CENTRO UNIVERSITÁRIO DE LAVRAS
CURSO DE GRADUAÇÃO EM DIREITO

ANDRÉ LUIZ TORRES RIBEIRO

RESPONSABILIDADE CIVIL NO CÓDIGO DE DEFESA DO CONSUMIDOR E PROTEÇÃO DE DADOS PESSOAIS: O DIREITO À PRIVACIDADE NA LEI N. 13.709/2018

LAVRAS – MG

2023

ANDRÉ LUIZ TORRES RIBEIRO

RESPONSABILIDADE CIVIL NO CÓDIGO DE DEFESA DO CONSUMIDOR E PROTEÇÃO DE DADOS PESSOAIS: O DIREITO À PRIVACIDADE NA LEI N. 13.709/2018

Monografia apresentada ao Centro Universitário de Lavras como parte das exigências do curso de graduação em Direito.
Orientadora: Profa. Ma. Adrielly Francine Rocha Tiradentes.

LAVRAS – MG

2023

Ficha Catalográfica preparada pelo Setor de Processamento Técnico
da Biblioteca Central do UNILAVRAS

R484r

Ribeiro, André Luiz Torres.
Responsabilidade civil no código de defesa do consumidor e proteção de dados pessoais: o direito à privacidade na lei n. 13..709/2018 / André Luiz Torres Ribeiro. – Lavras: Unilavras, 2023.

51f.

Monografia (Graduação em Direito) – Unilavras, Lavras, 2023.

Orientador: Prof.ª Adrielly Francine Rocha Tiradentes.

1. Lei geral de proteção de dados. 2. Direito do consumidor. 3. Tratamentos de dados. 4. Responsabilidade civil. I. Tiradentes, Adrielly Francine Rocha (Orient.). II. Título.

ANDRÉ LUIZ TORRES RIBEIRO

RESPONSABILIDADE CIVIL NO CÓDIGO DE DEFESA DO CONSUMIDOR E PROTEÇÃO DE DADOS PESSOAIS: O DIREITO À PRIVACIDADE NA LEI N. 13.709/2018

Monografia apresentada ao Centro Universitário de Lavras como parte das exigências do curso de graduação em Direito.

APROVADO EM: 09/11/2023

ORIENTADORA

Profª. Ma. Adrielly Francine Rocha Tiradentes / UNILAVRAS

MEMBRO DA BANCA

Prof. Pós-Dr. Denilson Victor Machado Teixeira / UNILAVRAS

LAVRAS – MG

2023

A todos os envolvidos ao longo dessa caminhada.

AGRADECIMENTOS

Primeiramente, agradeço à minha mãe Cely, ao meu irmão Flávio, aos meus padrinhos e madrinhas, e também à minha namorada Moisa.

Agradeço também a todos os meus tios, bem como a todos aqueles amigos que sempre me ajudaram.

“Todas as vitórias ocultam uma abdicação”. (Simone de Beauvoir).

RESUMO

Introdução: Os avanços tecnológicos podem muitas vezes entrar em conflito com o direito fundamental à privacidade. No mundo de hoje, a privacidade dos cidadãos é violada e os seus direitos individuais são transgredidos a partir do momento em que a mesma se tornou mercadoria. Com isso, foi criado a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), que estabeleceu, pela primeira vez no ordenamento jurídico pátrio, conjunto de normas no intuito de regular o tratamento de dados pessoais em todas as atividades do cotidiano do brasileiro. A lei foi criada com o intuito de definir os deveres dos agentes que tratam dados, bem como estabelecer um regime jurídico para a sua responsabilidade face aos potenciais perigos que advêm de tais práticas. **Objetivo:** O objetivo principal da pesquisa foi realizar uma análise abrangente dos direitos do consumidor em relação ao princípio da publicidade, concentrando-se na aplicação deste princípio no âmbito digital, e na subsequente vulnerabilidade e responsabilidade que surge como resultado deste viés, particularmente no que diz respeito à LGPD. A pesquisa também buscou examinar o significado do direito à privacidade na esfera digital, e avaliou a LGPD sob essa perspectiva específica. Por fim, a pesquisa teve como objetivo escrutinar a LGDP no que diz respeito ao Código de Defesa do Consumidor e à responsabilidade associada a este tema. **Metodologia:** Trata-se do método hipotético-dedutivo em suas pesquisas, tendo sido utilizadas fontes bibliográficas especializadas e procedimentos hermenêuticos para alcançar uma compreensão profunda e definitiva do objeto de análise. **Resultado:** A discussão em torno deste tema enfatiza que, embora o quadro de responsabilidade civil para incidentes que envolvam tratamento de dados pessoais seja neutro, determinar a compensação por ganhos ilícitos exige mais do que avaliar a extensão dos danos sofridos pela parte afetada. É fundamental levar em conta os lucros auferidos pela empresa infratora, uma vez que a aplicação da responsabilidade civil opera de forma punitiva. **Conclusão:** O tratamento de dados pessoais acarreta riscos inerentes, pois envolve o direito fundamental à privacidade. Para mitigar esses riscos, a LGPD interpreta a responsabilidade civil de forma objetiva, responsabilizando quem descumprir as obrigações legais pelos danos resultantes, a menos que consiga provar que o nexo de causalidade foi rompido de acordo com a LGPD. Assim, a comunicação colaborativa entre CDC e LGPD potencializa a compreensão desse conceito, aumentando a proteção aos indivíduos vulneráveis cujas informações pessoais estão sendo manipuladas por um processador de dados, o qual funciona com maior responsabilidade e prestação de contas.

Palavras-chave: Lei Geral de Proteção de Dados; Direito do Consumidor; tratamento de dados; responsabilidade civil; ganhos ilícitos.

ABSTRACT

Introduction: Technological advances can often conflict with the fundamental right to privacy. In today's world, citizens' privacy is violated and their individual rights are transgressed from the moment it becomes a commodity. With this, the General Data Protection Law (Law No. 13,709/2018) was created, which established, for the first time in the national legal system, a set of rules with the aim of regulating the processing of personal data in all daily activities. of the Brazilian. The law was created with the aim of defining the duties of agents who process data, as well as establishing a legal regime for their responsibility in the face of the potential dangers arising from such practices**. Objective:** The main objective of the research was to carry out a comprehensive analysis of consumer rights in relation to the principle of advertising, focusing on the application of this principle in the digital sphere, and the subsequent vulnerability and liability that arises as a result of this bias, particularly with regard to Regard the LGPD. The research also sought to examine the meaning of the right to privacy in the digital sphere, and evaluated the LGPD from this specific perspective. Finally, the research aimed to scrutinize the LGDP with regard to the Consumer Protection Code and the responsibility associated with this topic. **Methodology:** This is the hypothetical-deductive method in their research, using specialized bibliographic sources and hermeneutic procedures to achieve a deep and definitive understanding of the object of analysis. **Result:** The discussion around this topic emphasizes that, although the civil liability framework for incidents involving the processing of personal data is neutral, determining compensation for ill-gotten gains requires more than assessing the extent of the damage suffered by the affected party. It is essential to take into account the profits made by the offending company, since the application of civil liability operates in a punitive manner. **Conclusion:** The processing of personal data carries inherent risks, as it involves the fundamental right to privacy. To mitigate these risks, the LGPD interprets civil liability objectively, holding those who fail to comply with legal obligations responsible for the resulting damages, unless they can prove that the causal link was broken in accordance with the LGPD. Thus, collaborative communication between CDC and LGPD enhances the understanding of this concept, increasing the protection of vulnerable individuals whose personal information is being handled by a data processor, which works with greater responsibility and accountability.

