FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO "RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Aécio Aparecido da Silva

APLICAÇÃO E ADEQUAÇÃO À MUTABILIDADE SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS

Americana/SP

2023

FACULDADE DE TECNOLOGIA DE AMERICANA – MINISTRO RALPH BIASI

Curso Superior de Tecnologia em Segurança da Informação

Aécio Aparecido da Silva

APLICAÇÃO E ADEQUAÇÃO À MUTABILIDADE SOCIAL DA LEI GERAL DE PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Profª. Dra. Maria Cristina Aranda.

Área de concentração: Segurança da Informação

Americana/SP.

2023

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi-CEETEPS Dados Internacionais de Catalogação-na-fonte

SILVA, Aécio Aparecido da

Aplicação e adequação à mutabilidade social da Lei Geral de Proteção de Dados. / Aécio Aparecido da Silva – Americana, 2023.

44f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientadora: Profa. Dra. Maria Cristina Aranda

1. Direito 2. Direito de informática 3. Lei de tecnologia de informação. I. SILVA, Aécio Aparecido da II. ARANDA, Maria Cristina III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 34
34:681.3
34:381.3

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Aécio Aparecido da Silva

Aplicação e adequação à mutabilidade social da Lei Geral de Proteção de Dados

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana – Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 01 de dezembro de 2023

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
Fatec Americana – Ministro Ralph Biasi

Maxwel Vitorino da Silva (Membro)
Mestre
Fatec Americana – Ministro Ralph Biasi

Clerivaldo José Roccia (Membro)
Mestre
Fatec Americana – Ministro Ralph Biasi

AGRADECIMENTOS

Em primeiro lugar agradeço a todos aqueles que contribuíram, direta ou indiretamente para eu trilhar esse caminho. Agradeço aos colaboradores, funcionários e professores da Fatec Americana. Continuamente agradeço também aos meus familiares que mesmo distantes de alguma forma também fizeram parte desta jornada. Deixei para agradecer por último, aquela que em nível de importância é a primeira, agradeço a Eloá Crystini de Oliveira e Silva, filha, amiga e parceira, pessoa impar, que ostenta local de estrema relevância em minha vida e que a minha pessoa jamais poderia deixar de agradecer. A todos aqueles aqui citado e a muitos outros coadjuvantes o meu MUITO OBRIGADO.

DEDICATÓRIA

Dedico este estudo;
aos meus pais, Manoel e Helena, “in memoriam”;
a razão da minha vida, minha princesa, minha filha Eloá;
ao meu irmão, Acácio;
à minha irmã, Aline;
aos meus sobrinhos Erick e Ayla
e a minha namorada / amiga / irmã / esposa Soraia.

RESUMO

O presente trabalho procurou demonstrar, de forma clara e objetiva, a importância de uma legislação para regulamentar o tratamento dos dados pessoais, analisando a Lei Geral de Proteção de Dados (LGPD), no que tange à sua criação, aplicação, conceitos, tratamentos de dados, de forma paralela com as premissas do direito fundamental à privacidade e todas as Legislações esparsas que se remetem ao tema. Foi observado, durante o estudo, que a LGPD traz importantes inovações para o contexto brasileiro, refletindo influências e princípios comuns encontrados em regulamentações internacionais de proteção de dados, possibilitando adequação, as normas pertinentes e as legislações que regulam o mundo cibernético, trazendo também consigo uma nova abordagem das temáticas de tratamento de dados pessoais, garantindo ainda mais o direito fundamental da privacidade aos cidadãos. Nesse contexto, uma criteriosa investigação foi conduzida para esclarecer se a tutela jurídica, bem como diversas informações derivadas de documentos pessoais, exercem alguma influência sobre a representação virtual da pessoa humana perante a sociedade. Além disso, foi abordada a construção histórica da lei, os conceitos relacionados aos dados pessoais no contexto tecnológico, as abordagens no tratamento desses dados, os direitos à privacidade e à informação. Por fim, o trabalho incluiu uma análise e comparação de várias legislações pertinentes ao tema, incluindo o Regulamento Geral de Proteção de Dados da Europa, que tem servido como referência para a elaboração de regulamentações similares em níveis nacional e regional em todo o mundo.

Palavras-Chave: Código Civil. Código de Defesa do Consumidor. Constituição Federal. Segurança da Informação. LGPD

ABSTRACT

This work demonstrates, in a clear and objective way, the need from legislation to regulations the processing of personal data, analyzing the The General Data Protection Law (LGPD), not regarding its creation, application, concepts, data processing, in parallel with the indications of the fundamental right to privacy and all the scattered Legislation that refer to the topic. It was observed, during the study, that the LGPD brings important innovations for the Brazilian context, reflecting common influences and principles found in international data protection regulations, enabling adaptation, relevant standards and legislation that regulate the cyber world, also bringing a new approach to personal data processing issues, further guaranteeing the fundamental right to privacy for citizens. In this context, a careful investigation was conducted to clarify whether legal protection, as well as various information derived from personal documents, exert any influence on the virtual representation of the human person before society. Furthermore, the historical construction of the law, concepts related to personal data in the technological context, approaches to processing this data, and the rights to privacy and information were addressed. Finally, the work included an analysis and comparison of various legislation relevant to the topic, including the European General Data Protection Regulation, which has served as a reference for the development of similar regulations at national and regional levels around the world.

Keywords: Civil Code. Consumer Protection Code. Federal Constitution. Information Security. LGPD.

SUMÁRIO

RESUMO.....6
1. INTRODUÇÃO.....9
2. LEI GERAL DE PROTEÇÃO DE DADOS.....12
2.1. Contexto Histórico da LGPD.....12
2.2. Marco Civil da Internet e sua Importância na Formulação da LGPD.....13
2.3. Resumo da Legislação Esculpida na LGPD.....13
2.4. Do Funcionamento da LGPD.....15
2.5. O Tratamento dos Dados na Posse das Empresas.....16
2.6. O Mercado em Face à LGPD.....17
3. OUTRAS LEGISLAÇÕES ATINENTES AO TEMA LGPD.....19
3.1. *Compliance*.....19
3.1.1. A *Compliance* e sua Importância na LGPD.....20
3.2. Direito a Privacidade.....21
3.3. Os Direitos da Personalidade da Segurança da Informação.....24
3.4. A Proteção da Criança e do Adolescente em Face da LGPD.....25
4. OS DADOS PESSOAIS E SUA PROTEÇÃO.....28
5. O DANO QUE EXTRAPOLA O AMBITO DA LGPD SE PERFAZENDO EM RESPONSABILIDADE CIVIL.....30
5.1. Noções Precedentes da Responsabilidade Civil.....30
5.2. Responsabilidade Objetiva.....33
5.3. Responsabilidade Subjetiva.....35
6. CONCLUSÃO.....39
REFERÊNCIAS.....42

1. INTRODUÇÃO

A Lei Geral de Proteção de Dados – LGPD não é uma legislação criada recentemente, o tema foi lançado para consulta pública pelo Ministério da Justiça, por meio de uma plataforma *online*, que permitia ampla contribuição pelos indivíduos e empresas, isso a partir de 2006. Com o passar dos anos e com a mutação natural do meio social fizeram com que fossem criados três projetos de Leis principais: 4.060/2012, 330/2013, 5.276/2016, os quais foram fundamentais para a construção do Projeto de Lei n° 53/2018, que viria a ser aprovada pelo Congresso Nacional e sancionada pela Presidência da República em 14 de agosto de 2018. Dentre esses fatores importantes para a criação da Lei Específica, pode-se citar a CPI da Espionagem, a aprovação do Marco Civil da Internet e a entrada em vigor, em maio de 2018 do Regulamento Geral sobre a Proteção de Dados (RGPD/GDPR) da União Europeia.

Necessário se pontuar e atribuir os créditos merecidos a alguns fatores extremamente importantes no histórico de evolução que resultou na criação da LGPD e já lembrados nessa introdução são eles, a CPI da Espionagem, a aprovação do Marco Civil da Internet e a entrada em vigor, em maio de 2018 do Regulamento Geral sobre a Proteção de Dados (RGPD/GDPR) da União Europeia.

A legislação especifica quando aborda o mundo digital, tem em seu escopo a necessidade de um diálogo constante entre o Direito e a Tecnologia, pois o Direito nasce da dicotomia entre dados pessoais e dados anônimos para a proteção dos primeiros. Entretanto a tecnologia atualmente se apresenta complexa de ser acompanhada ou regida por uma lei escrita que consiga abranger de forma plena todos as divergências que dessa relação possam advir.

Se assim for entendido, escrever e entender sobre o direito fundamental a privacidade na Internet e as leis específicas sobre os temas e as legislações esparsas, não é apenas oportuno, mas, é essencial para que a tutela jurisdicional seja prestada da melhor forma possível.

Escrever sobre a proteção do estado prestada pelo judiciário, sendo o estado um ente que tem o poder dever de parametrizar os limites de direito no mundo virtual, com uma abordagem à necessidade de um diálogo constante, entre o Direito e a Tecnologia, pois assim como na sociedade real que evolui constantemente obrigando as leis a acompanhar essa evolução. No meio virtual essa evolução é

infinitamente maior e de maior lastreamento, desafiando nossos legisladores a acompanhar essa evolução desenfreada de modo a regulá-la com a criação e colocação de novas leis em vigor munidas de eficácia.

