privacidade dos dados (ISO 27701), o passo seguinte é trazer, uma proposta de projeto de implantação do processo de gestão de dados pessoais no âmbito da universidade em estudo.

A priori, insta salientar que, a implantação deste novo sistema de gestão de dados não é, de maneira alguma, uma tarefa simples. Esta afirmação encontra amparo no fato de que ela requer mudança de hábitos e práticas consolidadas há muitos anos, além de necessitar da aprovação da direção, bem como do comprometimento e auxílio de todos os colaboradores da instituição.

Ressalta-se que este projeto de proteção de dados englobará todas as informações que levem à identificação de um sujeito, direta ou indiretamente, o que pode ter relação com o nome, dados/elementos de identificação (ex.: número de documentos) física, fisiológica, psíquica, econômica, cultural ou social tratados na secretaria acadêmica da UniRV.

A ISO 27701/2019 define um conjunto de diretrizes, que fornece orientações para estabelecer, implementar, manter e melhorar continuamente – um PIMS (*privacy information management system*) - com base nos controles da norma ISO 27001 de gerenciamento e segurança das informações, corroborados por uma série de requisitos específicos da privacidade dispostos na norma 27701[2].

5.1 Planejamento

A fase de planejamento, contará com as seguintes etapas:

- Obtenção de apoio da direção: o encarregado pelo tratamento dos dados, deve apresentar para a direção o projeto de gestão de dados, bem como a forma como cada integrante dela deve se comprometer e colaborar com o projeto.

- Definição do escopo

[2] MINDSECBLOG. ISO 27701. **Extensão ISO 27001/2 para Privacidade de Dados.** Minuto da segurança. Disponível em: https://minutodaseguranca.blog.br/iso-27701- extensao-iso-27001-2-para-privacidade-dedados/#:~:text=ISO%2027701%20%2D%20Extens%C3%A3o%20ISO%20270 01%2F2%20para%20Privacidade%20de%20Dados. Acesso em: 18 fev. 2022.

- Definição da metodologia de avaliação de risco

- Plano de tratamento

- Avaliação da eficácia do controle

A primeira fase consistirá na apresentação do projeto e conscientização da direção da Universidade sobre a necessidade de se adotar uma política de gestão de dados que atenda aos ditames da LGPD e da ISO 27701. Para tanto, apurar-se-á e expor-se-á sobre o status e os contextos nos quais se inserem os dados pessoais à disposição da organização (ISO 27701, itens 7.3 e 7.4). Nesta etapa será necessária uma análise crítica e criteriosa por parte da direção da organização (27701, item 5.7.3).

5.2 Execução

A fase da execução contará, inicialmente, com a implementação de controles e processos aplicáveis e a elaboração de programas de treinamento e conscientização.

A segunda fase será o mapeamento de dados, que consistirá nos seguintes passos:

- Classificação das informações:

- tipo de dados (sinsível ou não – art. 5º, I e II LGPD e ISO 27001, item 6.5.2.1)

- origem (art. 19, II da LGPD)

- destino

- finalidade (art. 6º da LGPD

- local de armazenamento (meio digital ou analógico), com gerenciamento das mídias removíveis. Para tanto, a organização deverá utilizar, prioritarimante, mídias físicas, passíveis de criptograifa, além de elaborar um documento/termo, no qual serão registrados todos os acessos.

Para esta fase, a universidade deverá projetar um sistema de classificação de dados, assim como realizar e manter cópias com temporariedade de execução e testes (simulações), que indiquem que os procedimentos adequados foram implantados e são funcionais (GUIA).

Ademais, as mídias removíveis serão armazenadas em embalagens lacradas, com dispositivo inviolável, devidamente numerado, onde conste o termo de acesso e o número do lacre rompido, bem como do que irá substitui-lo após o uso.

Também deverão implementar um sistema próprio para o registro das entradas e saídas das mídias físicas que contenham dados pessoais, do qual constará o tipo de mídia, a pessoa que teve acessoa a ela, com a especificação de sua autorização para tanto, a data e horário do

acesso. Sempre que a mídia for retirada da universidade, o funcionário responsável deverá garantir que haja uma cópia de segurança da mesma.

Quanto aos privilégios de acesso (art. 5º, IX LGPD e ISO 27701, item 6.6.2.3), a organização criará um controle de acesso ao sistema, com senhas individuais e permissões limitadas, assim como registro no sistema do acesso, com data, horário, nome e matrícula da pessoa que acessou. Também deverá constar o período e as condições de armazenamento.

No que concerne à forma de tratamento, o programa abarcará as fases de coleta, armazenamento, alteração, recuperação, consulta, divulgação e anonimização, bem como o processo de transferência de dados (destinatários, protocolos de proteção).

Nesta etapa, o controlador dos dados pessoais na universidade realizará um treinamento com todos os envolvidos no tratamento de dados, a fim de conscientizá-los sobre o tipo e as características dos dados pessoais com os quais lidam (ISO 27701, item 6.5.2.2).

O projeto de gestão de dados abrangerá o levantamento dos fluxos de dados e demandará um trabalho conjunto das equipes de TI, jurídico, marketing e RH.

5.3 Controlar

A fase de controle envolverá:

- monitoramento;
- auditoria interna;
- planejamento: mapeamento dos fluxos de dados;
- mensuração dos riscos: identificação dos riscos;
- identificação dos impactos positivos e negativos de situações que possa acarretar prejuízo à imagem da organização: planejamento de respostas;
- produção de uma Declaração de Aplicabilidade que, nos termos da ISO 27701, 6.1.3, contemple:
    - os controles necessários;
    - a justificativa para suas inclusões;
    - informações quanto à implementação ou não dos controles necessários;
    - justificativa para a exclusão de controles necessários.

Esta terceira fase consistirá na estipulação dos riscos a serem evitados, avaliação e análise crítica do levantamento de dados. Esta etapa visa a identificar riscos relativos à perda de confiabilidade, integridade e disponibilidade, nos termos das ISOs 27001 e 27701.

A avaliação de riscos, terá como base um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), nos moldes do modelo constante do Guia de Boas Práticas da LGPD[3].

5.4 Agir

A fase da ação, abarcará:

- análise crítica da direção;

- ações corretivas;

- adoção de ferramentas que visem garantir a segurança dos dados pessoais e impedir o acesso por pessoas não autorizadas, assim como sua destruição, perda, alteração, comunicação ou difusão;

- estabelecimento de uma governança digital e de boas práticas relativas ao tratamento dos dados sensíveis;

- criação de processos internos de eliminação de dados após o fim do tratamento;

- estabelecimentos de mecanismos internos de detecção de eventuais incidentes;

- definição de uma pessoa responsável pela gestão dos dados.

Nesta etapa a universidade revisará as políticas de segurança das informações, para alinhar procedimentos e corrigir possíveis problemas. Para tanto, indicará um servidor responsável pelas ações de segurança de dados.

A quarta fase será o plano de ação e sua implementação, que consiste na indicação das medidas concretas a serem adequadas e efetiva adoção das estratégias necessárias para tanto. Para atender ao disposto nos arts. 5º, 6º, 46, 47, 49 e 50 da LGPD, a organização elaborará um programa de governança e segurança a ser adotado na Universidade, a fim de evitar acessos indevidos e incidentais. Este programa deve conter:

a) natureza;

b) escopo;

c) finalidade;

d) probabilidade; e

e) gravidade dos riscos e dos benefícios de se adotá-lo.