Keywords: General Data Protection Law; Consumer Law; data processing; civil responsability; illicit gains.

LISTA DE ABREVIATURAS

ANPD	Autoridade Nacional de Proteção de Dados
ART	Artigo
CDC	Código de Defesa do Consumidor
CF	Constituição Federal
LGPD	Lei Geral de Proteção de Dados
STJ	Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO

O ato de construir informações legalmente é considerado significativo e uma extensão do direito do indivíduo à privacidade. A origem deste direito remonta à dissolução do feudalismo e, desde então, evoluiu para um conceito multifacetado, com ligações aos bens e propriedades de uma pessoa.

O reconhecimento legal da privacidade como um direito fundamental surgiu muito mais tarde, a nível social e institucional. O estatuto da privacidade evoluiu de um privilégio de uns poucos seletos para se tornar uma necessidade para todos à medida que as condições materiais de vida da classe trabalhadora melhoraram. Só quando as necessidades básicas de privacidade são satisfeitas é que esta pode ser considerada uma exigência natural e não um luxo para alguns.

À medida que a nossa sociedade continua a evoluir e a dar prioridade à recolha e partilha de informação, as ciências, especificamente o direito, enfrentam desafios novos e únicos. Com o poder agora derivado do acesso à informação, a identificação dos tipos de informação que os indivíduos consentiram em partilhar e o conceito de privacidade tornaram-se cada vez mais importantes.

O processamento de dados também permite a concentração e o fortalecimento das estruturas de poder existentes. Em resposta a isto, surgiram legislações com o objetivo de salvaguardar e preservar os dados pessoais na nossa sociedade em rede. O seu objetivo é impedir, ou idealmente impedir, os perigos potenciais que advêm da acumulação e manipulação de dados pessoais. A defesa da privacidade no sistema jurídico brasileiro progrediu significativamente tanto do ponto de vista institucional quanto social. Ultrapassou a noção única de propriedade e permitiu a integração de controles individuais sobre os dados recolhidos e processados.

Nesse contexto brasileiro, a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), estabeleceu, pela primeira vez no ordenamento jurídico pátrio, conjunto de normas no intuito de regular o tratamento de dados pessoais em todas as atividades do cotidiano do brasileiro, incluindo, portanto, todos os setores da economia.

A lei foi criada com o intuito de definir os deveres dos agentes que tratam dados, bem como estabelecer um regime jurídico para a sua responsabilidade face aos potenciais perigos que advêm de tais práticas. Considerando os riscos que os indivíduos enfrentam neste mundo cada vez mais complexo, é inevitável que haja

consequências indesejáveis que devem ser remediadas e, idealmente, prevenidas. Como resultado, a parte da lei que diz respeito à responsabilidade e à indenização por danos – Seção III, do Capítulo VI, da LGPD – representa um desafio difícil em termos de teoria e prática jurídica.

Dentro da multiplicidade de cenários possíveis, existe responsabilidade civil pelas ações de particulares públicos e privados relacionadas com o tratamento de dados. Sob tais considerações, estipula-se o seguinte problema de pesquisa: aplica-se a responsabilidade civil a esses sujeitos na modalidade objetiva ou subjetiva? Quais as consequências de sua incidência? Para satisfazer os requisitos metodológicos, a conclusão mais direta é aplicar a responsabilidade objetiva de acordo com as disposições legais. Porém, há exceções e peculiaridades que serão vistas ao longo do trabalho em tela.

O objetivo geral da pesquisa foi analisar de modo sintético o direito do consumidor, sob a ótica do princípio da publicidade como um todo, afunilando-se na questão da aplicação de tal princípio sob o viés digital e sua vulnerabilidade e, por fim, a responsabilidade na LGPD. Já quanto ao objetivo específico foi verificar o de verificar a importância do direito à privacidade de modo geral e sob o aspecto do âmbito digital, bem como analisar a LGPD sob tal ótica. Por fim, buscou-se especificamente analisar a LGDP sob o ponto de vista do Código de Defesa do Consumidor e a responsabilidade afeta ao tema.

No que tange à justificativa do presente estudo, se configura pela grande quantidade de processos no Poder Judiciário que versam sobre o presente tema, bem como pela atualidade de um mundo globalizado e a legislação brasileira tardia a respeito do próprio tema. Além disso, no sistema jurídico brasileiro, a proteção da privacidade obteve progressos substanciais tanto do ponto de vista social como institucional. O conceito de privacidade evoluiu para além da mera propriedade e agora abrange a capacidade de um indivíduo exercer controle sobre a recolha e processamento dos seus dados.

Quanto à metodologia do presente trabalho, aos autores observados e aqui analisados, é cediço que se trata do método hipotético-dedutivo em suas pesquisas, tendo sido utilizadas fontes bibliográficas especializadas e procedimentos hermenêuticos para alcançar uma compreensão profunda e definitiva do objeto de análise.

2 REVISÃO DE LITERATURA

2.1 DIREITO FUNDAMENTAL À PRIVACIDADE

Anteriormente, é importante conceber que a evolução histórica da legislação sobre proteção de dados, demonstra tênue linha sobre tal direito – que em breve será demasiadamente apreciado – e o direito de tutela à privacidade e, consequentemente, os direitos fundamentais. Dito isso, passa-se à análise do direito à privacidade no âmbito nacional, bem como as noções gerais sobre tal princípio e também sua normativa prevista e também inserido no contexto digital.

De mais a mais, necessário destacar primeiramente que, a palavra "privacidade", conforme aduz Assis (2015), é apontada como um anglicismo da palavra *privacy*, tendo raiz no termo latim *privare*. Contudo, a palavra "privacidade" não tem um único conceito e objetivo, mas sim tendo diversos posicionamentos doutrinários a respeito de seu significado, desde os mais abrangentes até aos mais restritos.

Para Robert Alexy (2002, *apud* MARQUES, 2008), existem três níveis de proteção à vida privada, sendo elas:

> A esfera mais interna, caracterizando-se por ser o âmbito mais íntimo, a esfera íntima intangível, o âmbito núcleo absolutamente protegido da organização da vida privada, compreendendo os assuntos mais secretos que não devem chegar ao conhecimento dos outros devido à sua natureza extremamente reservada; a esfera privada ampla, que abarca o âmbito na medida em que não pertença à esfera mais interna, incluindo assuntos que o indivíduo leva ao conhecimento de outra pessoa de sua confiança, ficando excluído o resto da comunidade; e a esfera social, que engloba tudo o que não for incluído na esfera privada ampla, ou seja todas as matérias relacionadas com as notícias que a pessoa deseja excluir do conhecimento(s) de terceiros. (ALEXY, 2002, *apud* MARQUES, 2008, p. 1).

Assim, de forma ampla, o contexto da privacidade guarda relação com o direito subjetivo e inerente de cada indivíduo, abrangendo, portanto, o modo de vida individual, doméstico, bem como as relações familiares e afetivas, também os hábitos, nome, imagens e pensamentos. Dessa forma, o direito à privacidade é entendido nada mais do que aquilo que nos preserva do conhecimento alheio, sendo reservada a cada indivíduo a própria vivência (VIEIRA, 2017).

Para Lafer (1998, *apud* MACEIRA, 2012), o conceito de privacidade tem relação não somente ao direito de estar só, mas também resguardado a toda pessoa

a possibilidade de excluir do conhecimento de terceiros aquilo em que só diz respeito ao modo de ser no espaço da vida privada.

No mesmo sentido, sob um viés constitucionalista, a definição de privacidade poderá ser:

> A faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano. (BASTOS, 2000, p. 56)

Nesse contexto, destaca Paesani (2014) que o direito à privacidade tem como fundamento a defesa da personalidade humana contra intromissões alheias.