A proteção e regulamentação da política de tratamento de dados e não só, mas também, de muitas ações que quando praticadas no mundo virtual ainda não encontram legislação específica para se enquadrar, tendo que aplicar leis aproximadas ou jurisprudências equiparadas para se chegar a uma decisão jurisdicional não questionável, pautada em legalidade, imparcialidade e justiça.

O presente trabalho tem o propósito de analisar as diretrizes e aplicação da Lei Geral de Proteção de Dados (LGPD) a par de outras legislações específicas que também se aderem ao tema assim como as leis básicas que não foram criadas pensando em doutrinar o mundo tecnológico, mas que também servem de base para a regularização das ações praticada no mundo virtual como o Código Civil, Código Penal, Constituição Federal dentre outros.

A Lei só se torna de forma incontestável Lei, quando esta adquire eficácia dentro do meio social, ou seja, quando a lei que foi criada e implementada para devida finalidade realmente passa a ser respeitada e a ação por ela combatida realmente é regulada seja por punição, seja por indenização seja por simples regulamentação na forma que os legisladores imaginaram antes da validação.

Destarte que, o cerne do trabalho é trazer um panorama atual e social das aplicações positivadas na Lei Geral de Proteção de Dados – LGPD e escoltada pelas leis esparsas e outras legislações atinentes diante de uma sociedade plenamente mutável e que se altera no mundo virtual e tecnológico muito além do que as novas leis criadas possam ou consigam doutrinar.

Para o desenvolvimento deste trabalho, foi realizada uma análise retrospectiva, a fim de compreender de maneira clara e objetiva como o direito à privacidade evoluiu ao longo do tempo e qual foi o impacto dos avanços tecnológicos na proteção de dados pessoais. Em meio a essa evolução muitos fatores buscaram acompanhar na tentativa de oferecer mais segurança aos usuários, é o caso da legislação brasileira e dos operadores e usuários/consumidores das áreas que trafegam sob o manto da Tecnologia da Informação. Essa compreensão é fundamental para reconhecer o direito à privacidade como um direito fundamental, o que culmina na criação da Lei Geral de Proteção de Dados Pessoais (LGPD).

Objetiva-se também esclarecer que a direção que se toma no contexto do mundo digital é assegurar que as informações coletadas recebam um tratamento apropriado, livres riscos e preservado em sua integridade. Além disso, busca-se garantir que as pessoas tenham o controle sobre os seus próprios dados pessoais fornecidos às empresas, possibilitando a modificação, correção ou exclusão dessas informações. A LGPD foi estabelecida com o propósito de garantir esse direito, seguindo o exemplo de outras nações que já implementaram mecanismos de fiscalização semelhantes como o Regulamento Geral de Proteção de Dados (GDPR) aplicado aos países da União Europeia, a Lei de Proteção de Dados Pessoais (APPI) implementada no Japão em 2005, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) implementada no Canadá dentre outras, sendo todas sem exceção direcionadas proteger a privacidade dos cidadãos e estabelecer diretrizes para o tratamento responsável e seguro de dados pessoais.

Por fim, o presente trabalho vem então, expor algumas noções acerca das teorias para o tratamento de dados pessoais, e aplicações da legislação às ações ocorridas no mundo virtual diante da intensa evolução tecnológica, conforme apresentado, e evidenciar se tanto o Direito à Privacidade quanto o Direito a Proteção de Dados tendo como base a proteção da personalidade jurídica e o princípio da dignidade humana.

2. LEI GERAL DE PROTEÇÃO DE DADOS

2.1. Contexto Histórico da LGPD

O cenário para a regulamentação de dados tornou-se proeminente no ano de 2016, com a introdução do Regulamento Geral de Proteção de Dados (GDPR) na União Europeia. Nesse período, o mundo estava enfrentando questões de privacidade notáveis, envolvendo o *Facebook*, umas das redes sociais mais populares e amplamente utilizada pelo mundo, fundada por Mark Zuckerberg e seus colegas de quarto em 2004 e a *Cambridge Analytica* que foi a empresa de análise de dados que se envolveu à época em uma polêmica significativa relacionada à coleta e uso indevido de dados pessoais de usuários do *Facebook* para fins políticos. Esse destaque levou o tema a ganhar espaço na agenda da política nacional, uma vez que não havia uma legislação específica para assegurar a proteção dos dados pessoais.

O Brasil já possuía outras leis que garantiam o direito à privacidade, como a Lei de Acesso à Informação (Lei n. 12.527, de 18 de novembro de 2011), a Lei Carolina Dieckman (Lei n. 12.737, de 30 de novembro de 2012) e o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014), mas nenhuma delas tratava especificamente da proteção de dados.

Em agosto de 2018, a Lei Nacional de Proteção de Dados foi promulgada e publicada no Diário Oficial da União. Após ser sancionada, houve um veto à criação da Autoridade Nacional de Proteção de Dados (ANPD), fazendo com que os legisladores determinassem que *Vacatio Legis* fosse de 18 meses e desta forma o regulamento só entraria em vigor, em fevereiro de 2020. Por várias razões, incluindo à particularidade da crise causada pela Covid-19 que o Brasil e o mundo atravessava naquela época, um pedido de prorrogação do período de *vacância* da mencionada Lei de Proteção de Dados Pessoais foi processado e somente em 18 de setembro de 2020 a LGPD entrou em vigor, com o devido sancionamento pelo Presidente da República da Lei 14.058 de 17 de setembro de 2020.

A LGPD passou a vigorar com base em princípios que visam garantir a proteção dos dados pessoais dos cidadãos, estabelecendo direitos e responsabilidades tanto para pessoas físicas, proprietária dos dados pessoais, quanto para empresas que lidam com dados destas pessoas. A lei busca proteger a

privacidade e a segurança dos dados em um contexto digital em constante e acelerada evolução.

2.2. Marco Civil da Internet e sua Importância na Formulação da LGPD

Diante do tema explorado, é importante mencionar a Lei nº 12.965/2014, conhecida como Marco Civil da Internet/MCI, que desempenha um papel fundamental nas relações humanas protegidas através da Internet.

Conforme destacado por Bioni (2018, p. 127), o MCI foi uma iniciativa da sociedade civil brasileira para evitar que o Poder Legislativo regulamentasse a Internet exclusivamente por meio de leis penais. Nesse contexto, o Marco Civil da Internet foi estabelecido como um marco regulatório que visa garantir os direitos e garantias dos cidadãos no mundo virtual.

Foi compreendido que o Marco Civil da Internet (MCI) foi elaborado com o propósito de estabelecer uma regulamentação legal das atividades no meio eletrônico. O Direito Digital no Brasil representou um marco inicial, uma vez que, até então, as relações na Internet eram tratadas por meio de legislações não específicas. Nesse contexto, aplicavam-se leis relacionadas ao direito penal, direito autoral e direito da personalidade, entre outras.

Além disso, é importante destacar que o MCI apresentou uma notável omissão no que diz respeito aos dados pessoais no âmbito do direito digital brasileiro. Embora tenha conseguido as relações jurídicas virtuais e seus impactos, bem como tratado dos crimes cibernéticos, não deu orientações claras sobre como as empresas deveriam lidar com os dados gerados pelos usuários (BASTOS, 2020, p. 1). Nesse contexto, fica evidente a importância da Lei Geral de Proteção de Dados na proteção e segurança tanto dos proprietários dos dados assim como dos portadores dos dados.

2.3. Resumo da Legislação Esculpida na LGPD

A LGPD tem gerado significativas mudanças em empresas de todos os setores, abordando o tratamento de dados pessoais. Seu principal propósito é resguardar as informações pessoais de indivíduos. As etapas de adaptação das

empresas à LGPD são, essencialmente, semelhantes às implementações de programas de conformidade (PALHARES; PRADO; VIDIGAL, 2021).

A legislação, em essência, corresponde à regulamentação do tratamento de dados pessoais, abrangendo todas as atividades relacionadas a esses dados, desde sua entrada nos sistemas das empresas até sua remoção desses sistemas (PALHARES; PRADO; VIDIGAL, 2021).

Segundo a Lei, o tratamento de dados engloba todas as ações possíveis em relação aos dados pessoais, realizadas por empresas, órgãos públicos ou profissionais autônomos. A Lei tem como finalidade estabelecer as diretrizes para o que pode ou não ser feito com dados pessoais a partir de sua coleta.

Conforme o artigo 3º da LGPD, a Lei é aplicável a todas as operações de tratamento de dados pessoais, independentemente de serem realizadas no Brasil, desde que envolvam a oferta de bens ou serviços a titulares de dados que estejam no Brasil (sejam gratuitos ou pagos) e envolvam dados pessoais coletados no país. O artigo 4º da Lei apresenta exceções à sua aplicação, excluindo situações de natureza pessoal, não econômica, bem como atividades estritamente jornalísticas, artísticas, acadêmicas, de segurança pública, defesa nacional e investigação e repressão de infrações penais, desde que não haja conexão com o Brasil em todo o processo.

Ao analisar a Lei, é possível observar que o artigo 6º estabelece uma série de princípios a serem seguidos no tratamento de dados pessoais, incluindo adequação, finalidade, livre acesso, não discriminação, necessidade, prevenção, qualidade de dados e responsabilização.

Já o artigo 5º da Lei diferencia dados pessoais de dados pessoais sensíveis, com estes últimos abrangendo informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, dados de saúde, dados genéticos e biométricos quando vinculados a indivíduos.