A universidade também disponibilizará, nos termos da ISO 27701 (6.3.2.1), aparelhos móveis, aptos a realizar o tratamento de dados de forma segura.

---

[3] CCGD. Comitê Central de Governança de Dados. **Guia de Boas Práticas LGPD.** abr. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-dedados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 20 ago. 2022.

6 CONSIDERAÇÕES FINAIS

Nas últimas décadas, por ocasião da evolução das tecnologias de comunicação, com destaque para aquelas relacionadas à internet, o acesso às informações pessoais se tornou deverás mais fácil e rápido, o que trouxe benefícios inegáveis. Contudo, associado a estas benesses, observou-se, também, um aumento vertiginoso das práticas ilícitas realizadas por conta da utilização indevida de dados pessoas. No afã de resolver tal problemática, o legislador, no ano de 2011, criou a Lei de Acesso à Informação (Lei 12.527), destinada aos entes públicos.

Ocorre que, à medida que a sociedade evoluiu, a norma supracitada se mostrou insuficiente ou ineficiente para solucionar os problemas afetos à utilização ilegal de dados, o que culminou com a edição da Lei Geral de Proteção de Dados (Lei 13.709/2018). Entrementes, para se cumprir os ditames desta legislação, mostrou-se necessárias orientações ou regramentos práticos.

Com base no estudo realizado, percebeu-se que a norma ISO 27701 e a LGPD apresentam uma correlação positiva, em razão de a citada norma técnica servir de base para a colocação em prática dos mandados trazidos pela legislação protetiva, em virtude de abordar diversas temáticas enfrentadas também pela LGPD.

Após explorar vastamente o conteúdo da norma legal e da ISO, é possível afirmar-se que as duas, quando utilizadas combinadamente, são capazes de dar origem a um sistema de gestão aplicável às organizações de modo geral, em especial o tipo aqui em foco, qual seja instituições de ensino superior. Observou-se que a junção das determinações e aspectos práticos consta das duas normas, é capaz de trazer resultados práticos, com a gestão dos dados de modo a acarretar a segurança necessárias às instituições.

A análise comparativa realizada sobre a ISO e a LGPD induziu à conclusão de que os dois sistemas se conversam, ou seja, trazem similaridades e se complementam. Contudo, também notou-se que a ISO aborda alguns pontos sobre os quais a legislação protetiva restou silente, bem como quedou-se inerte sobre outros que o legislador disciplinou. De outro aspecto, viu-se que há pontos da LGPD que não podem ser colocados em prática apenas com o auxílio da ISO 27701, carecendo, portanto, da associação com outras normas.

Em que pese as limitações acima expostas, acredita-se que as normas ISO e LGPD, associadas, são capazes de embasar um sistema de conformidade na gestão dos dados pessoais de instituições da natureza daquela aqui em estudo, qual seja uma Universidade, por trazerem elementos suficientes para a elaboração de um projeto de *compliance* exitoso.

Chegou-se, ainda, a ilação de que este tipo de sistema de gestão consubstancia-se perfeitamente com a necessidade das Instituições de Ensino Superior, em especial a UniRV, de modo que faz total sentido a aplicação do modelo aqui proposto.

No que concerne à forma de implementação de um sistema de gestão desta natureza no âmbito da Universidade, observou-se que isto será possível com a observâncias das regras técnicas trazidas pela ISO, utilizando-se, para tanto, a metodologia PCDA, que engloba todas as etapas necessária para implantar o programa, pois vai desde a etapa de planejamento, passando por pelas ações práticas, pela verificação dos resultados do programa e chegando até às ações a serem adotadas para o fim de corrigir as falhas.

Inobstante isto, ficou bastante clara a necessidade de comprometimento da alta direção da instituição para com a implantação do projeto de gestão da conformidade com a Lei Geral de Proteção de Dados. Porém, insta salientar a necessidade do envolvimento de todas as pessoas que fazem parte da organização para que haja êxito no trabalho, de modo que todos estejam dispostos a respeitar os princípios exigidos pela norma protetiva de dados e todo o regramento legal correlato.

Em termos práticos, acredita-se que a proposta de elaboração de um projeto de gestão de *compliance* de dados nos moldes aqui defendidos, permitirá à UniRV a implementação de um sistema muito bem estruturado, que atenda às necessidades da instituição e a leve a respeitar os mandamentos legais e ter uma melhor imagem diante da sociedade de modo geral.

Por fim, com base no arcabouço de argumentos e proposições constantes do presente estudo, restam claros os benefícios que a implantação de um projeto de *compliance* de gestão de dados pessoais que observe os pontos destacados neste estudo pode acarretar para a Universidade de Rio Verde.

De igual forma, ficou claramente demonstrado que as Normas ISO, em especial a 27701, têm o condão de, em conjunto com as determinações encartadas na LGPD, balisar a elaboração de um programa de conformidade, tendo em vista o objetivo da ISO, qual seja ajudar as organizações a manter os seus ativos de informação seguros.

Notou-se, ainda, que a colocação em prática de um modelo de *compliance* adequado favorece às instituições de ensino o melhoramento de suas práticas, o que se traduz num diferencial competitivo, representado pela segurança ofertada quanto aos dados pessoas de seus clientes e usuários.

Portanto, é realmente imprescindível um projeto de *compliance* para que a Universidade de Rio Verde, em especial por conta do seu porte, consiga garantir a segurança

dos dados dos titulares e, via de consequência, estar em conformidade com os ditames da Lei Geral de Proteção de Dados e demais normas legais que disciplinam esta temática.

7 CONCLUSÕES

A realização do presente estudo objetivou avaliar os elementos que devem ser contemplados num projeto de conformidade de gestão de dados no âmbito da Universidade de Rio Verde, embasado nas práticas da ISO 27701 e tendo em vista a necessidade de implementação de um programa *compliance* de proteção de dados que atenda às determinações trazidas pela LGPD.

Diante de todo o exposto no bojo do presente, conclui-se que o trabalho culminou por alcançar o objetivo proposto, uma vez que foi possível fazer uma análise detalhada tanto dos preceitos trazidos pela LGPD, bem como das normas técnicas abordadas pelas ISOs, em especial a 27701.

Ademais, no que tange aos objetivos específicos definidos, no decorrer deste estudo, conseguiu-se realizar um espelhamento das normas em comento (LGPD e ISO/IEC 27701), apontando as similaridades e diferenças existentes entre elas, o que serviu de parâmetro para a elaboração de uma proposta de projeto de gestão de conformidade com a legislação protetiva de dados, com a aplicação das regras técnicas trazidas pela ISO 27701, bem como outras normas que abordam questões práticas atinentes à segurança de dados pessoais nas organizações, em especial nas Instituições de Ensino Superior.

Por outro enfoque, foi possível, após uma análise detida das normas legais apontar os elementos que devem ser abordados no projeto de *compliance* de gestão de dados na Universidade de Rio Verde, a fim de estar em conformidade com a legislação.