Em um contexto histórico, cumpre ressaltar que a respeito do presente tema, a Constituição Francesa de 1791, bem como a Constituição Norte-Americana de 1787, trouxeram o constitucionalismo moderno, fazendo com que o Estado se tornasse limitado pelas próprias leis, abstendo-se de causar determinadas interferências, de forma massiva, na liberdade dos indivíduos, passando a haver prerrogativas e sujeições para a formação do Estado Democrático de Direito (DI PIETRO, 2017).

Dessa forma, conforme ressaltado por Canotilho (2003), o constitucionalismo, em seu primeiro momento, significou apenas manobra de forma especificada para as limitações de poder, porém, com fins de garantias.

Nesse sentido, no século XX, para cumprir as suas funções, como a defesa da justiça e a proteção dos cidadãos, o Estado passou por um processo de constitucionalização dos direitos privados. Como resultado, a Constituição foi redefinida como a norma primária para todo o sistema jurídico no Brasil, servindo como pré-requisito para a validade de todas as leis (KELSEN, 1998).

Como cediço, a evolução histórica das leis de proteção de dados é indicativa da associação entre este direito e a proteção da privacidade, por isso está associado aos direitos fundamentais. Sobre isso, Mendes (2014) destaca tal evolução legislativa subdivida entre quatro gerações.

Em um primeiro momento, durante a década de 70, as pessoas começaram a preocupar-se com as bases de dados da administração pública e com a influência que estas tinham no poder do Estado sobre a vida pessoal dos cidadãos. Nesse ponto, foram estabelecidas regulamentações relativas a novos bancos de dados, como a necessidade de permissão prévia por escrito para criar um sistema de armazenamento (MENDES, 2014).

Numa segunda fase, o foco foi nas regulamentações de proteção de dados pessoais e privacidade, onde tais regulamentações estavam mais preocupadas com o procedimento em si do que com os padrões de proteção de dados e privacidade. A terceira geração, ocorrida na década de 80, deu início ao conceito de autonomia informacional, que é definida como a participação das pessoas no tratamento dos dados, “como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como opção entre ‘tudo ou nada’” (MENDES, 2014, p. 42).

A quarta iteração dos regulamentos de proteção de dados incorporou a proteção de “dados sensíveis”, ao mesmo tempo que estabeleceu padrões para vários setores. Os dados sensíveis abrangem informações pessoais relativas a aspectos específicos e potencialmente sensíveis, incluindo, entre outros, orientação sexual, género, etnia, origem social, crenças religiosas, tendências filosóficas, registos de saúde e dados genéticos. Dado esse contexto, em âmbito nacional, tal conceito foi positivado pela Lei do Cadastro Positivo (Lei n. 12.414/2011) (MENDES, 2014).

Em momento posterior, a Lei Geral de Proteção de Dados, mais precisamente em seu artigo 5º, inciso II, dispôs sobre o dado pessoal sensível, sendo taxado como aquele de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, bem como dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

A proteção constitucional à privacidade é uma observação bem reconhecida. Não é suficiente que o Estado se limite a restringir a sua autoridade nas interações verticais com os indivíduos. Pelo contrário, deve tomar medidas para fazer cumprir e salvaguardar os direitos fundamentais nas relações horizontais entre vários membros da sociedade (NETO VASCONCELOS, 2022).

O objetivo principal do Estado é garantir que o direito à privacidade seja protegido nas relações intersubjetivas onde tenha havido violação devido ao exercício irregular da liberdade de outrem. Esse direito é ainda reforçado pela competência descrita no artigo 5º, inciso XXXV, da CF/88, que deixa claro que o Poder Judiciário levará em conta eventuais alegações de lesão ou ameaça a direitos (NETO VASCONCELOS, 2022).

No entanto, a privacidade adquiriu novo significado com os avanços tecnológicos, quando se aborda o tema da privacidade no espaço cibernético.

> Apresenta duas ordens de problemas: o primeiro reporta-se ao respeito à esfera privada alheia que nos conduz no terreno tradicional da tutela da privacidade. O segundo refere-se à privacidade de quem se movimenta naquele espaço e, consequentemente, requer o anonimato. Contudo, os dois problemas estão destinados a saberem as consequências que o indivíduo pode ter se for considerada que a sua privacidade está sendo violada por uma informação na rede. (PAESANI, 2014, p. 39)

No que concerne aos dados pessoais, é cediço que sua proteção se encontra galgada pela necessidade de preservação da privacidade e da complementaridade e solidariedade dos princípios constitucionais (art. 5º, §2º, da CF). Não obstante, no mesmo artigo, em seu inciso X, também da Constituição Federal, dispõe-se que são “invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas” (BRASIL, 1988). De mais a mais, o Código Civil também preconiza em seu artigo 21 que a vida privada da pessoa natural é inviolável, constituindo a privacidade um direito da personalidade (BRASIL, 2002).

2.1.2 O Direito à privacidade no âmbito digital

Desde a virada do milênio, novos avanços tecnológicos têm emergido rapidamente e dominado vários campos. Com o passar do tempo, tem havido uma tendência crescente de interatividade entre os utilizadores desta unidade, onde a antiga mídia não detém o monopólio da criação de informação. A noção de comunicação formal evoluiu e, em vez de ser um conceito independente, tornou-se integrada na comunidade global.

Sob esse contexto, é importante ressaltar que a privacidade no mundo moderno é influenciada pela grande quantidade de dados e informações que são processadas, isso altera a perspectiva dos responsáveis quanto à sua abordagem (MENDES, 2023). Nesse sentido, de acordo com Doneda (2006), não é suficiente mentalizar a privacidade no modelo de um direito subjetivo, que deva ser tutelado de acordo com as conveniências individuais.

Sendo assim, conforme destaca Vieira (2017), o expoente que cresce cada vez mais ocupando espaço na era das tecnologias, diz respeito às redes sociais, visto que permitem o compartilhamento de ideias e informações entre seus usuários com objetivos e valores comuns.

Assim, as redes sociais são consideradas um tipo especial de comunidade online na qual os usuários se comunicam usando suas informações pessoais para criar perfis e se conectar com outros usuários. Essas informações fornecidas pelos usuários muitas vezes podem incluir entretenimento, interesses pessoais e profissionais, informações de identificação pessoal e fotos ou vídeos de suas vidas sociais ou pessoais (SLAVOV, 2009).

Neste contexto, uma das maiores preocupações das pessoas nas redes sociais é a incapacidade de filtrar ou selecionar eficazmente o que é útil. Isso porque, a cada segundo, milhões de usuários divulgam suas opiniões, emoções, fotos e vídeos nas redes sociais, sem levar em conta o fator segurança dessas informações, fundamental para preservar a privacidade e a dignidade do ser humano (SLAVOV, 2009).

O progresso da tecnologia pode por vezes entrar em conflito direto com o direito fundamental à privacidade. Estes avanços podem alterar subitamente o âmbito da recolha de dados, exigindo que os utilizadores exerçam controle e possuam conhecimento das suas preferências, hábitos e interesses. À medida que a rede se expande, a probabilidade de ligações entre bases de dados aumenta, tornando imperativo que os indivíduos estejam conscientes dos costumes e tendências que moldam a sua pegada digital (LIMBERGER, 2016).