Tratando dos artigos 7º e 11º da LGPD esses detalham as condições sob as quais dados pessoais e dados pessoais sensíveis podem ser processados, exigindo consentimento legal, cumprimento de obrigações legais ou regulatórias, execução de políticas públicas, estudos por órgãos de pesquisa, exercício de direitos em processos judiciais, proteção da vida e saúde, entre outras circunstâncias específicas.

Portanto, o principal objetivo do legislador que trabalhou na criação da Lei foi salvaguardar dados pessoais e garantir que empresas e órgãos cumpram os requisitos estabelecidos, promovendo a conformidade entre a legislação e o uso de dados pessoais.

2.4. Do Funcionamento da LGPD

A Lei estabelece diretrizes relacionadas à coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo rigorosos procedimentos e aplicando sanções em casos de não conformidade. Essa legislação se aplica a todas as entidades, sejam elas pessoas físicas ou jurídicas, de caráter público ou privado, que se envolvam no tratamento de dados pessoais de indivíduos.

Os dados pessoais são informações que possibilitam a identificação direta ou indireta de uma pessoa, incluindo itens como CPF, RG, passaporte, carteira de habilitação, endereço, telefone, *e-mail*, endereço de IP e *cookies*.

O artigo 5º da LGPD (BRASIL, 2018) aborda o conceito de dados pessoais sensíveis, englobando qualquer informação que se relacione com a origem racial ou étnica, crenças religiosas, opiniões políticas, filiação a sindicatos ou organizações de cunho religioso, filosófico ou político, bem como dados relacionados à saúde, vida sexual, informações genéticas ou biométricas quando associadas a uma pessoa natural.

Conforme mencionado, existem normas para a coleta e eliminação adequada de dados. A não observância dessas diretrizes acarreta consequências legais. O artigo 52 da Lei estabelece os tipos de sanções administrativas que a Autoridade Nacional de Proteção de Dados pode impor aos responsáveis pelo tratamento de dados, incluindo:

- Advertência com prazo para correção;
- Multa simples, que pode chegar a até 2% do faturamento da empresa responsável pela coleta de dados, limitada a R$ 50.000.000,00 (cinquenta milhões de reais);
- Multa diária, com o mesmo limite de R$ 50.000.000,00 (cinquenta milhões de reais);
- Publicização da infração;
- Bloqueio dos dados até que a situação seja regularizada;

- Eliminação dos dados envolvidos na infração.

É importante destacar que o não cumprimento das regras tem impactos significativos, não apenas em termos financeiros, devido às multas substanciais, mas também em termos de reputação, uma vez que a empresa ou organização pode perder sua credibilidade no mercado e junto aos clientes.

2.5. O Tratamento dos Dados na Posse das Empresas

Diversos intervenientes participam do processo de armazenamento de dados, começando pelo Titular, que detém e é o proprietário dos dados pessoais, seguido pelo Controlador, que pode ser uma pessoa física ou jurídica responsável por determinar como o tratamento dos dados será realizado. O Operador, seja uma pessoa física ou jurídica, desempenha a função de realizar o tratamento em nome do Controlador. O Encarregado atua como intermediário designado pelo Controlador para facilitar a comunicação entre o Controlador, o Titular e a Autoridade Nacional de Proteção de Dados (ANPD). Por último, mas não menos importante, temos a ANPD, que tem a responsabilidade de supervisionar o cumprimento da LGPD.

A lei também aborda o ciclo de vida dos dados, desde sua entrada em uma empresa ou organização até seu descarte. Esse ciclo compreende cinco etapas:

- Coleta, que envolve a aquisição inicial dos dados;
- Processamento, que diz respeito à forma como os dados serão utilizados;
- Compartilhamento, indicando com quem os dados e informações serão compartilhados;
- Armazenamento, especificando como os dados serão mantidos;
- Descarte, determinando quando, como e por que os dados são eliminados, requerendo políticas específicas para a eliminação de dados e informações coletadas.

Na coleta de dados, as empresas devem assegurar o consentimento expresso e específico do Titular, proibindo o uso de aprovações genéricas. Dados previamente coletados devem obter autorização de seus Titulares para continuar a serem arquivados e podem ser utilizados para várias finalidades.

Para se adequar à LGPD, as empresas devem analisar em qual âmbito, setor e segmento estão inseridas, uma vez que cada segmento possui riscos e requisitos específicos. Embora a Lei se aplique a todos, a forma como cada área deve agir é

particular. Nesse contexto, os programas de *compliance* auxiliam na gestão de riscos e na implementação eficaz da Lei, conduzindo uma análise e recomendando políticas e procedimentos que facilitem a adaptação à LGPD. Isso torna o processo mais preciso e eficaz.

Alguns passos que podem contribuir para a implementação da LGPD incluem a conscientização e a capacitação. A empresa que manifesta interesse e iniciativa na aplicação da Lei está à frente de outras. Nesta fase, é crucial sensibilizar toda a equipe, desde a alta administração até cargos mais baixos, sobre a importância da LGPD por meio de treinamentos conduzidos pelo departamento de *Compliance* e a elaboração de políticas, manuais e diretrizes para conscientizar os funcionários sobre a proteção de dados.

O mapeamento de dados é uma etapa subsequente que permite identificar quais áreas e profissionais manipulam as informações e como ocorre a troca e o fluxo de dados entre eles.

Após o mapeamento, uma análise de riscos deve ser realizada para identificar situações que possam resultar em problemas que exijam gerenciamento de crises, a fim de evitá-los. Isso é seguido por um plano de ação para priorizar demandas e analisar riscos, culminando na criação de políticas, manuais e treinamentos institucionais.

Na fase de implementação, uma vez que a importância da LGPD tenha sido amplamente divulgada, é hora de introduzir tecnologias, ferramentas e disseminar os códigos e políticas internas para uma adaptação eficaz à Lei.

Por fim, no que diz respeito ao monitoramento, todo o processo deve estar em constante evolução para sua efetivação. Esse monitoramento deve ser realizado pelo departamento de *compliance*, com a manutenção e atualização dos dados necessários e das políticas, para garantir que a implementação esteja em conformidade com a Lei.

2.6. O Mercado em Face à LGPD

Além de cumprir com as obrigações legais, que são inegavelmente fundamentais, as empresas que optam em aderir à LGPD desfrutam de uma série de vantagens em relação às demais no mercado.

Os benefícios associados à conformidade com a LGPD transcendem a mera adesão à legislação, uma vez que a implementação da LGPD impulsiona uma série de melhorias na reputação e imagem da empresa no mercado. Isso inclui o destaque em relação às empresas concorrentes, a transmissão de confiança aos clientes que sabem que a empresa trata seus dados com responsabilidade, a demonstração de cuidado com a preservação dos dados coletados e o fortalecimento das relações comerciais devido à responsabilidade sólida, o que, por sua vez, pode resultar em uma atração maior de clientes e, consequentemente, ter um impacto positivo.

Além das vantagens competitivas no mercado, a implementação da Lei, em conjunto com programas de *compliance*, previne diversos transtornos e não conformidades que poderiam surgir, incluindo multas substanciais, vulnerabilidade da empresa, exposição negativa na mídia, compartilhamento inadequado de dados, suspensão de banco de dados, proibição do tratamento de dados, danos à reputação, escândalos e um aumento no risco de enfrentar processos administrativos e judiciais.

A conformidade com a Lei representa uma oportunidade para as empresas expandirem e protegerem seus negócios, demonstrando respeito pelos dados de seus clientes e, consequentemente, construindo uma sólida credibilidade no mercado.

3. OUTRAS LEGISLAÇÕES ATINENTES AO TEMA LGPD

3.1. *Compliance*

Atualmente, o mundo está imerso em uma realidade em que as ações dos agentes públicos e privados frequentemente dominam as manchetes com casos de corrupção e os diversos impactos econômicos e sociais que deles advêm. Diante dessa situação, o conceito de *compliance*, embora relativamente novo e desconhecido por muitos, está se tornando cada vez mais proeminente tanto na mídia quanto no cotidiano das empresas brasileiras.

A ideia de *compliance* teve sua origem nos Estados Unidos, com a criação da *Prudential Securities* em 1950 e a regulamentação da *Securities and Exchange Commission* em 1960, quando surgiu a necessidade de institucionalizar programas de *compliance* visando estabelecer procedimentos internos de controle e monitoramento de operações (BERTOCCELLI, 2019).

Na Europa, em 1977, a Convenção Relativa à Obrigação de Diligência dos Bancos do Marco da Associação de Bancos Suíços estabeleceu as bases para um sistema de autorregulação de conduta, e nos Estados Unidos, em outubro de 2001, o Ato Partidário estabeleceu, em seu artigo 352, que as entidades financeiras deveriam desenvolver políticas de controle interno para proteger-se contra lavagem de dinheiro (BERTOCCELLI, 2019).

No Brasil, foram promulgadas leis que fazem parte da rotina de um programa de *compliance* e que obrigam as empresas e instituições a manterem a conformidade, como é o caso da LGPD. A Lei de Prevenção à Lavagem de Dinheiro (Lei nº 9.613, de 3 de março de 1998) trata dos crimes de lavagem de dinheiro e ocultação de bens, direitos e valores. A Lei Anticorrupção (Lei nº 12.846 de agosto de 2013) prevê sanções para empresas que praticam atos prejudiciais à administração pública, seja no âmbito nacional ou estrangeiro. Além disso, o Acordo de Leniência, presente na Lei Anticorrupção, busca facilitar a investigação de crimes e fraudes com o objetivo de recuperar recursos desviados dos cofres públicos.