Diante do alcance dos objetivos propostos, geral e específicos, o presente estudo traz algumas implicações, de cunho teórico e prático. Pelo enfoque da teoria, tem-se que a revisão minuciosa do material bibliográfico acerca das determinações trazidas pela Lei Geral de Proteção de Dados e os desafios que surgem para a colocação em prática de tais ditames legais, tem o poder de trazer clareza sobre os pontos para os quais as organizações precisam se atentar no intuito de estar em conformidade com a legislação e evitar os ricos que a má-gestão de dados pessoais pode acarretar.

Ademais, a correlação realizada entre o conteúdo da LGPD e as regras práticas que a ISO 27701 que com ele guarda relação e favorece a implementação prática de ações que visem à conformidade, é de grande relevância para a realização de um projeto de *compliance* que atenda, de fato, a necessidade das organizações.

Pelo enfoque prático, as abordagens constantes do presente estudo auxiliarão na construção de um sistema integrado da LGPD e a ISO 207701, com a elaboração de uma

proposta específica para uma Instituição de Ensino Superior, qual seja a Universidade de Rio Verde, em que pese ser perfeitamente passível de ser aplicada em outras instituições desta natureza ou mesmo outro tipo de organização que deseja criar um projeto de *compliance* pautado na integração das normas em comento.

Ao final, é interessante pontuar que, o conteúdo aqui produzido pode ser interessante para que o legislador trabalhe futuras normas protetivas de dados mais completas, que abordem tanto mandamentos, quanto a forma de colocá-los em prática no âmbito das Instituições de Ensino Superior como instituições de outros segmentos, com enfoque no conteúdo das Normas ISOs e a integração delas com a legislação. Esta iniciativa poderia gerar leis que preencham as lacunas apresentadas neste estudo como existentes na LGPD, em especial por trazer deveres, mas não determinar a forma de cumpri-los.

Ressalta-se que, a exemplo do que já fora discutido em alguns fóruns realizados, esta correlação entre a LGPD e as normas constantes da ISO 27701, permitiria a edição de normas legais bem mais completas e que teriam efeitos práticos muito mais eficazes.

No tocante às limitações para a realização do presente estudo, o principal empecilho verificado foi a inexistência de testes de modelos de projetos similares ao aqui proposto e sua efetividade. Contudo, acredita-se que eventuais auditorias, implementações e reconhecimentos futuros permitiriam ampliar o estudo.

Inobstante isto, é fortemente recomendável que a universidade implemente um projeto nos termos aqui sugeridos, pois ela lida com dados pessoais e contar com um programa de *compliance* de dados, pautado na necessidade de cumprir os mandamentos legais encartados na lei protetiva, em especial na Lei Geral de Proteção de Dados, e elaborado tendo por parâmetro não somente a legislação em vigor, mas, também, as normas técnicas trazidas pela ISO 27701, consoante se extrai da proposta de modelo integrado aqui exposta, acarretaria segurança dos dados pessoais por ela geridos, bem como evitaria problemas futuros e melhoraria a imagem da instituição frente à sociedade.

Frente a tudo isto, recomenda-se a realização de novos estudos em sentido semelhante ao presente, porém com a avaliação da viabilidade de integração da LGPD com outras normas legais que guardem relação com as regras nela encartadas, a fim de gerar conteúdo para legislações a serem elaboradas futuramente que sejam mais completas e, via de consequência, mais eficazes.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001:** 2013. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro: ABNT, 2006.

ABNT. Associação Brasileira de Normas Técnicas. **Normalização.** 2011. Disponível em: http://pwt.net.br/site/o-que-e-normatizacao-segundo-a-abnt/. Acesso em: 7 fev. 2022.

ABNT. Associação Brasileira de Normas Técnicas. **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. 2019. Disponível em: https://www.normas.com.br/autorizar/visualizacao-nbr/11548. Acesso em: 7 fev. 2022.

ALMEIDA, Bethania de Araujo et. al. Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva,** v. 25, p. 2487-2492, 2020. Disponível em: https://www.scielo.br/j/csc/a/T6rwdhnTNzp5vYr84w9xthB/?format=pdf&lang=pt. Acesso em: 10 mar. 2021.

ALVES, Érika Andrade Castro. O PDCA como ferramenta de gestão da rotina. 2015. Disponível em: https://www.inovarse.org/sites/default/files/T_15_017M_7.pdf. Acesso em: 15 jun. 2022.

ANAHP. Associação Nacional de Hospitais Privados. **Manual de melhores práticas LGPD.** 2020. Disponível em: https://www.anahp.com.br/pdf/manual-melhores-praticas-lgpd.pdf. Acesso em: 14 set. 2021.

ANDRADE, Nayara Santos; RABELO, Maria Helena Silva. Segurança da informação: um estudo sobre o processo de segurança da informação em instituições financeiras localizadas na região centro-oeste de Minas Gerais. **Revista Acadêmica Conecta FASF,** v. 2, n. 1, p. 126-144, 2017.

ANWAR, Memoona Javeria; GILL, Asif Qumer. **Developing an Integrated ISO 27701 and GDPR based Information Privacy Compliance Requirements Model.** Disponível em: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1055&context=acis2020. Acesso em: 28 jan. 2022.

AURIGA. **Digital Transformation:** History, Present, and Future Trends. Retrieved June 15, 2017. Disponível em: https://auriga.com/blog/digital-transformation-history-presentand-future-trends. Acesso em: 21 mar. 2021.

AZEVEDO, Gleyson. **Gestão de segurança da informação I.** Disponível em: https://free-content.direcaoconcursos.com.br/demo/curso-8913.pdf. Acesso em: 25 jan. 2022.

BATIMARCHI, Susana. **A diferença entre dados estruturados e não estruturados.** 2015. Disponível em: http://docmanagement.com.br/03/06/2015/a-diferenca-entre-dados-estruturados-e-não-estruturados/. Acesso em: 10 jun. 2022.

BENAVIDES, Lina Maria Castro et. al. Digital transformation in higher education institutions: a systematic literature review. **Sensors,** v.20, n. 11, 2020. Disponível em: https://www.mdpi.com/1424-8220/20/11/3291. Acesso em: 05 mar. 2021.

BENESOVÁ, Andrea; TUPA, Juri. Requirements for Education and Qualification of People in Industry 4.0. **Procedia Manufacturing,** v. 11, p. 2195-2202, 2017. Disponível em: https://reader.elsevier.com/reader/sd/pii/S2351978917305747?token=BF8AA30CE35F49BE276E21889B18F730598F9E93441847FA0F68CA276B56BFB27C47137E20BDAA7AF54BAD195C1310CF&originRegion=us-east-1&originCreation=20210911145230. Acesso em: 11 set. 2021.

BERMAN, Saul J. Digital transformation: opportunitIEs to create new business models. **Strategy and Leadership,** v. 40, n. 2, 2012. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/10878571211209314/full/pdf?casa_token=GsPGR1a3DkYAAAAA:PeSHVXK4HbWNICRhYvW5Qd_y4n4SxgR8Go7vClXyg2PCUb-Gzd8Z6WM53sRoNuB2MEtLi2xx7_PpH-uv_wLb9ANflqBLzQDFCCNZWRWjlWUGnG_LnzhdEw. Acesso em: 20 mar. 2021.

BEUREN, Ilse Maria. **Gestão da informação:** um recurso estratégico no processo de gestão empresarial. 2. ed. São Paulo: Atlas, 2000.