Nesse sentido, destaca Graieb que:

> A violação da privacidade muitas vezes é realizada pela própria vítima, o que pode se chamar de “paradoxo da privacidade”, sendo que todos os dias, as pessoas se afligem por estar vulneráveis à espionagem digital. Contundo desvelam sua intimidade on-line ao permitir que desconhecidos tenham acesso a seu computador, em redes sociais, por exemplo, local em que revelam uma larga fatia de sua vida com fotos, depoimentos e vídeos. (GRAIEB, 2009, p. 81)

Num mundo onde a maioria das informações pessoais é armazenada em formato digital, algumas informações que deveriam permanecer privadas podem tornar-se perigosas. A privacidade online torna-se então um bem precioso de valor limitado, mas que ainda deve ser preservada (GRAIEB, 2009).

Nesse sentido, com a existência de conflitos que envolvem a violação da privacidade das informações dos usuários nas redes, anteriormente, aplicava-se por analogia o artigo 5º, inciso X, da Constituição Federal, justamente por não existir lei específica que pudesse solucionas os conflitos existentes decorrentes do espaço virtual (VIEIRA, 2017).

Diante desse cenário, no ano de 2014, nasceu com a aprovação do Congresso Nacional, no dia 25 de março, a Lei n. 12.965/2014, conhecida popularmente como Marco Civil da Internet, com o objetivo de finalmente regulamentar o uso da Internet no Brasil, no intuito de preencher o vazio legislativo que existia no ordenamento jurídico brasileiro a respeito do presente assunto (VIEIRA, 2017).

Em paralelo ao Marco Civil da Internet, surgiu a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), vindo a disciplinar o uso da internet no Brasil, justamente para quem faz uso de tal rede, vindo a delimitar, inclusive, a própria atuação do Estado nesse âmbito.

Como já mencionado, atualmente, há uma quantidade excessiva de auto exibição em plataformas de mídia social que são cada vez mais sinônimos de internet. Estas plataformas oferecem uma vasta gama de informações, incluindo opiniões, imagens e dados potencialmente pessoais, o que apenas intensifica a propagação contínua da comunicação que pode ser espalhada pelo mundo (MENDES, 2023).

Consequentemente, o impacto da internet na autonomia das pessoas, na liberdade de ação e na tomada de decisões é direto, seja nas comunicações através de redes ou nas conversas quotidianas realizadas em tempo real. Neste contexto, a privacidade dos cidadãos é violada e os seus direitos pessoais são violados. A intimidade tornou-se uma mercadoria numa sociedade que valoriza o consumo e tornou-se uma moeda de troca constante, com muitos dispostos a pagar para sua divulgação (MENDES, 2023).

Para Miragem (2013), e evidente, portanto, que vivemos num mundo de dados e os nossos pensamentos, ações e falhas na aquisição foram convertidos num produto de poder financeiro, sendo os dados a fonte e alicerce do mundo moderno, tornando-se, atualmente, o ativo mais importante. Sendo assim, proteção de dados e a privacidade na internet estão diretamente relacionadas com a proteção dos dados pessoais dos consumidores, os quais requerem uma proteção eficaz, visto que há um liame intrínseco ao Código de Defesa do Consumidor (MENDES, 2023).

2.1.2.1 Vulnerabilidade das redes sociais no espaço digital

Como é de conhecimento geral, a era digital, que se caracteriza pela internet e pelas tecnologias de informação e comunicação, tornou o mundo mais pequeno, à distância de um clique, vindo a permitir uma maior migração de pessoas e informações pessoais. Uma verdade que confronta todos com a necessidade de salvaguardar os

seus dados pessoais, evitando que sejam utilizados indevidamente por terceiros, desrespeitando um direito básico, que é o direito à privacidade.

Como é de conhecimento amplo, a corrida em busca do lucro marca como crivo central os entremeios das redes sociais, onde grandes corporações com fins lucrativos, tais como Facebook e Instagram, adotam estratégias de negócios no intuito de angariar a atenção dos usuários aos seus produtos e serviços (FUGAZZA; SALDANHA, 2017)

De acordo com Eli Pariser (2012), ativista político e cibernético, tais corporações se dignam a conquistar a fidelidade de seus usuários por meio da personalização e filtros de conteúdo, sendo realizado através de solicitação e análise de dados pessoais dos mesmos, como é o caso dos *cookies* e *beacons*[1].

Ainda conforme os ditames do mesmo estudioso, tais empresas reúnem o maior número possível de informações sobre os usuários, em que tais corporações desenvolvem algoritmos de personalização no intuito de direcionar anúncios, serviços aos usuários alvo, a partir de uma análise de perfil. Nesse sentido, para Pariser (2012, p. 12), “a tentativa de saber o máximo possível sobre seus usuários tornou-se a batalha fundamental da nossa era entre gigantes da internet, como Google, Facebook, Apple e Microsoft”.

Segundo o autor, o problema surge quando as empresas digitais utilizam os dados dos seus utilizadores sem a sua permissão explícita e, por vezes, até em seu detrimento. Os termos de uso, que descrevem as políticas de privacidade, políticas de cookies e o uso dos dados fornecidos, entre outras coisas, regem o acordo legal entre as corporações digitais (incluindo redes sociais) e seus usuários (PARISER, 2012).

> A personalização se baseia numa barganha. Em troca do serviço de filtragem, damos às grandes empresas uma enorme quantidade de dados sobre nossa vida diária [...]. Essas empresas estão ficando cada vez melhores no uso desses dados para traçar suas estratégias. No entanto, muitas vezes acreditamos excessivamente que essas empresas irão cuidar bem dessas informações, e, quando nossos dados são usados para tomar decisões que nos afetam negativamente, em geral não ficamos sabendo. (PARISER, 2012, p. 20)

---

[1] *Cookies* são pequenos arquivos de texto (normalmente composto por letras e números inseridos na memória do navegador ou dispositivo quando se visitar algum *website*, para que este último reconheça o navegador ou dispositivo em específico. Já os *beacons* são pequenas imagens gráficas (também conhecidas como *pixel tags* ou *clear GIFs*) que podem ser incluídas em *websites*, serviços, aplicativos, mensagens e ferramentas, que normalmente funcionam em conjunto com os *cookies* para identificar os usuários e seu comportamento. Disponível em: <https://www.sumup.com/pt-br/transparencia/cookies/> Acesso em: 15 out 2023.

De acordo com Ferreira (2014), a vigilância atual assumiu determinada posição através do setor privado, sendo possível observar a forma como as empresas, precipuamente as digitais, lidam com as informações dos usuários da internet, vindo a possuir vasta liberdade de acesso às informações dos usuários e, principalmente, daqueles usuários que utilizam seus serviços.

Nos tempos modernos, os princípios de independência, singularidade e confidencialidade sofreram uma metamorfose e emergiram como atributos interligados (CAPURRO, 2016).

O mesmo autor postula que a compreensão atual de “ser-no-mundo” é sinônimo de “ser-no-mundo-compartilhado”, dando origem à ideia de conhecimento ético coletivo. Além disso, o autor sugere que a noção de partilha se estende para além do domínio digital e é contígua ao mundo não digital. Segundo o autor, os dois mundos não são mutuamente exclusivos, mas sim em constante estado de alternância (CAPURRO, 2016).

A percepção de privacidade de Rafael Capurro (2016) é vista através das lentes da fenomenologia da identidade, ou “quem”. Este fenômeno envolve a manifestação de indivíduos em um mundo compartilhado, onde eles mostram quem são por diversos meios. Essa exibição de si mesmo depende da utilização de “máscaras de habilidade”, que incluem a adoção de comportamentos específicos e o uso de determinados trajes para se apresentar de uma maneira específica. Através destes meios, os indivíduos desenvolvem o seu poder pessoal e moldam a forma como são percebidos no mundo.