No sentido literal, o termo *compliance* deriva do verbo inglês *to comply*, que significa agir de acordo com a lei. Estar em *compliance* significa estar em conformidade com as normas. Em um contexto mais amplo, o *compliance* vai além

do mero cumprimento de regras formais e deve ser compreendido como uma ferramenta para mitigar riscos e preservar valores éticos (NUNES, 2019).

Alguns dos elementos presentes em programas de *Compliance* segundo (FRAZÃO; MEDEIROS, 2018) incluem:

1. Avaliação contínua de riscos e atualização do programa.
2. Elaboração de Códigos de Ética e Conduta para orientar o comportamento na empresa.
3. Organização adequada ao risco da atividade.
4. Comprometimento da alta administração.
5. Autonomia e independência do departamento responsável pela supervisão do programa de c*ompliance*.
6. Treinamentos periódicos.
7. Promoção de uma cultura corporativa que valorize a ética e o cumprimento da lei.
8. Monitoramento constante dos controles e processos estabelecidos pelo programa de *compliance*.
9. Estabelecimento de canais seguros e abertos para denúncias e mecanismos de proteção aos informantes.
10. Detecção, investigação e punição de condutas contrárias ao programa de *compliance*.

3.1.1. A *Compliance* e sua Importância na LGPD

Após a entrada em vigor da LGPD, tornou-se evidente que os dados pertencem, de fato, aos cidadãos, portanto, para que as empresas possam fazer uso desses dados, é necessário que elas se adaptem às exigências da lei. Isso implica na necessidade de reformular a maneira como os dados pessoais são tratados, coletados, armazenados e utilizados.

Quando uma empresa coleta os dados pessoais de um cidadão, deve haver um processo transparente e documentado entre as partes. Todo o ciclo de tratamento de dados deve ser registrado e justificado, garantindo a responsabilização por parte da empresa e a veracidade dos dados coletados.

Visto que a LGPD estabelece diversos requisitos para o tratamento apropriado de dados pessoais, a finalidade do *compliance* em relação a essa lei é

atuar como uma ferramenta e um mecanismo para facilitar a transição das práticas antigas para o cumprimento da lei. O *compliance* visa garantir a adaptação às novas normas sem impactos severos.

O programa de *compliance* representa uma ferramenta crucial para as empresas, uma vez que a própria LGPD pode ser interpretada como um programa de *compliance*. Seu objetivo é regular e promover a conformidade no uso de dados pessoais. Os programas de *compliance* complementam a lei e são projetados para identificar os riscos aos quais a empresa está exposta durante o processo de adaptação (PALHARES; PRADO; VIDIGAL, 2018).

Esses programas seguem etapas bem definidas para sua implementação, incluindo o mapeamento dos riscos da área, uma análise dos riscos identificados e seu impacto, a criação de um plano de ação com a implementação de políticas, manuais, diretrizes e procedimentos, controles internos para manter a atualização dos documentos, treinamento dos colaboradores e monitoramento periódico dos procedimentos. Essas etapas auxiliam o departamento de *compliance* no processo de adaptação à conformidade com a LGPD.

Assim fica claro que, a *compliance* desempenha um papel fundamental na garantia de que as empresas estejam em conformidade com a LGPD, o que, por sua vez, protege os direitos dos titulares de dados e ajuda as organizações a evitar problemas legais, construir confiança com os clientes e gerenciar eficazmente os dados pessoais.

3.2. Direito a Privacidade

O direito à privacidade é estabelecido como um direito fundamental de acordo com o Artigo 5º, incisos X, XI e XII da Constituição Federal de 1988. No entanto, a compreensão clara da origem desse direito requer uma análise da sua evolução histórica à medida que avanços tecnológicos surgem. Para uma melhor compreensão de como a privacidade se tornou um direito fundamental, foram criadas várias retrospectivas ao longo das gerações.

A Constituição brasileira em seu artigo 5º descreve de forma pormenorizada sobre o assunto:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no país a

> inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X – 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;
> XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;
> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (BRASIL, 1988)

Para entender a origem do direito à privacidade, é necessário voltar à Constituição de 1824, também conhecida como Constituição do Império. Naquele momento, um incipiente direito à privacidade estava sendo proposto para proteger o "segredo da carta" e a "inviolabilidade da casa". Esses elementos representavam um direito emergente que estava em processo de construção. Quando Fernandez (2019, p.1) menciona o segredo da carta, refere-se à proteção do meio físico da correspondência, e não ao seu conteúdo propriamente dito.

À luz dos eventos relatados anteriormente, tornou-se evidente a necessidade de uma proteção mais abrangente para garantir a salvaguarda dos direitos aos dados pessoais. Assim sendo, em 1948, com a promulgação da Declaração Universal dos Direitos Humanos, o Direito à Privacidade foi consagrado como um direito fundamental de todas as pessoas. Tal consagração pode ser encontrada no Artigo 12 da Declaração, e sua validade permanece até os dias atuais. É importante ressaltar que:

> Ninguém sofrerá intromissões arbitrários ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Toda a pessoa tem direitos à proteção da lei contra tais intromissões ou ataques. (NAÇÕES UNIDAS, 2018, p.3).

Ao longo do tempo, o conceito de privacidade passou por diversas transformações. No passado, restringe-se principalmente à inviolabilidade das residências e ao sigilo das comunicações. No entanto, sua definição evoluiu significativamente, abrangendo uma variedade de aspectos em uma perspectiva mais ampla e tolerante. A privacidade desempenha um papel crucial na definição de limites sobre quem pode acessar dados ou informações relacionadas a corpos, locais, objetos, comunicações e informações pessoais sem autorização autorizada.

A Segurança da Informação buscou acompanhar os passos da evolução social e do mundo cibernético concentrando-se na proteção dos ativos de

informação de uma organização contra ameaças, garantindo a confidencialidade, integridade e disponibilidade desses ativos. Os pilares fundamentais da SI são frequentemente resumidos como o tripé da Segurança da Informação, que consiste em três princípios que se mantem inter-relacionados, sendo eles Confiabilidade, Integralidade e Disponibilidade.

O princípio da confidencialidade diz respeito à proteção das informações contra o acesso não autorizado. Isso significa que apenas pessoas ou sistemas autorizados têm permissão para acessar informações sensíveis. As medidas de segurança para garantir a confidencialidade incluem a implementação de controles de acesso, criptografia de dados e o uso de políticas de segurança. A integridade na SI refere-se à proteção das informações contra alterações não autorizadas ou corrupção. Em outras palavras, as informações devem permanecer precisas e completas ao longo do tempo. Para garantir a integridade, são implementados controles que rastreiam as mudanças nos dados, como assinaturas digitais, *checksums* e sistemas de controle de versão. O princípio da disponibilidade diz respeito à garantia de que as informações e sistemas estejam acessíveis quando necessário, sem interrupções não planejadas. Isso envolve a prevenção de ataques que possam interromper serviços, como ataques de negação de serviço (DDoS), bem como a implementação de planos de contingência e recuperação de desastres para lidar com interrupções.

Importante destacar que além do tripé da SI, outros princípios e conceitos trabalham em segundo plano e também são aplicados e possuem seu grau de importância na gestão da SI, são eles Autenticidade, Responsabilidade, Não Repúdio e Privacidade (LIMA, 2016, p. 184).

Esclarecendo a autenticidade se relaciona com a verificação da autenticidade das informações e a identificação das partes envolvidas em uma transação. Isso envolve a utilização de autenticação de usuário, como senhas ou autenticação de dois fatores. Enquanto a responsabilidade está relacionada com a atribuição de responsabilidades específicas para a proteção da informação e a prestação de contas das ações tomadas. Isso pode incluir políticas de segurança, treinamento de funcionários e auditorias. O princípio de não repúdio visa garantir que uma parte em uma transação não possa negar sua participação ou a autenticidade da transação. Isso é frequentemente aplicado em transações eletrônicas e pode envolver a utilização de assinaturas digitais. Já a privacidade que também é um componente

crítico da segurança da informação, envolve a proteção dos dados pessoais e a garantia de que as organizações estejam em conformidade com regulamentos de privacidade, como a LGPD no Brasil ou o GDPR na União Europeia.

3.3. Os Direitos da Personalidade da Segurança da Informação

Os direitos da personalidade são um conjunto de direitos reconhecidos pela lei que visam proteger aspectos essenciais da identidade e dignidade das pessoas. Eles são inerentes à própria natureza humana e não podem ser alienados, renunciados ou transferidos para outras pessoas. Não englobando o mundo cibernético os direitos da personalidade seriam direitos à vida, integridade física e moral, privacidade, imagem, nome, à honra, ao respeito, liberdade de expressão e de pensamento entre outros e estão esculpidos na Constituição Federal, art. 5º, inciso X, conjuntamente com artigo 11 do Código Civil Brasileiro.

Traçando um parâmetro para a aplicabilidade dentro do mundo da Segurança da Informação pode-se entender que os direitos da personalidade são de suma importância porque as informações pessoais e privadas de indivíduos precisam ser protegidas contra acesso não autorizado e uso indevido. Os direitos da personalidade podem ser agredidos quando as informações consideradas ativos da corporação sofrem algum dano referente a sua integridade, privacidade, confidencialidade e consentimento além de acesso e exclusão de suas próprias informações pessoais e não discriminação baseado em informações pessoais de cor, raça, religião, orientação sexual dentre outras.