BIEGELMAN, Martin. T; BIEGELMAN, Daniel R. Building a World-**Class Compliance Program:** Best Practices and Strategies for Success. Editora: John Wiley & Sons, 2008.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais – a função e os limites do consentimento.** 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BLUM, Renato Opice; LÓPEZ, Nuria. Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito. **Cadernos Jurídicas,** a. 21, n. 53, p. 171-177, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_7_cadernos_juridicos_epm.pdf?d=637250348268501368. Acesso em: 22 jan. 2022.

BORGES, Cyonil. **Resumo da lei de acesso à informação – concurso público.** 2012. Disponível em: https://www.tecconcursos.com.br/blog/resumo-da-lei-de-acesso-a-informacao-lei-125272011/. Acesso em: 11 jan. 2022.

BOUEÉ, Charles-Edouard; SCHAIBLE, Stefan. **Die Digitale Transformation der Industrie.** Studie: Roland Berger und BDI. 2015. Disponível em: https://bdi.eu/media/presse/publikationen/information-und-telekommunikation/Digitale_Transformation.pdf. Acesso em: 12 maio 2022.

BOUTER, Rick. **Accenture digital transformation re-imagine from the outside-in.** Accenture Interactive – Point of View SerIEs, dec. 2014. Disponível em: https://www.slideshare.net/rbouter/accenture-digital-transformation-reimagine-from-the-outsidein. Acesso em: 12 mar. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Emendas Constitucionais. **Diário Oficial da União,** Brasília, 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 21 jan. 2021.

BRASIL. **Declaração dos Direitos Humanos.** 1948. Disponível em: https://www.oas.org/dil/port/1948%20Declara%C3%A7%C3%A3o%20Universal%20dos%20Direitos%20Humanos.pdf. Acesso em: 8 fev. 2022.

BRASIL. Decreto n. 8.777, de 11 de maio de 2016. Institui a Política de Dados Abertos do Poder Executivo Federal. **Diário Oficial da União,** Brasília, 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8777.htm. Acesso em: 8 fev. 2022.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 03 jan. 2021.

BRASIL. Ministério Público Federal. **Sistema brasileiro de proteção e acesso a dados pessoais:** análise de dispositivos da Lei de Acesso à Informação, da Lei de Identificação Civil, da Lei do Marco Civil da Internet e da Lei Nacional de Proteção de Dados. Brasília: MPF, 2019. 85p.

BRASIL. Emenda Constitucional n. 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, 11 fev. 2022. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm>. Acesso em: 20 dez. 2022.

CALABRICH. Bruno Freire de Carvalho. O conceito de tratamento de dados pessoais e o acordo Lindqvist, do Tribunal de Justiça da União Europeia. **Revista Tribunal Regional Federal da 1ª Região,** a. 31, n. 2, 2019. Disponível em: https://rtrf1.emnuvens.com.br/trf1/article/view/103/92. Acesso em: 28 dez. 2021.

CARAFFINI, Josiane Piva Testolin da Silva; SOUZA, Romina Batista de Lucena de; BEHR, Ariel. **Transformação digital e desempenho no setor bancário.** 2018. Disponível em: http://bibliotecadigital.fgv.br/ocs/index.php/ctd/ctd2018/paper/viewFile/6965/1971.Acesso em: 23 ago. 2022.

CAROSSI, Daniel Fernando. **Dados abertos:** categorias e temas prioritários a serem disponibilizados pelas instituições federais de ensino superior (IFES) aos cidadãos. 2016. 139f. Dissertação (Mestrado em Sistemas de Informação) – Universidade Federal de Pernambuco, Recife, 2016.

CCGD. Comitê Central de Governança de Dados. **Guia de Boas Práticas LGPD.** abr. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-dedados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 20 ago. 2022.

CHEPKASOVA, Elena. **Transformation in the Era of Digitization:** A study of organizations implementing digital transformation projects with integrated project management and change management. 2017. Disponível em: http://www.diva-portal.se/smash/get/diva2:1071105/FULLTEXT01.pdf. Acesso em: 12 mar. 2022.

CHRISTENSEN; Clayton M.; EYRING, Henry J. **A universidade inovadora:** mudando o DNA do Ensino Superior de fora para dentro. Porto Alegre: Bookman, 2014.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa Alessi. **Manual de compliance:** preservando a boa governança e a integridade das organizações. São Paulo, Atlas, 2010.

COLLIN, Jari et al. **It Leadership in transition – the impacto f digitalization on finnish organizations.** 2015. Disponível em: https://research.aalto.fi/en/publications/it-leadership-in-transition-the-impact-of-digitalization-on-finni. Acesso em: 02 maio 2021.

CORREIA, Carlos Manuel Rosa. **Plano de implementação da norma ISSO /IEC 27001 no INEM.** 2016. 110f. Dissertação (Mestrado em Gestão de Informação) – Instituto Superior de Estatística e Gestão de Informação, Lisboa, 2016.

COSTA NETO, Luiz Gonzaga da; CAMPOS, Fernando Celso de. Oportunidades de aplicações de *business intelligence* no contexto da indústria 4.0: revisão sistemática da

literatura 2015-2020. **Exacta Engenharia de Produção,** 2021. Disponível em: https://periodicos.uninove.br/exacta/article/view/19525. Acesso em: 23 mar. 2022.

CRUZ, Danielle da Costa Santos. **A lei geral de proteção de dados pessoais (LGPD):** contribuições sobre o uso e proteção de dados para as instituições de ensino. 2021. 36f. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação) - Universidade Federal Rural da Amazônia, Belém, 2021.

DAVIS, Alison; LE MERLE, Matthew C. **Blockchain competitive advantage.** Tiburon: Fifth Era Media, 2019. *e-book.*

DINIS, Eduardo Henrique. Tecnologia em tempos de Covid-19. **Revista GV Executivo,** Conhecimento e impacto em gestão. v. 19, n. 4, p. 47, jun./ago. 2020. Disponível em: https://rae.fgv.br/sites/rae.fgv.br/files/coluna_tecnologia_0.pdf. Acesso em: 10 jan. 2021.

DOHMANN, Indra Spiecker Genannt. A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia. In: BIONI, Bruno (Coord.). **Tratado de proteção de dados pessoais.** Rio de Janeiro: Forense, 2021. p. 9-32.

DONEDA, Danilo. A proteção de dados em tempos de coronavírus. Redes Sociais como canais de distribuição de conteúdo. **Jota Info,** 2020. Disponível em https://www.jota.info/opiniao-e-analise/artigos/a-protecao-de-dados-em-tempos-de-coronavirus-25032020. Acesso em: 01 abr. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law,** v. 12, n. 2, p. 91-108, 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 13 jan. 2021.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico,** v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 19 ago. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais:** fundamentos da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DUNBRACK, Lynne, et al. **IOT and Digital Transformation:** a Tale of Four IndustrIEs. 2016. Disponível em: https://vods.dm.ux.sap.com/publicsectoruk/2016/pdfs/IoTandDigitalTransformation_ATalesofFourIndustrIEs.pdf. Acesso em: 18 mar. 2021.

ELER, Kalline Carvalho Gonçalves. A releitura da privacidade: do “direito de ser deixado só” ao direito à autodeterminação informativa. **Revista Internacional de Tecnologia, Ciencia y Sociedad,** v. 5, n. 2, p. 185-196, 2020.