> A “personalidade pública” (public persona) do indivíduo, qual seja, a máscara que este indivíduo apresenta aos outros acerca de quem ele é, recebe certa reputação, referente ao quão estimada é a pessoa ao longo dos anos. Ética, no entendimento de Eldred (ibid.), significa viver em concordância com o ethos de um estilo de vida compartilhado ao longo da história por um povo. Isto implica que um dano à reputação de um indivíduo corresponde a um ataque à sua vida privada. Com a Internet, as possibilidades de revelar sua identidade cresceram exponencialmente, assim como as formas de rastrear as atividades digitais que se queira recuperar através de uma consulta à matriz da rede, que registra todo e qualquer movimento digital; tornando mais fácil ferir a reputação de alguém. Assim como cresceram as formas de auto apresentação no ciberespaço, também as ações que ocasionam os cibercrimes possuem mais “chances” de serem eficazes no ambiente digital do que no não digital. Isto porque, segundo Eldred, toda ação no ciberespaço é melhorada quando comparada com as ações no mundo físico. O autor ainda nos fornece a concepção de que a nossa identidade digital consiste em responder à questão acerca do que somos no ciberespaço. Ele afirma que, neste contexto, somos nossos dados digitais; e que são estes os que necessitam de proteção ética e legal. (FUGAZZA; SALDANHA, 2017, p. 98)

Para que um indivíduo exerça a sua liberdade, deve ter um conjunto de opções para revelar a sua identidade num espaço partilhado, incluindo a escolha do horário e do local. Até o Estado reconhece a importância desta questão, nomeadamente em termos de segurança nacional. Assim, acredita-se que o direito à privacidade pessoal e familiar implica a liberdade de escolher o próprio método de divulgação ou ocultação de si mesmo e de suas informações. Esta liberdade envolve a autoridade para determinar como se quer interagir com os outros num mundo que se está a tornar cada vez mais interligado e comunitário (CAPURRO, 2016).

2.2 A LGPD E A PROTEÇÃO DA PRIVACIDADE

Como é sabido, o intenso debate a respeito da proteção da privacidade dos usuários da internet, em conluio com inúmeras práticas invasivas e abusivas, contribuiu firmemente para o surgimento da Lei n. 13/709/2018 (Lei Geral de Proteção de Dados).

A Lei Geral de Proteção de Dados (LGPD), dentre seus fundamentos, um dos mais importantes é o do respeito à privacidade, previsto em seu artigo 2º, inciso I.

Seus regulamentos contêm várias disposições destinadas a salvaguardar o direito básico de um indivíduo à privacidade. Uma delas dita a necessidade do consentimento informado, o que significa que a recolha de dados deve ser transparente e os indivíduos devem estar cientes de como os seus dados serão utilizados antes de os fornecer (VASCONCELOS NETO, 2022). Além disso, as regras proíbem a recolha de dados sem essa transparência, visto eu, conforme leciona o artigo 8º, §3º, da LGPD, “é vedado o tratamento de dados pessoais mediante vício de consentimento” (BRASIL, 2018).

Já em seu artigo 5º, inciso XII, resta expressa seu consentimento, preconizando ser o mesmo “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018). Nesse sentido, em tese, o referido artigo possibilita que a vontade do indivíduo seja considerada no tratamento de seus dados, isto é, vindo a afastar consentimentos genéricos e abstratos (VASCONCELOS NETO, 2022).

Conforme leciona Monteiro:

> O consentimento livre, expresso e informado, será aquele em que o usuário não é forçado a concordar com os termos do contrato, e as cláusulas que discorrem sobre qualquer tipo de tratamento de dados — inclusive

> fornecimento a terceiros — deverão ser redigidas de forma destacada, e se possível, separadas das demais. (MONTEIRO, 2014, p. 149)

É inviável alterar os dados dos usuários sem informá-los previamente que suas informações pessoais serão utilizadas para fins específicos. Para ilustrar, existem plug-ins que auxiliam nas métricas do site, rastreando a origem do tráfego do site. Esses plugins especializados exigem que as empresas obtenham a aprovação do usuário para utilizar seus dados pessoais, incluindo a identificação de seu dispositivo e localização geográfica. Isto está de acordo com a Política de Privacidade, que exige que as empresas informem os usuários sobre qualquer monitoramento que realizem (VASCONCELOS NETO, 2022).

> A denominada privacidade contextual é um direito da personalidade, desdobramento do direito à privacidade e do direito à intimidade, conferindo-se ao seu titular, em tempos de sociedade da informação, o exercício de sua autodeterminação informacional. Assim, o titular dos dados pessoais possui controle efetivo e contínuo a respeito do fluxo informacional. (LISBOA, 2019, p. 11)

Apesar de estar enquadrado no âmbito da privacidade em sentido geral, o direito à autonomia informacional difere deste, este último decorre da sua natureza dinâmica e fluida (BARRETO JÚNIOR; NASPOLINI, 2019).

Demais disso, é necessário ressaltar que a LGPD é reflexo da GDPR (*General Data Protection Regulation*), lei essa europeia que em 2016 passou a conferir maior transparência e proteção aos dados em nível internacional.

Como já mencionado, em 2014, o Marco Civil da Internet teve como objetivo revolucionar o espaço virtual seguro e confidencial. Isso se devia ao crescente ambiente caótico que estava se tornando predominante. É importante notar que, em 2012, foi introduzida a Lei Carolina Dieckman, que mudou o jogo para o sistema jurídico nacional no que diz respeito ao crime cibernético. Essa lei classificou a divulgação de informações privadas como potencial crime, conforme previsto na Lei de Crimes Cibernéticos (Lei 12.737/2012). Consequentemente, houve um impulso significativo no sentido de regulamentar o comportamento em ambientes virtuais, o que resultou na LGPD (VASCONCELOS NETO, 2022).

Com isso, a LGPD nasceu da necessidade de implementar a proteção da privacidade dos usuários, pois determina que os gestores dos sites revelem suas atividades para regular os dados dos usuários.

2.2.1 Armazenamento de dados e o princípio da finalidade

Para além de tudo que fora mencionado a respeito da LGPD, é de suma importância também destacar que a mesma determina que os dados são subdivididos entre: dados pessoais, dados pessoais sensíveis e dados anonimizados, com a seguinte definição:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. (BRASIL, 2018)

A implementação de tais ideias é vital para garantir a salvaguarda ideal dos dados relativos aos indivíduos, defendendo assim o seu direito à privacidade. Uma vez superado o obstáculo acima mencionado, é imperativo aderir a um princípio fundamental quando se trata de proteger dados pessoais: o princípio da finalidade ou especificação das finalidades. Este princípio determina que todas as ações relacionadas com a utilização de dados devem ser comunicadas ao proprietário dos referidos dados e que a sua finalidade original não deve ser alterada ou desviada (GODINHO; QUEIROGA NETO, *et. al.*, 2020).