Deve-se entender que, em um estado democrático de direito, a quantidade de deveres razoáveis, sejam eles maiores ou menores, também podem serem utilizadas como base para a proteção efetiva da individualidade da pessoa, especialmente no contexto da proteção de dados. Nessa perspectiva, a existência de uma entidade estatal é valorizada, pois é responsável pela implementação de mecanismos de coerção social que reforçam esses deveres. Em um ambiente democrático, é praticamente impossível agir de forma contrária, pois a imposição de deveres sem uma contrapartida de proteção adequada sugere que não está fundamentada na preservação qualitativa do interesse coletivo. Todos esses princípios podem e devem ser aplicados à proteção de dados pessoais conforme estabelecido LGPD, inclusive quando se trata de entidades públicas (Federação,

Estados, Municípios, Órgãos Públicos, etc) que processam informações de grande relevância.

Do ponto de vista doutrinário e jurídico, as concepções sobre a natureza humana e a personalidade estão interligadas. Essa conexão fica ainda mais evidente ao se tratar de questões de natureza privada, especificamente dentro do âmbito do Direito Civil. Isso ocorre porque o instituto da personalidade jurídica é fundamental para a configuração da pessoa como sujeito de direitos e deveres. No entanto, é importante ressaltar que a mera adoção de uma personalidade não garante o exercício prévio de um direito específico (LIMA, 2016, p. 507).

No contexto do direito da personalidade, existe uma interligação entre a possibilidade de usufruir de direitos e a existência de obrigações sociais simultâneas. Esses princípios são aplicáveis com grande rigor quando se trata da proteção de dados pessoais, conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD), especialmente em instituições da gestão pública.

A personalidade jurídica é vista como um atributo exclusivo que confere uma divisão clara entre direitos e deveres, os quais são definidos pelo ordenamento jurídico. No âmbito jurídico, é notável que a personalidade pode ser utilizada sem requisitos adicionais além da sua própria existência, seja para pessoas físicas ou jurídicas. Essas entidades têm o direito de desfrutar de uma variedade de direitos, mas também têm o dever de cumprir obrigações que são impostas visando o bem coletivo (Silva, 2014, p. 202).

Atualmente, a LGPD está dedicada à proteção das informações e dados armazenados em bancos de dados, de forma análoga aos direitos da personalidade. Além disso, em prol da proteção do ser humano, essa salvaguarda se estende aos bancos de dados sob a gestão das entidades organizacionais da Administração Pública, como destacado por Zubko (2015, p. 7).

3.4. A Proteção da Criança e do Adolescente em Face da LGPD

A nova legislação também abrange as crianças e adolescentes, que continuam sendo usuários da internet, estabelecendo regras significativas para esse público considerado mais vulnerável devido à sua idade.

É fundamental ressaltar que, no que diz respeito a esse grupo, a nova legislação não distingue entre dados pessoais e dados sensíveis; ambos são tratados como um único conjunto, conforme observado por Sena (2019).

O artigo 14 da LGPD determina que o tratamento de dados pessoais de crianças e adolescentes deve ser realizado em seu melhor interesse, de acordo com este artigo e a legislação relevante (BRASIL, 2020). Isso implica que o tratamento de dados pessoais para crianças deve ocorrer mediante um consentimento claramente destacado para esse público, o qual deve ser concedido pelos pais ou pelos responsáveis legais do usuário menor. Essa exigência tem como objetivo garantir o respeito à integridade da criança, proibindo qualquer tentativa, mesmo com o uso das mais avançadas tecnologias, de obter consentimento diretamente do usuário menor (SENA, 2019). Além disso, todas as informações coletadas pelos controladores devem ser disponibilizadas de forma pública, esclarecendo quais dados foram coletados, como serão utilizados e quais procedimentos são adotados em relação a esses dados, conforme estabelecido no artigo 14, § 2° (BRASIL, 2020).

Há também isenções e ressalvas em relação ao consentimento, conforme previsto no § 3° do artigo 14, que permite a coleta de dados a serem utilizados apenas uma vez. Conforme o estabelecido:

> § 3° Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo (BRASIL, 2020).

Conscientes da crescente presença da Internet na vida de crianças e adolescentes, os redatores da Lei Geral de Proteção de Dados implementaram disposições legais com o objetivo de estabelecer controles nas atividades em que esses grupos etários participam e nas quais ocorre a coleta de suas informações, respeitando as exceções previstas nos parágrafos 4° e 5° do artigo 14 (BRASIL, 2020).

Embora o princípio da transparência seja inerente a toda a legislação como um requisito fundamental, torna-se necessário adaptar o dispositivo legal para incluir a capacidade de compreensão por parte das crianças e adolescentes. Segundo Valente (2018), os legisladores demonstraram preocupação ao estabelecer o princípio da transparência no dispositivo legal, seguindo o modelo da União Europeia, exigindo que todas as informações fornecidas sejam apresentadas em

linguagem clara, acessível e simplificada no que diz respeito ao tratamento de dados. Como afirma o autor:

> A Lei Geral de Proteção de Dados exige que empresas envolvidas em algum tipo de tratamento de dados de crianças devem dar transparência a eles. Segundo o texto, “os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos” dos usuários.
> Além disso, a norma prevê que as informações sobre tratamento de dados sejam disponibilizadas “de maneira simples”, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (VALENTE, 2018, p. 1).

Por último, Sena (2019, página 22), argumenta que:

> Considerando que as crianças são sujeitos em desenvolvimento, a instituição de responsabilidade compartilhada do Poder Público e os cuidados dos pais em relação à utilização da tecnologia pelos seus filhos, é razoável notar que com a dispensa do consentimento do responsável do titular, em determinadas situações, a proteção de dados pessoais de crianças poderá sofrer diversos desafios, por se tratar de um ordenamento ambíguo e amplo.

4. OS DADOS PESSOAIS E SUA PROTEÇÃO

Em 1970, a Alemanha foi pioneira ao promulgar a primeira lei global sobre proteção de dados pessoais. Schertel (2011, p. 37) enfatizou a importância de elevar o nível de proteção dos dados pessoais, defendendo que a salvaguarda desses dados é uma projeção da individualidade da pessoa e, portanto, deve ser protegida pela jurisdição de forma definitiva.

No Brasil, durante a década de 1990, surgiram os primeiros instrumentos jurídicos relacionados à proteção do uso de dados, o que trouxe novas concepções sobre a importância desses dados. Um exemplo é o Código de Defesa do Consumidor, estabelecido pela Lei nº 8.078/90, que regulamenta o uso de bancos de dados de consumidores. Esse código estabelece o direito do consumidor de acessar "informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele". Embora não tenha previsto expressamente o consentimento para a coleta desses dados, o código permite a correção de informações obscuras e reivindica que o consumidor seja informado sobre a abertura do registro.

Em 1996, a Lei nº 9.296, conhecida como Lei de Interceptação Telefônica e Telemática, restringiu o uso desses recursos como meio de investigação, estabelecendo que seu uso deve ocorrer apenas mediante autorização judicial. Essa lei reconhece o direito à privacidade.

No ano de 1997, foi promulgada a Lei nº 9.507, conhecida como Lei do Habeas Data, que regulamenta o direito constitucional e o procedimento de acesso e correção de informações pessoais. Essa lei estabelece diretrizes para garantir o exercício desse direito fundamental.

No ano de 2002, o Código Civil Brasileiro incorporou, em seu artigo 21, disposições relacionadas aos direitos da personalidade, abrangendo a vida privada e fornecendo o interruptor para controlar a violação desse direito. Essa inclusão, embora gradual, destaca a privacidade como um direito subjetivo e não limitada ao direito à propriedade.

Chegando ao ano de 2011, no Brasil, foi promulgada a Lei n° 12.527/11, popularmente conhecida como Lei de Acesso à Informação. Essa legislação estabeleceu, em seu Artigo 4°, inciso IV, e Artigo 6°, inciso III, o direito de acesso à informação pessoal, que assim positivava em suas entrelinhas (BRASIL, 2011):

> Art. 4º Para os efeitos desta Lei considera-se:
> IV - Informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;
> Art. 6º Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:
> III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

No primeiro quarto de 2013, ocorreu uma regulamentação de determinados aspectos da legislação de defesa do consumidor, aguardando que os fornecedores implementem medidas de segurança eficazes para o processamento e tratamento dos dados dos consumidores. Diante da crescente velocidade de renovação das leis de proteção de dados em diversos países ao redor do mundo, surgiu a necessidade de proteger as informações pessoais, como afirmado por Fernandes (2019, p. 10).

De acordo com Bioni (2019, pp. 171-173), é possível dividir a evolução das leis de proteção de dados pessoais em quatro gerações distintas. A primeira geração consistia em normas que refletiam o estágio da tecnologia e a visão dos juristas daquela época.

A segunda geração representa uma mudança central no sistema regulatório, indo além dos dados pessoais de entidades governamentais e voltando-se também para os dados pessoais de indivíduos na esfera privada. Nessa geração, a responsabilidade pela segurança desses dados é imposta aos detentores dos mesmos.

A terceira geração, que surgiu na década de 1980, buscou aprimorar a proteção dos dados pessoais, mantendo o foco no indivíduo, mas indo além da mera liberdade de consentir ou não com o fornecimento de seus dados pessoais. Essa geração também se preocupou em garantir a passagem dessa liberdade.