ELSAADANY, Amr; SOLIMAN, Mohamed. Experimental Evaluation of Internet of Things in the Educational Environment. **International Journal of Engineering Pedagogy,** v. 7, n. 3, 2017. Disponível em: https://online-journals.org/index.php/i-jep/article/view/7187. Acesso em: 12 jun. 2022.

ESPINOZA, Javier. EU admits it has been hard to implement GDPR. **Finacial Times,** 23 jun. 2020. Disponível em: https://www.ft.com/content/66668ba9-706a-483d-b24a-18cfbca142bf. Acesso em: 17 maio 2021.

EUR-LAX. Disponível em: https://eurlex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:31995L0046&from=EN. Acesso em: 24 jan. 2021.

EUROPENA STUDENTS’ UNION - ESU. **Policy Paper on Public Responsibility, Financing and Governance of Higher Education**. Disponível em: https://web.a.ebscohost.com/ehost/detail/detail?vid=0&sid=40bf2670-879b-4163-b543-77a9a4ec6801%40sessionmgr4008&bdata=Jmxhbmc9cHQtYnImc2l0ZT1laG9zdC1saXZl#AN=ED610895&db=eric. Acesso em: 01 set. 2021.

FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital – uma releitura do art. XII da Declaração Universal dos Direitos Humanos (DUDH) na sociedade do espetáculo. **Revista Internacional Consinter de Direito,** a. 5, n. 9, 2019. Disponível em: https://revistaconsinter.com/revistas/ano-v-numero-ix/direitos-difusos-coletivos-e-individuais-homogeneos/direito-a-privacidade-na-era-digital-uma-releitura-do-art-xii-da-declaracao-universal-dos-direitos-humanos-dudh-na-sociedade-do-espetaculo/. Acesso em: 11 de outubro de 2021.

FINKELSTEIN, Maria Eugênia; FINKELSTEIN, Cláudio. Privacidade e lei geral de proteção e dados. **Revista de Direito Brasileira,** Florianópolis, SC, v. 23, n. 9, p. 284-301, ago. 2019. Disponível em: https://www.indexlaw.org/index.php/rdb/article/view/5343/4545. Acesso em: 13 jan. 2022.

FITZGERALD, Michael et. al. **Embracing Digital Technology:** A New Strategic Imperative | Capgemini Consulting Worldwide. MIT Sloan Management Review, 1-13. Retrieved from. Disponível em: https://emergenceweb.com/blog/wp-content/uploads/2013/10/embracing-digital-technology.pdf. Acesso em: 23 mar. 2021.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.).

A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Revista dos Tribunais, 2019. p. 677-715.

FREIRE, Gianfrancesco Ranieri D.A. et al. **Gestão da informação e do conhecimento, segurança da informação e normalização:** diferentes perspectivas para unidades de informação. 2012. Disponível em: https://brapci.inf.br/index.php/res/download/86511. Acesso em: 22 jan. 2022.

FUNDAÇÃO VANZOLINI. **ISO/IEC 27701:** gestão de segurança da informação e privacidade. Disponível em: https://vanzolini.org.br/produto/iso-iec-27701/. Acesso em: 6 fev. 2022.

GARCIA, S. Gallego; GARCIA, M. García. Industry 4.0 implications in production and maintenance management: na overview. **Procedia Manufacturing,** v. 41, p. 415-422, 2019. Disponível em: https://www.sciencedirect.com/science/article/pii/S235197891931114X. Acesso em: 21 nov. 2021.

GASIOLA, Gustavo Gil. **Criação e desenvolvimento da proteção de dados na Alemanha.** 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-daprotecao- de-dados-na-alemanha-29052019. Acesso em: 2 fev. 2022.

GEISSBAUER, Reinhard; VEDSO, Jesper; SCHRAUF, Stefan. Industry 4.0: Building the digital enterprise. 2016. **PwC.** Disponível em: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf>. Acesso em: 17 ago. 2022.

GILCHRIST, Alasdair. **Industry 4.0:** The Industrial Internet of Things. Tailândia: Apress, 2016.

GIOVANINI, Wagner. **Entenda a diferença entre a LGPD e a ISO 27.701.** 2021. Disponível em: https://www.compliancetotal.com.br/conteudos/detalhe/302/entenda-a-diferenca-entre-a-lgpd-e-a-iso-27-701. Acesso em: 9 fev. 2022.

GOMES, Heloisa dos Santos. **Lei geral de proteção de dados (LGPD):** uma análise dos impactos da lei na cultura e tratamento de dados no Brasil. 2019. 28f. Monografia (Curso de Tecnologia em Análise e Desenvolvimento de Sistemas) - Universidade do Sul de Santa Catarina, Florianópolis, 2019.

HARARI, Yuval Noan. **21 lições para o século 21.** Tradução de: Paulo Geiger. São Paulo: Companhia das Letras, 2018.

HEILIG, Leonard; SCHWARZE, Silvia; STEFAN, Voss. An analysis OF digital transformation in the history and future of modern ports. **Proceedings of the 50th Hawaii**

International Conference on System Sciences, 2017. Disponível em: https://www.researchgate.net/publication/312218687_An_Analysis_of_Digital_Transformation_in_the_History_and_Future_of_Modern_Ports. Acesso em: 23 abr. 2022.

HESS, Thomas et al. Options for Formulating a Digital Transformation Strategy. **MIS Quarterly Executive,** v. 15, n. 2, p. 123-125, 2019. Disponível em: https://doi.org/10.1108/10878571211209314. Acesso em: 01 fev. 2021.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital: transformação digital, desafios para o direito.** Tradução de: Italo Fuhrmann. Rio de Janeiro: Forense, 2020. p. 311-345, jan./jun. 2021.

IBGC. Instituto Brasileiro de Governança Corporativa. **Compliance à luz da governança corporativa.** São Paulo: IBGC, 2017.

ISO/IEC 27701 DNV AS. **All rights reserved.Privacy Information management system**. Disponível em: https://www.dnv.com/services/iso-iec-27701-privacy-information-management-system-159186. Acesso em: 05 jan. 2021.

ISO/IEC 27701, 2020. **O que é a ISO/IEC 27701/2019.** Disponível em: https://bedu.tech/wp-content/uploads/2020/10/iso-iec-27701.pdf. Acesso em: 14 jan. 2021.

JARDIM, José Maria. **A lei de acesso à informação pública:** dimensões politico-informacionais. 2012. Disponível em:<https://revistas.ancib.org/index.php/tpbci/article/view/266/266>. Acesso em: 20 dez. 2022.

JESUS, Mauricio Barros de. **Modelo Corporativo para Governança e Gestão de TI da Organização.** ISACA, 2012. Disponível em: https://wiki.tce.go.gov.br/lib/exe/fetch.php/acervo_digital:cobit5.pdf. Acesso em: 27 mar. 2021.

KALENDAE. **Saiba como a ISO 27000 pode ser útil na sua empresa.** Disponível em: https://kalendae.com.br/blog/iso-27000/>. Acesso em: 12 jan. 2021.

KANE, By Gerald C. et al. **Strategy, not technology, drives digital transformation.** MIT Sloan Management Review and Deloitte University Press, 14, 2015.