Sobre esse princípio aplicado ao caso da LGPD, esclarece márcio Cots e Ricardo Oliveira o seguinte:

> O tratamento de dados precisa ter uma finalidade, ou seja, um resultado único, específico e legítimo que deve ser alcançado com tal tratamento. O princípio serve não apenas para delimitar o objetivo final do tratamento, mas para tornar previsível o que dele se espera, inviabilizando tratamento posterior desvinculado com a finalidade original. Exemplos de violação ao princípio da finalidade: i) informar que a coleta de dados servirá para faturamento de produto ou serviço, mas utilizar os dados para campanhas de marketing; ii) informar que o compartilhamento de dados se dará com a empresa X, mas compartilhar os mesmos com a empresa Y, iii) informar que os dados não serão copiados, mas realizar cópias destes. (COTS; OLIVEIRA, 2019, p. 77)

A implementação de tais ideias é vital para garantir a salvaguarda ideal dos dados relativos aos indivíduos, defendendo assim o seu direito à privacidade. Uma vez superado o obstáculo acima mencionado, é imperativo aderir a um princípio fundamental quando se trata de proteger dados pessoais: o princípio da finalidade ou

especificação das finalidades. Este princípio determina que todas as ações relacionadas com a utilização de dados devem ser comunicadas ao proprietário dos referidos dados e que a sua finalidade original não deve ser alterada ou desviada (GODINHO; QUEIROGA NETO, *et. al.*, 2020).

2.2.2 Legislação especial sobre proteção de dados pessoais e implicações

Devido à importância do controle da pessoa sobre seus dados pessoais, a LGPD instituiu um sistema altamente baseado em princípios que, principalmente, exige consentimento em relação ao armazenamento de dados, com ênfase especial neste requisito, exigindo que a pessoa consinta especificamente com o armazenamento de seus dados e, o mais importante, autorizando a pessoa a revogar os seus direitos de armazenamento de dados de forma voluntária (NOVAKOSKI; NASPOLINI, 2020).

Nesse sentido:

> Entende-se que o sistema desenvolvido tem como pilares centrais: a) amplo conceito de dado pessoal; b) necessidade de que qualquer tratamento de dados tenha uma base legal; c) rol taxativo de hipóteses legais para o tratamento de dados; d) caracterização detalhada do consentimento do titular e preocupação com sua manifestação; e) legítimo interesse como uma das hipóteses autorizativas e necessidade de realização de um teste de balanceamento de interesses para a sua regular aplicação; f) amplo rol de direitos do titular; e g) densa carga principiológica. (TEFFÉ; VIOLA, 2020, p. 38)

Após a obtenção dos dados pessoais, sejam eles gerais ou sensíveis e com o consentimento do indivíduo, o responsável pelo tratamento ou operador da base de dados fica livre para tratar os referidos dados. No entanto, esse tratamento deverá obedecer aos princípios estabelecidos e às limitações prescritas pela legislação e regulamentação emanada da autoridade nacional de proteção de dados (ANPD) para evitar incorrer em responsabilidade civil. Esses princípios e limitações estão descritos nos artigos 6º, I a X e no artigo 46 da LGPD (NOVAKOSKI; NASPOLINI, 2020).

A legislação LGPD trouxe diversas mudanças dignas de nota, incluindo a introdução de certos pré-requisitos que os processadores de dados devem cumprir ao armazenar dados do usuário. O mais significativo destes pré-requisitos é a exigência de que a recolha e utilização de dados pessoais apenas ocorra para uma finalidade específica que tenha sido comunicada ao titular dos dados e com a sua autorização explícita. Além disso, a lei determina que os processadores de dados devem informar os titulares dos dados sobre quaisquer violações potenciais, sejam incidentais ou

ilícitas, da segurança das suas informações pessoais, pondo assim fim - pelo menos em teoria - a práticas antiéticas, como a divulgação de informações pessoais sem o conhecimento ou consentimento do titular dos dados (NOVAKOSKI; NASPOLINI, 2020).

> Os agentes de tratamento deverão proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais. Para tanto, deverão adotar uma série de medidas de segurança, técnicas e administrativas. (MATTOS FILHO; VEIGA FILHO, *et. al*, 2018, p. 25)

Uma das principais ações exigidas por lei para garantir a proteção de dados é a nomeação de um indivíduo designado responsável por supervisionar o controle interno do processamento de dados. Este indivíduo, que deverá ser contratado pelos agentes de tratamento, será responsável por facilitar a comunicação entre os titulares dos dados, as empresas que tratam os dados pessoais e o órgão de controle externo (ANPD) conforme especificado no art. 5º, VIII da LGPD (NOVAKOSKI; NASPOLINI, 2020).

> Outra fundamental característica da nova legislação consiste no significativo fomento ao aspecto preventivo, estabelecendo procedimentos mandatórios para os controladores e operadores de dados pessoais, tais como os deveres atinentes à implementação de severas políticas de segurança para proteção dos dados de acessos não autorizados.9 Cuida-se de perspectiva alvissareira, na medida em que as características inerentes ao “meio digital” – entre elas a velocidade das transformações tecnológicas, a capacidade de propagação de informações e a dificuldade na contenção do fluxo de dados –, associadas à expansão da coleta e do tratamento implicam desafios à lógica repressiva, ainda mais quando esta decorre do modelo comando-controle.10 O engajamento espontâneo dos titulares dos deveres e a prevenção na tutela do direito fundamental aos dados pessoais afiguram-se essenciais e, não à toa, no que diz respeito a este último aspecto, cuida-se de princípio plasmado no art. 7º, VIII, da LGPD. (FRAZÃO; OLIVA, *et. al.*, 2019, p. 681)

Uma das mudanças notáveis que vieram com a LGPD foi a introdução de uma nova entidade, a Autoridade Nacional de Proteção de Dados (ANPD), que visava garantir maior sensibilidade à proteção de dados. Infelizmente, esta disposição foi rejeitada pelo então Presidente Michel Temer, citando fundamentos constitucionais de que apenas o Presidente tem autoridade para criar “cargos, funções ou empregos públicos na administração direta e autónoma”. No entanto, a Medida Provisória nº. Em dezembro de 2018, foi editada a Portaria nº 869, que instituiu a ANPD, mas ainda está em tramitação no Congresso Nacional (NOVAKOSKI; NASPOLINI, 2020).

Ainda de acordo com Novakoski e Naspolini (2020), à ANPD são atribuídas tarefas críticas pela LGPD, incluindo o monitoramento do cumprimento das regulamentações previstas na legislação. Além disso, a ANPD é responsável por criar padrões de segurança para armazenamento de dados e avaliar a gravidade de quaisquer violações de segurança de dados que ocorram.

Em resposta a estas violações, são tomadas medidas para mitigar os efeitos do incidente, podendo ser impostas sanções administrativas aos agentes de tratamento. As empresas enfrentam multas pesadas de acordo com esta legislação, com penalidades que chegam a 2% de sua receita anual, limitadas a R$ 50 milhões por violação. Embora a lei permita multas elevadas em casos de divulgação de dados pessoais, os recursos arrecadados são integralmente destinados aos cofres do Estado e não indenizam os titulares dos dados que tenham sido prejudicados. Este aspecto da sanção realça o seu carácter pedagógico e punitivo, mas não serve de compensação para os afetados pela infracção (NOVAKOSKI; NASPOLINI, 2020).

Nesse sentido:

> A implementação de boas práticas no tratamento de dados pessoais possui estrondoso potencial para auxiliar no atendimento aos comandos gerais da lei de acordo com as particularidades de determinados agentes econômicos, bem como prevenir a ocorrência de violações aos direitos dos titulares, na medida em que permite orientar os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus standards e conceitos abertos. Por se tratar de complemento à regulação estatal, apresenta, ainda, a capacidade de gerar incentivos que agregam e aprofundam controles, adaptando-lhes diante da natureza extremamente dinâmica das evoluções tecnológicas em matéria de dados. (FRAZÃO; OLIVA, *et. al.*, 2019, p. 682)

Pode-se inferir que a eficácia prática da LGPD será significativamente limitada sem a criação e organização da Autoridade Nacional de Proteção de Dados. Isto porque uma parte significativa das suas responsabilidades inclui monitorizar o cumprimento da lei, garantir a segurança e proteção dos dados, bem como investigar quaisquer potenciais violações de segurança (NOVAKOSKI; NASPOLINI, 2020).