Uma quarta geração de leis de proteção de dados, presente em diversos países atualmente, emergiu com o objetivo de tratar a limitação da abordagem individual adotada nas gerações anteriores. Essa nova geração busca superar as informações protegidas, buscando um equilíbrio entre a proteção dos direitos individuais e as necessidades legítimas das organizações e da sociedade como um todo.

5. O DANO QUE EXTRAPOLA O AMBITO DA LGPD SE PERFAZENDO EM RESPONSABILIDADE CIVIL

Diante da hermenêutica trazida pelas entrelinhas de estudo e tendo como base as várias vertentes da LGPD foi realizada neste trabalho uma análise desta lei explorando as responsabilidades do detentor dos dados, sejam eles pessoas físicas ou jurídicas no âmbito judicial civil.

Neste contexto de estudo e diante do explorado foi possível concluir que a responsabilidade já determinada tanto pela LGPD quanto pelo nosso Código Civil Brasileiro se divide em duas correntes distintas, objetiva e subjetiva, prevalecendo esta última, como explicado de forma pormenorizada nos subtítulos a seguir.

5.1. Noções Precedentes da Responsabilidade Civil

Tal como ocorre quando da adoção de novas tecnologias devendo adequá-las o mesmo ocorre com responsabilidade civil que deve procurar seu melhor cenário, ajustando-se às necessidades identificadas e surgidas com o progresso, com o aparecimento de novas atividades e da multiplicação das adversidades causadas pela vida moderna.

A noção da responsabilização ao reparar danos injustamente causados, por ser própria da natureza humana, existe desde os primórdios da civilização. Todavia, a maneira de reparação deste dano foi transformando-se ao longo do tempo, evoluindo conforme a dinâmica da sociedade.

Em rápidas pinceladas, o instituto da responsabilidade civil tem a sua previsão desde as mais primitivas expressões do Direito, tendo a sua trajetória iniciada juntamente com a responsabilidade penal, com base na regra de Talião – olho por olho, dente por dente – caracterizada por uma vingança privada e, finalmente, chegando aos dias de hoje, em que há um afastamento da sua função sancionatória e um enfoque na função reparatória, deslocando-se assim a ênfase outrora atribuída ao ofensor para o ofendido.

Sobre mais, esclarecem os autores Gagliano e Pamplona Filho (2012) em sua obra que o conceito jurídico de responsabilidade pressupõe uma atividade danosa de alguém que, atuando, a priori ilicitamente, viola uma norma jurídica preexistente

(legal ou contratual), subordinando-se, dessa forma, às consequências do seu ato (obrigação de reparar).

Na mesma esteira, ressaltando que sem a violação de um dever jurídico previamente existente, não há que se falar em responsabilidade civil, expõe Cavalieri Filho (2012):

> Em seu sentido etimológico, responsabilidade exprime a ideia de obrigação, encargo, contraprestação. Em sentido jurídico, o vocábulo não foge dessa ideia. A essência da responsabilidade está ligada à noção de desvio de conduta, ou seja, foi ela engendrada para alcançar as condutas praticadas de forma contraria ao direito e danosas a outrem. Designa o dever que alguém tem de reparar o prejuízo decorrente da violação de um outro dever jurídico. Em apertada síntese, responsabilidade civil é um dever jurídico sucessivo que surge para recompor o dano decorrente da violação de um dever jurídico originário.

O sistema jurídico brasileiro adotou, no Código Civil de 2002, o modelo dualista de responsabilidade civil, fixando tanto uma norma geral de responsabilidade civil subjetiva, quanto uma cláusula geral de responsabilidade civil objetiva. Com efeito, essas duas facetas da responsabilidade divergem no tocante aos fundamentos que justificam a incidência do dever de indenizar.

Em que pese haja essa distinção, os requisitos para que se reconheça a aplicabilidade do instituto da responsabilidade civil são os mesmos em ambas as classificações, a conduta, o dano e o nexo de causalidade entre os dois primeiros. Como se pode notar, as soluções serão idênticas, independentemente da modalidade empregada, pois uniformes são os seus efeitos, a reparação patrimonial do dano sofrido, cuja indenização é medida de acordo com a sua extensão.

Aspecto essencial para que se configure o dever de indenizar, o conceito jurídico de dano sofreu alterações no decorrer do tempo. Antes, baseado na Teoria da Diferença, em que, segundo Bodin (2019):

> Tradicionalmente, define-se dano patrimonial como a diferença entre o que se tem e o que se teria, não fosse o evento danoso. A assim chamada ‘Teoria da Diferença’, devida à reelaboração de Friedrich Mommsen, converteu o dano numa dimensão matemática e, portanto, objetiva e facilmente calculável.

A definição cunhada pela Teoria da Diferença, em que se identificava o dano como uma diferença entre o patrimônio antes do evento danoso e após a sua ocorrência, foi abandonada em favor de uma noção normativa do dano.

Nesse sentido, o dano passa a ser compreendido como a lesão a qualquer interesse jurídico merecedor de tutela.

Em suma, com essa releitura do pressuposto central da responsabilidade civil, a tendência é a de que a indenização pelo dano gerado passa a ser medida tão somente pelos impactos da lesão na vítima, independentemente de qualquer consideração acerca do ofensor ou de seu patrimônio.

De igual importância, outro pressuposto para a imputação da responsabilidade civil é a conduta do ofensor, devendo-se analisar se fundamentada na culpa ou no risco.

A regra geral de responsabilização consagrada na lei civil brasileira se dá por meio da aplicação da teoria subjetiva, que, conforme a classificação sugere, consiste no exame do comportamento do sujeito, observando se o dano causado ocorreu em decorrência de ato doloso ou culposo, ao praticar uma conduta ilícita. É, portanto, uma responsabilidade pautada na verificação de culpa em sentido amplo de culpa ou dolo, com base no artigo 927, *caput*, segundo os ditames dos artigos 186 e 187, ambos do Código Civil Brasileiro (2002):

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. [...]
> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

Pereira (1999) preceitua que a culpa é:

> [...] como um erro de conduta, cometido pelo agente que, procedendo contra direito, causa danos a outrem, sem a intenção de prejudicar, e sem a consciência de que seu comportamento poderia causá-lo.

Cabe ressaltar que existe um limite à discricionariedade do juiz consistente na verificação das normas jurídicas como padrões a serem seguidos pelos tribunais, obedecendo assim ao princípio da legalidade.

Apesar do fenômeno de objetivação da responsabilidade civil diante da insuficiência da teoria subjetiva com a explosão tecnológica, de modo geral, a interpretação de que a responsabilidade objetiva se dará apenas em casos excepcionais foi mantida pela jurisprudência brasileira.

Em derradeiro, o nexo de causalidade é o elemento de ligação entre os dois elementos qualificados anteriormente, a conduta e o dano causado.

5.2. Responsabilidade Objetiva

Referente a responsabilidade civil objetiva fundamentada no risco da atividade desenvolvida, ou seja, que prescinde da discussão sobre a culpa do agente bastando que se comprove o dano e o nexo causal, argumentam que este modelo foi adotado pelo legislador com base em diversos aspectos.

Para os defensores da responsabilidade objetiva, os princípios já dão o tom do que se espera no tratamento de dados em eventuais danos ocasionados. Deste modo, ao se afastar os fundamentos principiológicos da Lei Geral de Proteção de Dados, que são justamente as bases por meio das quais é possível se identificar o espírito da lei, a intenção do legislador ao enumerar uma série de princípios que regulam e servem como um cobertor da lei foi proporcionar um arcabouço de direitos, sanções, regulamentações específicas com o objetivo de alcançar a máxima proteção do titular de dados.

Nesse sentido, Mulholland (2021) destaca três princípios da LGPD, quais sejam, segurança, prevenção e responsabilização e prestação de contas, que trazem uma fundamentação que permite ao intérprete da LGPD considerar que se está diante de uma lei que protege o titular de dados o concedendo um direito a ser indenizado pelos danos sofridos com base na chamada teoria do risco.

Segundo ela, a transparência a ser adotada pelo agente acerca dos procedimentos que são tomados para a segurança e prevenção no tratamento de dados deve ser considerada como um dever ativo, gerando a obrigação ao agente de tratamento de prestar contas, onde serão evidenciadas as medidas que estão sendo tomadas para uma atuação em conformidade com as boas práticas impostas pela lei.

Outro fator que leva à defesa da adoção da responsabilidade objetiva pela Lei Geral de Proteção de Dados é a sua similaridade com o Código de Defesa do Consumidor (Lei nº 8.078/ 1990), no tocante aos dispositivos de responsabilidade civil. Neste diploma legal, adota-se a responsabilidade objetiva do fornecedor vinculada à ideia de vulnerabilidade do consumidor e o consequente desequilíbrio na relação processual.

Neste raciocínio, demonstram os especialistas (MENDES, 2021, p. 16) adeptos da teoria objetiva que o titular de dados é considerado presumidamente vulnerável, dada a clara dificuldade de controlar o fluxo dos seus dados pessoais,

bem como de adotar medidas de autoproteção contra os riscos do tratamento dessas informações. Destaca Mendes (2021):

> A vulnerabilidade do consumidor nesse processo de coleta e tratamento de dados pessoais é tão patente que se cunhou a expressão “consumidor de vidro” para denotar a sua extrema fragilidade e exposição no mercado de consumo, diante de inúmeras empresas que tomam decisões e influenciam as suas chances de vida, a partir das informações pessoais armazenadas em bancos de dados.