KOHAN, Sarah. **Entenda a importância da gestão de privacidade da norma ISO 27701.** jun. 2021. Disponível em: https://vanzolini.org.br/produto/entenda-a-importancia-da-gestao-de-privacidade-da-norma-iso-27701/. Acesso em: 12 jan. 2021.

KOTLER, Philip; KELLER, Kevin Lane. **Administração de marketing.** 12. ed. São Paulo: Editora Pearson, 2011.

LANGEN, Talita da Silva Carlos. **Lei geral de proteção de dados:** diagnóstico do grau de conformidade de micro e pequenas empresas. 2020. 137f. Dissertação (Mestrado em Administração de Micro e Pequenas Empresas) - Centro Universitário Campo Limpo Paulista, Campo Limpo Paulista, 2020.

LEHONG, Hung; SWANTON, Bill. A Digital Business Technology Platform Is Fundamental to Scaling Digital Business. **Gartner Research,** 2017. Disponível em: https://www.gartner.com/en/documents/3810972. Acesso em: 18 abr. 2021.

LOBATO, Diego Botelho. **Marketing digital:** estudo sobre a importância de sua aplicação emu ma imobiliária de pequeno porte. 2012. 27f. Trabalho de Conclusão de Curso (Bacharel em Administração) – Centro Universitário de Brasília, 2012.

LORENTE, José A. A transformação Digital. **Revista Uno**, v. 24, 2016. Disponível em: https://www.revista-uno.com.br/numero-24/a-transformacao-digital/. Acesso em: 20 ago. 2018.

LÓSSIO, Claudio Joel Brito. **Proteção de dados e compliance digital.** São Paulo: Almedina, 2021.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre a proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito,** v. 12, n. 2, 2020. Disponível em: https://webcache.googleusercontent.com/search?q=cache:IErV4URFlxwJ:https://periodicos.ufv.br/revistadir/article/download/10597/5880/48773+&cd=1&hl=pt-BR&ct=clnk&gl=br. Acesso em: 2 fev. 2022.

LUZ, Charlley. **Lei geral de proteção de dados.** 2019. Disponível em: https://www12.senado.leg.br/institucional/arquivo/apresentacoes/slide-7a. Acesso em: 21 jan. 2022.

MACHADO, José Mauro Decoussau; SANTOS, Matheus Chucri dos; PARANHOS, Mario Cosac Oliveira. **LGPD e GDPR:** uma análise comparativa entre as legislações. 2018. Disponível em: https://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes. Acesso em: 12 jan. 2021.

MACHADO, Matheus Fogaça. **Medidas de proteção de dados pessoais no planejamento e operação de SMART grid utilizando computação em nuvem:** estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil. 2019. 117f. Dissertação (Mestrado em Planejamento e Governança Pública) - Universidade Tecnológica Federal do Paraná, Curitiba, 2019.

MAGRANI, Eduardo. **Entre dados e robôs:** ética e privacidade na era da hiperconectividade. Rio de Janeiro: Konrad Adenauer Stiftung, 2018.

MÄKINEN, Jenna. Data quality, sensitive data and joint controllership as examples of grey areas in the existing data protection framework for the Internet of Things. **Information & Communications Technology Law,** v. 24, n. 3, p. 262-277, 2015. Disponível em: https://www.researchgate.net/publication/282941950_Data_quality_sensitive_data_and_joint_controllership_as_examples_of_grey_areas_in_the_existing_data_protection_framework_for_the_Internet_of_Things. Acesso em: 19 abr. 2021.

MARTINS NETO, João dos Passos; PINHEIRO, Denise. Liberdade de informar e direito à memória: uma crítica à ideia do direito ao esquecimento. **Revista Novos Estudos Jurídicos Eletrônica,** v. 19 - n. 3 - set-dez 2014.

MATTOS FILHO, Veiga; QUIROGA JUNIOR, Marrey. **Guia para a Lei Geral de Proteção de Dados.** ago. 2018. Disponível em: https://www.mattosfilho.com.br/EscritorioMidia/LGPD_MattosFilho.pdf. Acesso em: 12 jan. 2021.

MILAGRE, José. **O que é ISO 27701 e como entender a aplicação da norma para gestão da norma para gestão da privacidade da informação em 5 passos.** Disponível em: https://josemilagre.jusbrasil.com.br/artigos/791257034/o-que-e-iso-27701-e-como-entender-a-aplicacao-da-norma-para-gestao-da-privacidade-da-informacao-em-5-passos#:~:text=Deste%20modo%2C%20a%20ISO%2027701,internacionais%20em%20prote%C3%A7%C3%A3o%20de%20dados. Acesso em: 4 jan. 2021.

MILICEVIC, Danijel; GOEKEN, Matthias. **Ontology-Based Evaluation of ISO 27001.** Conference on e-Business, e-Services and e-Society - I3E 2010: Software Services for e-Worldpp 93-102. Disponível em: https://link.springer.com/content/pdf/10.1007/978-3-642-16283-1_13.pdf. Acesso em: 10 abr. 2021.

MINDSECBLOG. ISO 27701. **Extensão ISO 27001/2 para Privacidade de Dados.** Minuto da segurança. Disponível em: https://minutodaseguranca.blog.br/iso-27701- extensao-iso-27001-2-para-privacidade-dedados/#:~:text=ISO%2027701%20%2D%20Extens%C3%A3o%20ISO%20270 01%2F2%20para%20Privacidade%20de%20Dados. Acesso em: 18 fev. 2022.

MIRAGEM, Bruno. A lei geral de proteção de dados (Lei 13.709/2018) e o direito de consumidor. **Revista dos Tribunais,** v. 1009, nov. 2019. Disponível: https://www.brunomiragem.com.br/wp-content/uploads/2020/06/002-LGPD-e-o-direito-do-consumidor.pdf. Acesso em: 20 jan. 2022.

MONAHAN, Sean T. **Who will lead the "Fourth Industrial Revolution?"** Disponível em: https://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=124030788&S=R&D=bth

&EbscoContent=dGJyMNLr40Sep7I40dvuOLCmsEmepq9Sr6a4SrGWxWXS&ContentCustomer=dGJyMPGssk62qbNRuePfgeyx44Dt6fIA. Acesso em: 13 set. 2021.

MONTEIRO, Renato Leite. **Existe um direito à explicação na lei geral de proteção de dados do Brasil.** 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf. Acesso em: 19 jan. 2022.

MORAIS, I. S. **Introdução a Big Data e Internet das Coisas (IoT).** Porto Alegre: SAGAH, 2018.

NAKAMURA, Emilio Tissato; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. **Metodologia de avaliação de riscos e medidas de segurança na proteção de dados.** Disponível em: https://sbseg2019.ime.usp.br/anais/197877.pdf. Acesso em: 14 dez. 2021.

NURSE, Jason R. C.; CREESE, Sadie; ROURE, David de. Security Risk Assessment in Internet of Things Systems. **IT Professional,** v. 19, n. 5, 2017. Disponível em: https://ieeexplore.ieee.org/document/8057728. Acesso em: 19 abr. 2021.

OLIVEIRA, João Pedro Costa Perdigão Maia. **O acesso à informação na administração pública, no contexto do regime geral de proteção de dados pessoais e das tecnologias da informação.** 117f. 2020. Dissertação (Mestrado em Direito e Prática Jurídica) – Universidade de Lisboa. Lisboa. 2020.