Ainda com relação à proteção de dados, é cediço que:

> Dizer que os danos aumentaram em nosso século envolve certo truísmo. Se nós, no início do século passado, engatinhávamos nas possibilidades tecnológicas, se sequer conhecíamos a televisão ou o avião, se uma notícia demorava lentos meses para partir da Europa e chegar até aqui, hoje, desnecessário dizê-lo, a situação modificou-se de modo impensável. É possível até afirmar, sem medo de errar: talvez a mais otimista das previsões não previsse que chegaríamos aonde chegamos, em possibilidades tecnológicas. As possibilidades de danos são muitas. Algumas perfazem

> crime, como o uso de dados de cartões de crédito ou débito de forma indevida ou sem autorização. Da mesma forma, a invasão não autorizada para furtar informações confidenciais. (FARIAS; ROSENVALD, *et. al*, 2018, p. 771)

A eficácia da exclusão de dados é de extrema importância. Isso é abordado inicialmente no Marco Civil da Internet (artigo 7º, dados). Adicionalmente, o dispositivo primário do artigo 16 da LGPD estabelece que o controlador é responsável pela disposição dos dados pessoais após a conclusão do seu tratamento, conforme estipulado no dispositivo acima mencionado. É importante notar, no entanto, que este direito não é absoluto. Isso é evidenciado pela extensa lista de situações descritas no item 16 da LGPD, em que o controlador não é obrigado a atender à solicitação de exclusão de dados do respectivo titular (NOVAKOSKI; NASPOLINI, 2020).

Nesse sentido, o artigo 16 dispõe que:

> Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
> I - cumprimento de obrigação legal ou regulatória pelo controlador;
> II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018)

Para examinar esta questão, deve-se realizar uma análise dos efeitos que o direito ao apagamento de dados tem tanto na atividade econômica exercida pelos processadores de dados como nos direitos fundamentais dos indivíduos envolvidos, incluindo o direito à privacidade.

> Qualquer dado vinculado ou potencialmente vinculável a uma determinada pessoa natural, portanto, encontra-se englobado no escopo protetivo da LGPD (observadas as exceções do art. 4º), independentemente do meio de armazenamento (art. 5º, IV), o que, em, conjunto com a definição de "tratamento de dados" (art. 50, X) – "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, X) – caracteriza a ampla incidência da LGPD às mais diversas atividades. (FRAZÃO; OLIVA, *et. al.*, 2019, p. 695)

Não se pode argumentar que o armazenamento de dados pessoais é um aspecto vital da economia empresarial, proporcionando uma fonte significativa de ativos. Exemplos desta prática são receber chamadas telefónicas não solicitadas de

operadores de telemarketing que oferecem produtos ou serviços não solicitados, ou ser inundado com anúncios de produtos após fazer uma compra ou navegar online por longos períodos de tempo. Além disso, há situações em que indivíduos cadastram seu CPF em supermercados ou farmácias para receber descontos nos preços dos produtos (NOVAKOSKI; NASPOLINI, 2020).

> Em decorrência do valor dessas informações, muitas empresas simplesmente preferem descumprir a lei, negando-se a eliminar os dados, por entender que é mais vantajoso arcar com possíveis sanções provenientes de tal conduta do que se livrar de uma das suas maiores fontes de ativo. É o que aponta uma pesquisa realizada pela *Talend*, que analisou a implementação da *General Data Protection Regulation* (GDPR) – a lei europeia, de abril de 2016, que regula o tratamento de dados. Segundo a pesquisa, até agosto de 2018 – após 25 meses de *vacatio legis* e 3 meses da entrada em vigor, totalizando 28 meses para as empresas se adequarem à legislação – 70% delas ainda não estavam cumprindo suas determinações. Dentre as principais incidências de descumprimento, figura a negativa de eliminar os dados pessoais arquivados. Apesar de algumas corporações assumirem o risco de eventuais sanções legais, importa atestar que a inobservância do direito à privacidade pode ter consequências prejudiciais para a respeitabilidade das empresas inadimplentes frente ao mercado, colocando-se em xeque sua reputação. Foi o que ocorreu com o Facebook, que, entre meados e o fim do ano de 2018, acumulou queda de 38% no valor de suas ações. (NOVAKOSKI; NASPOLINI, 2020, p. 9)

Para Frazão e Oliva (2019), considerando a noção de dados pessoais, mesmo as atividades mais básicas devem estar em conformidade com os regulamentos, uma vez que envolvem o armazenamento de informações que são legalmente protegidas até certo ponto. Isso inclui dados relativos a funcionários ou lista de clientes. Mesmo operações incidentais – como coleta e armazenamento de dados de condôminos, visitantes e funcionários – estão sujeitas à LGPD.

Na era moderna da revolução digital, o direito à privacidade é altamente valorizado do ponto de vista dos direitos da personalidade. A rápida recolha de informações pessoais, muitas vezes sem o conhecimento ou consentimento do proprietário, tornou este direito cada vez mais importante. No mundo de hoje, as informações pessoais são vulneráveis a ataques de terceiros, incluindo cibercriminosos. Isto é exemplificado pelas inúmeras violações de dados sofridas por utilizadores do *Facebook*, a mais significativa das quais ocorreu em março de 2018. Durante esta violação, a *Cambridge Analytica*, uma empresa de consultoria, recolheu indevidamente dados de 87 milhões de utilizadores da rede social (NOVAKOSKI; NASPOLINI, 2020).

Ainda nesse sentido:

> Um caso mais próximo ao consumidor brasileiro foi objeto de pesquisa feita pela Confederação Nacional dos Dirigentes Lojistas (CNDL), conjuntamente com o Serviço de Proteção ao Crédito (SPC), segundo a qual, de março de 2018 até março de 2019, quase 9 milhões de brasileiros foram vítimas de golpes, dos quais 41% tiveram seus cartões de crédito clonados após a efetivação de compras online, sendo esta a incidência mais corriqueira de golpes virtuais. (NOVAKOSKI; NASPOLINO, 2020, p. 10)

Como confere Novakoski e Naspolino (2020), sem dúvida, a questão da salvaguarda da privacidade dos dados tornou-se uma tendência global. Em inúmeras ocasiões, a preocupação com a segurança digital transcendeu até mesmo para o domínio da segurança física ou patrimonial. Por exemplo, os indivíduos que vivem em apartamentos ou condomínios horizontais podem não se preocupar em deixar as portas destrancadas quando saem, mas é altamente improvável que deixem os seus computadores desbloqueados ou os seus telemóveis sem um padrão de segurança quando não estão em uso.

2.3 O DIÁLOGO ENTRE A LGPD E O CDC: BREVE PARALELO ENTRE O CONSUMIDOR E O TITULAR DE DADOS

Como já foi referido, a comercialização dos dados pessoais tornou-se mais frequente na sociedade atual. Nesse sentido, fica evidente a associação entre a salvaguarda desses dados e as relações de consumo, que é regida pelo Código de Defesa do Consumidor no Brasil.

De acordo com Laura Mendes (2016), um serviço pode ser oferecido de forma gratuita ao consumidor, e mesmo assim, ainda ser considerado remunerado através de ganhos indiretos, seja através da comercialização de dados e informações, ou seja, por meio de publicidade.

No que diz respeito ao consumidor como titular dos dados pessoais, é importante reconhecer que este assume uma posição vulnerável; isso é explicitamente reconhecido pelo Código de Defesa do Consumidor, enquanto a Lei Geral de Proteção de Dados apoia tacitamente esta posição (MAIMONE, 2022).