Diante do reconhecimento da vulnerabilidade e hipossuficiência do titular de dados, nota-se que há um desequilíbrio anterior calcado na produção de um risco pelo ofensor que não é recíproco, ensejando assim o emprego da responsabilidade objetiva como ferramenta para a busca da igualdade entre as partes.

De fato, ao analisar a Lei Geral de Proteção de Dados, percebe-se a semelhança dos dispositivos com o Código de Defesa do Consumidor a Tabela 1 a seguir destaca em negritos pontos convergentes entre os dois ordenamentos.

Quadro 1: Breve comparação entre LGPD e CDC

Tabela Comparativa LGPD x CDC	
Art. 43. Os agentes de tratamento **só não serão responsabilizados quando provarem:** I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.	Art. 12. [...] §3º O fabricante, o construtor, o produtor ou importador **só não será responsabilizado quando provar:** I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste; III - a culpa exclusiva do consumidor ou de terceiro.

Fonte: Próprio autor

Em que pese os argumentos expostos ensejam uma tentação em se adotar a teoria objetiva, não se pode olvidar que o objetivo da nova Lei Geral de Proteção de

Dados é não somente proteger o titular dos dados, como também viabilizar o desenvolvimento das atividades na rede.

Não pode, evidentemente, a responsabilização ser um meio de impor um novo desequilíbrio na relação entre as partes, a tal ponto de atribuir ao agente de tratamento de dados deveres impossíveis de serem desempenhados, desmotivando assim a adoção de comportamento adequado.

5.3. Responsabilidade Subjetiva

Apesar da indefinição acerca da modalidade de responsabilidade civil na Lei Geral de Proteção de Dados, revela-se de suma importância atentar para as pistas deixadas pelo legislador que apontam para o regime subjetivo e da culpa como fundamento, pelo menos como regra geral, conforme os argumentos dos defensores desta corrente a serem expostos.

Com base nos princípios da responsabilização e da prestação de contas expressos no artigo 6º da LGPD, os agentes deverão comprovar a adoção de medidas eficazes e capazes de demonstrar a observância, o cumprimento e a eficácia das normas de proteção de dados pessoais. Diante disso, indagam Guedes e Meireles (2019, p. 219):

> Do ponto de vista do controlador, do que adianta ‘prestar contas’, se, ao final, se houver incidente, por mais diligente que tenha sido, ele será responsabilizado da mesma forma e independentemente de culpa?

Pode ser entendido claramente que a intenção do legislador, ao pautar a Lei Geral de Proteção de Dados na criação de deveres aos agentes de tratamento de dados estabelecendo um standard de conduta, é a de adoção da responsabilidade subjetiva.

Seria incompatível o legislador impor uma série de deveres de cuidado para, ao final, responsabilizar o controlador e o operador independentemente do cumprimento do padrão de comportamento exigível. Esta seria a lógica da responsabilidade objetiva, cuja concretização ocorre com a prática de atos lícitos que causam danos, independentemente da violação de qualquer dever jurídico por parte do agente.

As circunstâncias, portanto, ensejam a responsabilização subjetiva, fazendo-se necessária uma análise casuística investigando se o agente de tratamento agiu

conforme o padrão de comportamento esperado pela lei, adotando as medidas de segurança e medidas preventivas para evitar ao máximo um vazamento de dados pessoais.

A avaliação da responsabilidade no caso concreto é importante também para identificar o risco da atividade de tratamento de dados, visto que a LGPD não prevê um nivelamento de toda e qualquer atividade como sendo de risco acentuado.

Com o estudo do caso concreto, é possível a realização de um juízo de valor sobre a forma pelo qual deveria ter sido realizado o tratamento de dados diante da identificação dos riscos que da atividade razoavelmente eram esperados.

Cabe aos agentes de tratamento de dados ajustar as suas medidas de segurança para corresponder à probabilidade e à gravidade das violações possivelmente resultantes da atividade.

Essencial se mostra a avaliação do caso concreto para que se garanta a segurança jurídica, minimizando a produção de danos causados aos titulares de dados e, paralelamente, proporcionando um ambiente estimulante para a atividade econômica.

Contra o argumento dos defensores da responsabilidade objetiva acerca da similaridade da LGPD com o CDC, alegam os defensores da responsabilidade subjetiva que há indícios de que o modelo objetivo é apenas uma tentação.

A Tabela 2 a seguir demonstra de forma clara nos trechos em destaque que o legislador foi específico em determinar que no tratamento dos dados o detentor controlador ou o operador, só respondem pelo dano quando não foi aplicado tudo quanto necessário para a proteção no tratamento dos dados se perfazendo assim em responsabilidade subjetiva, diferentemente dos artigos 12 e 14 do CDC que afirmam de forma categórica que a parte autossuficiente da avença respondem independente de culpa, ou seja, sua responsabilidade nessa relação é cem por cento objetivas, não havendo margem para discussão.

Quadro 2: Resumo comparativo entre LGPD e CDC

Tabela Comparativa LGPD x CDC		
Art. 42. LGPD. O controlador ou o operador que, em razão	Art. 12. CDC. O fabricante, o produtor, o construtor, nacional ou	Art. 14. CDC. O fornecedor de serviços **responde,**

do exercício de atividade de tratamento de dados pessoais, **causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais**, é obrigado a repará-lo. [...]	estrangeiro, e o importador **respondem, independentemente da existência de culpa**, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. [...]	**independentemente da existência de culpa**, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos. [...]

Fonte: Próprio autor

Além do mais, no Código Civil, em todos os dispositivos em que se encontra prevista a responsabilidade objetiva, há clareza na sua escolha, seja pelo uso da expressão “independentemente de culpa”, como ocorre no art. 927, parágrafo único, que prevê a cláusula geral de responsabilidade objetiva, seja por outra expressão como, por exemplo, “ainda que não haja culpa de sua parte” ou “salvo motivo de força maior”.

Apesar da similaridade do artigo 43 da LGPD com o artigo 12, §3º, do CDC, percebe-se uma diferença fundamental: o inciso II do artigo 43 encontra-se intrinsecamente vinculado ao elemento culpa, diferentemente do que ocorre no CDC, cujos incisos são todos conectados ao elemento nexo de causalidade.

A reprovabilidade da conduta do agente de tratamento se vincula à violação do dever de observar os preceitos da LGPD.

Seguindo este raciocínio, o artigo 44, ao tratar dos incidentes de segurança, também se vincula ao elemento culpa em seu parágrafo único, ao prever que o

controlador ou o operador que deixar de adotar as medidas de segurança previstas na LGPD responderá pelos danos decorrentes da violação da segurança dos dados. Entende-se, contrariamente, que se adotar as medidas de segurança impostas pelo legislador e, ainda assim, ocorra um dano, ele não responde.

Nesse contexto, há de se ter prudência dada a sensibilidade da objetivação da responsabilidade civil, pois, por mais digno que seja o dever de reparar, protegendo assim os titulares de dados vulneráveis em uma sociedade cada vez mais sujeita a riscos, não se pode fazer do agente que adotou os esforços necessários para a proteção dos dados um ofensor.

Logo, considerando o foco da LGPD na conduta dos agentes de tratamento, a conclusão por um modelo de responsabilização objetiva é contraditória com o próprio espírito da lei, que busca incentivar os agentes de tratamento a adotar boas práticas.

6. CONCLUSÃO

Considerando o exposto, torna-se evidente que, apesar da existência de leis relacionadas à privacidade, esse direito fundamental continua sendo frequentemente violado. Após a ocorrência de escândalos de alcance global relacionados a vazamentos e manipulação de dados, surgiu a necessidade de criar o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Este regulamento serviu de influência para muitos outros países elaborarem suas próprias leis de proteção de dados, a fim de evitar possíveis prejuízos econômicos, diplomáticos e comerciais nas relações com a União Europeia.

No contexto do Brasil, apesar da existência de leis anteriores que tratavam de temas relacionados à privacidade e proteção de dados, como a Lei de Acesso à Informação, o Marco Civil da Internet, a Lei Carolina Dieckmann, entre outras, essas legislações ainda não conseguiam atender completamente às necessidades da sociedade. Portanto, a criação da Lei Geral de Proteção de Dados se mostrou uma necessidade real, trazendo impactos positivos para a sociedade.

A LGPD introduziu uma série de mudanças tanto internas quanto externas no cenário do tratamento de dados no Brasil. Hoje, está imerso em uma sociedade na qual a troca de informações e dados é constante, e essa lei foi estabelecida com o propósito de regulamentar e organizar o processamento de dados pessoais. Ela abrange todas as etapas, desde a coleta até o descarte dos dados.

Desta forma, ficou compreendido que a nova lei se baseia em princípios que têm o potencial de motivar tanto o setor público quanto o privado a contribuir para tornar a Internet mais democrática e segura. É evidente que imprecisões, erros ou violações podem acontecer, no entanto, antecipa-se que, mesmo diante dessas situações, haverá um nível mais substancial de proteção legal. Portanto, ao trilhar o caminho em direção à previsibilidade, a segurança jurídica emerge como um meio de preservar os direitos.