OMS. Organização Pan-Americana da Saúde (OMS). **OMS declara emergência de saúde pública de importância internacional por surto de novo coronavírus**. Disponível em: https://www.paho.org/bra/ index.php?option=com_content&view=ar ticle&id=6100:oms-declara-emergencia-de-saude-publica-de-importancia-internacional-em-relacao-a-novo-coronavirus&Itemid=812. Acesso em: 30 jan. 2020.

ONU. Organização Das Nações Unidas. **Declaração Universal dos Direitos Humanos.** Disponível em: https://brasil.un.org/pt-br/91601-declaracao-universal-dos-direitos-humanos. Acesso em: 15 abr. 2021

PANEK, Lin Cristina Tung. **Lei geral de proteção de dados nº 13.709/2018:** uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019. 35f. Monografia (Curso de Direito) - Universidade Federal do Paraná, Curitiba, 2019.

PERASSO, Valeria. **O que é a 4ª revolução industrial - e como ela deve afetar nossas vidas.** BBC Brasil, 2016. Disponível em: https://g1.globo.com/economia/negocios/noticia/2016/10/o-que-e-a-4a-revolucao-industrial-e-como-ela-deve-afetar-nossas-vidas.html. Acesso em: 23 jan. 2022.

PESSOA, Larissa Rocha de Paula. **Os desafios da governança de dados e a realidade cultural brasileira.** 2021. 152f. Dissertação (Mestrado em Direito) – Universidade Federal do Ceará, Fortaleza, 2021.

PINHEIRO, Patrícia Peck. **LGPD:** os prós e contras de prorrogar a Lei para 2022. Disponível em: https://www.cryptoid.com.br/identidade-digital-destaques/lgpd-os-pros-e-contras-de-prorrogar-a-lei-para-2022/. Acesso em: 18 set. 2021.

POLIDO, Fabrício B. Pasquot et al. **Instituto de Referência em internet e sociedade:** GDPR e suas repercussões no direito brasileiro. 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-IRIS-1.pdf. Acesso em: 12 jan. 2021.

PONCE, Silvana. **Panorama Geral ISO 27001:2013/ISO 27701:2020:** Sistema de Gestão da Segurança e Informação/Sistema de Gestão de Informação Privada. QMS Brasil. Disponível em: https://qmsbrasil.com.br/wp-content/uploads/2021/06/iso-27001-iso-27701-compactado.pdf. Acesso em: 12 ago. 2021.

PORTER, Michel E. **Competitive advantage:** creating and sustaining superior performance, New York: The Free Press, 1998.

PR NEWSWIRE. **Building Trust with Data Security - Why Explorium got** ISO/**IEC** 27701 **certification.** Disponível em: https://web.p.ebscohost.com/ehost/detail/detail?vid=7&sid=ef79619a-4613-4b4e-9e9a-d43b065e4c22%40redis&bdata=JkF1dGhUeXBlPWlwLHNoaWImbGFuZz1wdC1iciZzaXRlPWVob3N0LWxpdmU%3d#AN=202104280000PR.NEWS.USPR.UN55136&db=bwh. Acesso em: 05 mar. 2022.

PwC. **Transformação Digital - der gr o € ßte Wandel seit der Industriellen Revolution**. Frankfurt: PricewaterhouseCoopers. 2013.

REIS, Beatriz de Felippe. A cultura de compliance em matéria de proteção de dados e sua adoção no âmbito laboral. **Revista de Direito do Trabalho,** v. 214, p. 323-340, nov./dez. 2020. Disponível em: https://juslaboris.tst.jus.br/handle/20.500.12178/180571. Acesso em: 13 set. 2021.

ROCHA, Camila et al. Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. **Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará,** v. 2, n. 3, p. 78-97, ago. 2019. Disponível em: http://www.revistasfap.com/ojs3/index.php/tic/article/view/285. Acesso em: 10 mar. 2021.

RODRIGUES, Murilo Ramos Alambert. **Gestão Estratégica.** Rio de Janeiro: Editora FGV, 2012.

ROGERS, David L. **Transformação digital:** repensando o seu negócio para a era digital. Tradução de: Afonso Celso da Cunha Serra. São Paulo: Autêntica Business, 2017.

ROJKO, Andreja. Industry 4.0 Concept: Background and Overview. **International Journal of Interactive Mobile Technologies,** p. 77-90. 2017. Disponível em: https://online-journals.org/index.php/i-jim/article/view/7072. Acesso em: 17 jun. 2022.

SALDANHA, Paolma Mendes (Coord.). **O que estão fazendo com meus dados?** A importância da lei geral de proteção de dados. Recife: Serifafina, 2019. Disponível em: <https://www.udop.com.br/download/noticias/2020/03_03_20_arquivo_oab_pe.pdf>. Acesso em: 6 fev. 2022.

SAMPAIO, Rafael de. **Vantagem digital:** um guia prático para a transformação digital. Editora Alta Books, 2018. *e-book.*

SANTINI, Barbara et al. A eficácia da Lei Geral de Proteção de Dados (LGPD). In: SALDANHA, Paloma Mendes (Org.). **O que estão fazendo com meus dados?** A importância da Lei Geral de Proteção de Dados. Recife: SerifaFina, 2019. p. 19-30.

SANTOS, Bruno Pereira et al. **Internet das coisas:** da teoria à prática. Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. 2016. Disponível em: http://www.sbrc2016.ufba.br/minicurso/minicurso-1/. Acesso em: 01 set. 2021.

SANTOS, Renato Almeida dos et al. Compliance and leadership: the susceptibility of leaders to the risk of corruption in organizations. **Einstein¸** v. 10, n. 1, p. 1-10, jan.;mar. 2012.

SATO, Silvio Koiti. **Mobilidade, comunicação e consumo: expressões da telefonia celular em Angola, Brasil e Portugal.** 2015. 366f. Tese (Doutorado em Comunicação) - Universidade de São Paulo, São Paulo, 2015.

SCHALLMO, Daniel; WILLIAMS, Christopher; LUKE, Boardman. Digital Transformation of Business Models — Best Practice, Enablers, and Roadmap. **Ingernational Journal of Innovation Management,** v. 21, n. 1, nov. 2017. Disponível em: https://www.researchgate.net/publication/321394754_DIGITAL_TRANSFORMATION_OF_BUSINESS_MODELS_-_BEST_PRACTICE_ENABLERS_AND_ROADMAP. Acesso em: 18 mar. 2022.

SCHIRMER, Dara Luana; THAINES, Aleteia Hummes. A implementação da Lei Geral de Proteção de Dados nas rotinas dos profissionais da área contábil: percepções dos contabilistas associados à associação dos contabilistas do Vale do Paranhana/RS. **Revista Eletrônica de Ciências Contábeis,** v. 10, n. 1, p. 31-56, 2021. Disponível em: https://seer.faccat.br/index.php/contabeis/article/view/1956. Acesso em: 15 jun. 2022.

SCHWAB, Klaus; DAVIS Nicholas. **A Quarta Revolução Industrial.** Tradução de: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SPHIPMAN, Alan; WATKINS, Steve. **ISO/IEC 27701:2019 Na introduction to privacy information management.** Cambridgeshire CB7 4EA Reino Unido, 2020.