Antes da LGPD, ficou evidente, por meio de escândalos e violações de dados pessoais, que o tratamento inadequado e insustentável dessas informações estava ocorrendo em larga escala. Com a criação, implantação e aplicação da LGPD, tornou-se claro que o verdadeiro dono dos dados é o titular, e que para o armazenamento, coleta e compartilhamento desses dados, é essencial obter o consentimento expresso e a ciência do titular. Isso transformou o ambiente de

tratamento de dados em um espaço mais seguro, com regras claras sobre o uso e a coleta, dando ao titular o controle sobre a distribuição de suas informações.

No que diz respeito aos dados pessoais de indivíduos, os titulares agora desfrutam de plenos direitos, incluindo o acesso, exclusão ou anonimização de seus dados em instituições ou bases de dados, a qualquer momento que desejarem.

Os agentes envolvidos no tratamento de dados desempenham funções específicas, sendo eles o controlador, operador e encarregado de dados. O operador atua como intermediário entre a empresa, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares de dados. Em caso de fiscalizações ou dúvidas relacionadas ao tratamento de dados, esse profissional é o responsável pela empresa.

Muitas empresas costumavam e ainda usam dados pessoais de seus clientes para trocar informações, visando influenciar as opiniões e decisões desses usuários, direcionar anúncios de marketing para grupos específicos e consultar preferências políticas, ideológicas e religiosas, buscando obter alguma vantagem a partir dessas informações, muitas vezes sem o consentimento dos titulares.

É inegável o desafio constante que as empresas enfrentam ao buscar alinhar-se com a LGPD, elaborando e aprimorando suas políticas de proteção e tratamento de dados para estar em conformidade com as disposições legais estabelecidas. Além disso, é crucial manter em dia os termos legais relacionados às informações de seus clientes-usuários, estabelecendo padrões para o uso e o período de retenção de dados pessoais. Nesse contexto, as empresas devem agir com celeridade na adaptação, uma vez que a lei está em vigor integralmente, considerando que estão lidando com direitos fundamentais.

No que tange ao programa de *Compliance*, este demonstrou ser um meio eficaz de assegurar a conformidade com os requisitos da Lei, proporcionando abordagens preventivas para mitigar riscos, promover uma cultura ética mediante políticas e procedimentos que orientam as empresas na sua adaptação à Lei. Isso resulta na conquista da confiança dos clientes, na aderência à legislação e na percepção positiva por parte do mercado em relação a outras instituições.

Quanto às transformações específicas implementadas no ordenamento jurídico pátrio a respeito dos fundamentos para imputação da obrigação indenizatória, foi possível se concluir pela existência de uma paulatina expansão das hipóteses de incidência atreladas ao risco, em detrimento da culpa, a priori

implementadas de forma tímida, por meio de previsões específicas em legislações especiais com escopo de aplicabilidade mais restrito, porém depois consideravelmente alargadas, desde o advento do CDC e, posteriormente, também graças à instituição da cláusula geral do art. 927, parágrafo único, do Código Civil, a ponto de a responsabilidade objetiva, não obstante seja a exceção em termos puramente jurídicos, ter possivelmente se tornado, na prática, mais aplicada do que a, em tese, regra geral da responsabilidade subjetiva.

Ainda neste primeiro momento, de contextualização do tema, viu-se que o incipiente histórico legislativo e jurisprudencial do desenvolvimento do direito à proteção de dados pessoais no país está bastante atrelado ao direito do consumidor, apesar de se tratarem de áreas que não se confundem, muito embora existam diversos espaços de confluência entre elas. As influências do CDC sobre a LGPD, aliás, ficaram nítidas na redação dos próprios dispositivos presentes na seção sobre responsabilidade civil, mormente nos artigos 43 e 44, a ponto de ocasionarem em consequências palpáveis sobre o problema objeto de estudo.

Após a implementação da LGPD, houve mudanças significativas no cenário de proteção de dados pessoais no Brasil. No entanto, sua adesão ainda não ocorreu da maneira necessária, muitas vezes devido à falta de informações, desinteresse ou desconhecimento sobre como se ajustar. É imperativo que a cultura de *compliance* seja disseminada tanto em organizações públicas quanto no mundo empresarial, para que compreendam que a conformidade com a Lei não apenas é vantajosa, mas também resulta em benefícios positivos em diversas áreas. A criação da LGPD marcou o início da implementação e promoção dessa cultura e sua disseminação desse ser contínua em prol da proteção de todos envolvidos na manipulação dos dados pessoais.

REFERÊNCIAS

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Ed. Forense Ltda, 2019.

BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito “proativo”. **Civilistica.com**. Rio de Janeiro: a. 8, n. 3, 2019. p. 1-6.

BRASIL. Casa Civil, **Lei nº 12.527, dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências**. Brasília: Presidência da República, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 abr. 2023.

BRASIL. Casa Civil, **Lei nº 12.737, dá outras providências**. Brasília: Presidência da República, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 out. 2023.

BRASIL. Casa Civil, **Lei 12.965, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília: Presidência da República, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 out. 2023.

BRASIL. Casa Civil, **Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília: Presidência da República, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 out. 2023.

BRASIL. Casa Civil, **Lei nº 10.406, Institui o Código Civil**. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 26/10/2023.

BRASIL. Casa Civil**,** Altera a Lei nº 13.709, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. **Diário Oficial da União: seção 1**, Brasília, Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=14/06/2022&jornal=515&pagina=2. Acesso em: 17 out. 2023.

BRASIL. Casa Civil, Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. **Perguntas frequentes – ANPD.** Portal Gov.br, [Brasília], 10 fev. 2023. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd. Acesso em: 17 out. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**, DF: Senado Federal de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 mar. 2023.

BRASIL. **Código civil de 2002**. DF: Senado Federal de 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 07 mar. 2023.

BRASIL. **Código de processo civil de 2015**. DF: Senado Federal de 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 07 mar. 2023.

BRASIL. **Lei geral de proteção de dados de 2018**. DF: Senado Federal de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 mar. 2023.

CANCELIER, Mikhail Vieira de Lorenzi. **O direito à privacidade hoje**: perspectiva histórica e o cenário brasileiro. Disponível em: https://www. https://www.scielo.br/scielo.php?script=sci_arttext&pid=S217770552017000200213&lng=en&nrm=iso. Acesso em: 07 mar. 2023

CARVALHO, A. C.; **Manual de compliance**. 2. ed. Rio de Janeiro: Forense, 2019.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 10. ed. São Paulo: Atlas, 2012.

COTS, Marcio. Lei Geral de Proteção de dados pessoais comentada. **Revista dos Tribunais**. São Paulo: Editora Revista dos Tribunais. 2018

COUNCIL OF EUROPE. **Convention for the protection of individuals with regard to automatic processing of personal data.** Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 Acesso em: 07 mar. 2023.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). Compliance: perspectivas e desafios dos programas de conformidade. Belo Horizonte: **Fórum**, 2018.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 219-241.

MACIEL, Rafael Fernandes. **Manual prático sobre a lei geral de proteção de dados pessoais (Lei nº 13.709/18)**. Goiânia: RM Digital Education, 2019.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor**.https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1228/1155. Acesso em: 07 mar. 2023

MULHOLLAND, Caitlin. **A LGPD e o fundamento da responsabilidade civil dos agentes de tratamento de dados pessoais: culpa ou risco?** 2020. Disponível em: https://www.migalhas.com.br/coluna/migalhas-deresponsabilidade-civil/329909/a-lgpd-e-o-fundamento-da-responsabilidade-civil-dos-agentes-de-tratamento-dedados-pessoais--culpa-ou-risco. Acesso em 26/10/2023.

NAÇÕES UNIDAS BRASIL. **Artigo 12**: direito à privacidade. 1948. Disponível em: https://nacoesunidas.org/artigo-12-direito-a-privacidade/. Acesso em: 07 mar. 2023.

NAÇÕES UNIDAS. **Declaração universal dos direitos humanos**. 1948. Disponível em: https://nacoesunidas.org/wp-content/uploads/2018/10/DUDH.pdf. Acesso em: 07 mar. 2023.

NETTO, Thais. **Aplicabilidade e inaplicabilidade da LGDP**. Disponível em: https://direitoreal.com.br/artigos/aplicabilidade-e-inaplicabilidade-da-lgpd. Acesso em: 07 mar. 2023.

NUNES, Gabriela Victória Miranda**. Governança e boas práticas na lei geral de proteção de dados pessoais**: dos programas de compliance. 2019. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2019. Disponível em: https://bdm.unb.br/handle/10483/25080. Acesso em: 18 out.2023.

PALHARES, Felipe; PRADO, Luís Fernando; VIDIGAL, Paulo**. Compliance digital e LGPD**. São Paulo: Thomson Reuters Brasil, 2021.

PEREIRA, Caio Mário da Silva. 9ª ed. **Responsabilidade civil**. Rio de Janeiro: Forense, 1999.

PINHEIRO, Patrícia Peck**. Proteção de dados pessoais**: comentários à Lei N. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

POHLMANN, Sérgio Antônio. **LGPD ninja:** entendendo e implementando a lei geral de proteção de dados nas empresas. São Paulo: Editora Fross, 2019.

SERPRO. **Serpro e LGPD**: segurança e inovação. 2020. Disponível em: https://www.serpro.gov.br/lgpd/. Acesso em: 07 mar. 2023.

UNIÃO EUROPEIA. **Directiva 95/46/CE**. Luxemburgo: Parlamento Europeu, 1995.