SCHWAB, Klaus; DAVIS Nicholas; MIRANDA, Daniel Moreira. **Aplicando a Quarta Revolução Industrial.** Tradução de: Daniel Moreira Miranda. São Paulo: Edipro, 2018.

SEMESP. Excelência a Serviço do Ensino Superior. **Guia framework de inovação para IEs**. 2º Seminário o futuro do Ensino Superior. São Paulo. 2018. Disponível em: https://www.semesp.org.br/wpcontent/uploads/2018/08/E-book-Guia-Framework-inova%C3%A7%C3%A3o-1-1.pdf. Acesso em: 28 mar. 2021.

SHORES, Robert Daniel; OLIVEIRA, André. **Conhecendo a lei geral de proteção de dados do Brasil – LGPD.** Disponível em: https://www.daniel-ip.com/wp-content/uploads/2019/02/Daniel_Cartilha_LGPD_atual_fev2019.pdf. Acesso em: 11 jan. 2022.

SIBILLE, Daniel; SERPA, Alexandre; FARIA, Felipe. **Os pilares do programa de compliance:** uma breve discussão. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/BibliotecaDigital/BibDigitalLivros/TodosOsLivros/Os-pilares-do-programa-de-compliance.pdf. Acesso em: 12 mar. 2022.

SILVA, Aline Gama da; LOPES, Paloma de Lavor; MOURA, Renan Gomes de; BARBOSA, Marcus Vinicíus. Mecanismos de compliance em instituições de ensino superior. **Revista Valore,** 4. ed. p. 317-330. 2019. Disponível em: https://revistavalore.emnuvens.com.br/valore/article/download/373/274. Acesso em: 02 fev. 2022.

SILVA, Bitencourt da; KLINGENBERG, Cristina. **Estratégias para o desenvolvimento de inovações sociais voltadas a promoção de resiliência frente ao impacto gerado pelas tecnologias da quarta revolução indústria.** Disponível em: https://www.researchgate.net/publication/328190096_ESTRATEGIAS_PARA_O_DESENVOLVIMENTO_DE_INOVACOES_SOCIAIS_VOLTADAS_A_PROMOCAO_DE_RESILIENCIA_FRENTE_AO_IMPACTO_GERADO_PELAS_TECNOLOGIAS_DA_QUARTA_REVOLUCAO_INDUSTRIAL. Acesso em: 20 mar. 2021.

SILVA, Daniel Cavalcante; COVAC, José Roberto. ***Compliance* como boa prática de gestão no ensino superior privado.** Disponível em: https://periodicos.uninove.br. Acesso em: 15 out. 2021.

SILVA, Kátia Rejane da; LARANJA, Patricia Colona; OLIVEIRA, Adriana Carla Silva de. A importância do *compliance* no plano de gestão do centro de biociências da Universidade Federal do Rio Grande Norte. In: GUIMARÃES, Patrícia et al. (Org.). **Compliance:** estudos interdisciplinares aplicados na gestão de instituições de ensino superior públicas. Natal, RN: EDUFRN, 2018. p. 27-54.

SILVA, Luiz Gustavo Pereira da; LEMOS, Thiago Oliveira; RUFINO, Hugo Leonardo Pereira. **O impacto da Internet das Coisas na educação:** uma revisão. Disponível em: https://rsdjournal.org/index.php/rsd/article/view/7770/6919. Acesso em: 15 set. 2021.

SIVIERI, Edson Vicente. **Estruturação do departamento de segurança da informação para atender a gestão de dados em conformidade à lei geral de proteção de privacidade de dados (LGPD)**. 2021. 37f. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/20088/1/TCC_Edson_Sivieri.pdf . Acesso em: 11 dez. 2021.

SOUZA, Nicole Bêtta de; ACHA. Fernanda Rosa. A proteção de dados como direito fundamental: uma análise a partir da emenda constitucional 115/2022. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v.8, n.09, set.2022. Disponível em:<https://periodicorease.pro.br/rease/article/view/6822/2667>. Acesso em: 20 dez. 2022.

TALYA, Akanksha Manik; MATTOX, Matt. **GE's Digital Industrial Transformation Playbook, General Electrics.** 2016. Disponível em: https://fhi.nl/app/uploads/sites/5/2021/02/NOVOTEK-ge-digital-industrial-transformation-playbook-whitepaper.pdf. Acesso em: 23 jan. 2022.

TEIXEIRA, Tarcisio; ARMELIN, Ruth Maria Guerreiro da Fonseca. **Lei Geral de Proteção de Dados Pessoais:** comentada artigo por artigo. Salvador: JusPODIVM, 2020.

TRELEAVEN, Philip; BROWN, Richard Gendal; YANG, Danny. **The banking and financial-services industry has taken notice of blockchain technology's many advantages.** This special issue explores its unlikely origins, tremendous impact, implementation challenges, and enormous potential. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8048631. Acesso em: 28 ago 2021.

UNIRV. Universidade de Rio Verde. **Institucional**. Disponível em: http://www.unirv.edu.br/paginas.php?id=12. Acesso em: 18 mar. 2021.

VENTURA, Ivan. **A relação entre a lei de proteção de dados e o ingresso do Brasil no OCDE.** mar. 2019. Disponível em: https://www.consumidormoderno.com.br/2019/03/20/relacao-lgpd-desejo-brasil-ocde/. Acesso em: 03 fev. 2022.

VIAL, Gregory. Understanding digital transformation: a review and a research agenda. **The Journal of Strategic Information Systems,** v. 28, n. 2, p. 118-144, 2019.

WADE, Michael. **Digital Business Transformation**. IMD and Cisco, Working Paper, p. 1-16, 2017.

WEF. World Economic Forum. **Deep Shift Technology Tipping Points and Societal Impact, Survey Report, Global Agenda Council on the Future of Software & Society.** 2015. Disponível em: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. Acesso: em 20 jan. 2021.

WEILL, Peter; WOERNER Stephanie. **Qual o seu modelo digital de negócio?** São Paulo: M. Books do Brasil, 2019.

WHO. World Health Organization. **Coronavirus disease (COVID-19**). Disponível em: https://www.who.int/emergencIEs/diseases/novel-coronavirus-2019?gclid=Cj0KCQjwse-DBhC7ARIsAI8YcWIoKU2JK-ceoeVnZcZYV6NPO86b4XD2VZLBkQwHET_X8dNSs5mvekMaAgH5EALw_wcB. Acesso em: 18 abr. 2021.

WOLFANG, Hoffamann-Riem. **Teoria geral do direito digital:** transformação digital - desafios para o direito. Rio de Janeiro: Forense, 2021.

XAVIER, Deiverson Felipe Souza et al. **Compliance uma ferramenta estratégica para a segurança das informações nas organizações**. In: SIMPÓSIO Internacional de gestão de projetos, inovação e sustentabilidade, 6, São Paulo, nov. 2017. Disponível em: http://www.singep.org.br/6singep/resultado/429.pdf. Acesso em: 14 set. 2021.

YOO, Youngjin et al. **Organizing for innovation in the digital world**. Organization Science, v. 23, n. 5, p. 1398-1408, 2012. Disponível em: https://aaltodoc.aalto.fi/bitstream/handle/123456789/16540/isbn9789526062433.pdf?sequence=1&isAllowed=y. Acesso em: 26 maio 2021.