Nesse sentido, dispõe o artigo 4º do CDC os princípios que norteiam as políticas de consumo brasileira, sendo algum deles:

> Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
> I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo;

> [...]
> III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;
> [...]
> V - incentivo à criação pelos fornecedores de meios eficientes de controle de qualidade e segurança de produtos e serviços, assim como de mecanismos alternativos de solução de conflitos de consumo;
> VI - coibição e repressão eficientes de todos os abusos praticados no mercado de consumo, inclusive a concorrência desleal e utilização indevida de inventos e criações industriais das marcas e nomes comerciais e signos distintivos, que possam causar prejuízos aos consumidores;
> [...] (BRASIL, 1990)

Dos princípios apresentados, destaca-se aqueles previstos nos incisos I, III, V e VI, de forma que os mesmos trazem pontos em comum com a LGDP, isto é: o reconhecimento da vulnerabilidade do consumidor; a proposta de equilíbrio entre a proteção ao consumidor e a necessidade de desenvolvimento econômico e tecnológico; o incentivo à criação de meios eficientes de controle de qualidade pelos fornecedores; e a coibição e repressão de abusos praticados no mercado (SANTOS, 2022).

Ao examinar o papel do consumidor no domínio dos meios digitais, verifica-se que este número já passou por digitalização. Por outras palavras, mesmo que a transação em si não seja realizada online, o processo de recolha de informações sobre produtos e serviços ainda ocorre em grande parte através da Internet. Com a implementação do Código Brasileiro de Defesa do Consumidor, a dinâmica das relações de consumo, bem como dos próprios consumidores, passou por um processo de amadurecimento (PINHEIRO, 2018).

Quanto ao princípio previsto no inciso I, faz-se paralelo do mesmo com os incisos II, VI e VII, do artigo 2º da LGDP, os quais indicam fundamentos de proteção aos direitos humanos e da personalidade do titular na relação de tratamento, bem como fazendo menção ao próprio direito à privacidade. Desta feita, denota-se que em ambos os casos, o reconhecimento de que a relação entre consumidor e fornecedor – paralelamente o titular e o agente de tratamento, na LGPD – é desigual, sendo imprescindível, portanto, maior proteção do primeiro frente ao segundo (SANTOS, 2022).

No que tange ao inciso III do CDC, este estabelece conexão com os incisos V e VI do dispositivo supracitado, da LGPD, dos quais apontam “o desenvolvimento

econômico, tecnológico, a inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor como fundamentos da Lei n. 13.709/18" (SANTOS, 2022, p. 24).

Ainda de acordo com Santos (2022), os incisos V e VI do artigo 4º do CDC tem clara relação com o inciso X do artigo 6º da LGPD, o qual designa como princípio desta lei a responsabilização e prestação de contas, segundo o qual o agente deve tomar medidas eficazes que demonstrem o cumprimento da proteção de dados pessoais e a eficácia dessas ações.

A correlação entre o rol de direitos dos internautas e o Direito do Consumidor é indiscutível, pois permite o reconhecimento da intersecção entre os direitos digitais e os direitos do consumidor. O inciso VIII do referido dispositivo faz referência específica ao Direito à Informação, protegido pelo Código de Defesa do Consumidor. Esta convergência significa a relação íntima entre os direitos digitais e os direitos consumistas (GUIMARÃES FILHO; FERNEDA, *et. al.*, 2020).

Outro ponto, este de suma relevância ao presente trabalho, diz respeito ao artigo 43 do CDC, o qual em seu caput, garante ao consumidor o direito de acesso às informações referentes a ele arquivadas pelas empresas, bem como suas respectivas fontes, devendo os dados armazenados serem objetivos, claros, verdadeiros e em fácil compreensão, bem como em formato acessível (SANTOS, 2022).

No mesmo sentido, a LGPD trata em seu artigo 18 garantias aquelas quais não somente as previstas no CDC, mas ampliando outra gama de direitos, como se percebe:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
> V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.
> § 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.
> § 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:
> I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou
> II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.
> § 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.
> § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
> § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.
> § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor. (BRASIL, 2018)

O disposto no art. 18 conferem ao titular dos dados direitos e proteções adicionais, além daqueles já estabelecidos no CDC. Estes direitos adicionais incluem a capacidade de tornar os dados anónimos, bloquear ou eliminar quaisquer dados desnecessários, excessivos ou não conformes com a lei, transferir dados para outro fornecedor de serviços ou produtos e solicitar informações sobre entidades com quem os dados foram partilhados, como bem como retirar o consentimento (SANTOS, 2022).

Além disso, o § 1º do art. 42 enfatiza a importância do titular dos dados e reconhece a sua vulnerabilidade em relação ao tratamento dos dados. A Lei atribui a responsabilidade pela reparação a todas as partes envolvidas na cadeia de tratamento de dados, refletindo o princípio da solidariedade, que também é uma pedra angular do direito do consumidor (SANTOS, 2022).

> Com efeito, diante de eventual dano causado pelo controlador ou operador de dados pessoais, a aludida lei estabelece em seu art. 42 a obrigação de repará-lo, seja ele patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais. Ainda, a preocupação do legislador estendeu-se no art. 45, o qual prevê que em caso de violação do direito do titular no âmbito das relações de consumo, aplicam-se as regras de responsabilidade previstas na legislação pertinente, isso porque as informações possuem valor econômico. (GUIMARÃES FILHO; FERNEDA, *et. al.*, 2020, p. 49)

Outro instituto paralelo em ambas leis, mas não menos importante, trata-se da evidente hipossuficiência do titular dos dados e a inversão da prova – artigos 6º, VIII, CDC e 42, §2º, LGPD. Nesta ocasião, o agente de tratamento é responsável por criar provas de que o tratamento irregular dos dados não afetou negativamente o titular dos dados, nos casos em que o titular dos dados não consiga produzir provas suficientes ou excessivamente zelosas dos seus dados.

> Conforme apontado, quando se compreende o tratamento dos dados dessa forma, ao consumidor é garantida a permissão ou não do uso, mas também a informação e barragem dos usos e finalidades do armazenamento dos seus dados. Dessa forma, a autonomia privada retoma a sua posição de importância, ao permitir que o consumidor tenha pleno conhecimento de como seus dados serão e estão sendo utilizado, o que necessariamente deve estar acompanhado de um livre esclarecimento. (GUIMARÃES FILHO; FERNEDA, *et. al.*, 2020, p. 50)

Como é perceptível, a evidente ligação entre os dois diplomas legais cria uma influência robusta do Código de Defesa do Consumidor como referência complementar na determinação da responsabilidade civil que se aplica à Lei Geral de Proteção de Dados. Disso isso, passa-se à análise da própria responsabilidade civil prevista na LGPD.

2.3.1 A responsabilidade civil na Lei Geral de Proteção de Dados

Inicialmente, é necessário destacar que antes mesmo de adentrar ao mérito da responsabilidade civil prevista na LGPD, é preciso que se destaque alguns conceitos importantes trazidos pela mesma lei, como é o caso do previsto ao artigo 5º, a respeito de titular, controlador, operador e encarregado:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (BRASIL, 2018)

Como ressaltado por Godinho e Queiroga Neto (*et. al.*, 2020), esses conceitos dispostos pela Lei Geral de Proteção de Dados dizem respeito ao detentor dos dados

os quais o controlador e o operador fazem uso, de mesmo modo, ao responsável por manter a comunicação entre o controlador e o operador, o titular e a autoridade nacional de proteção de dados.

De adoro com Cots e Oliveira (2019), a título de exemplo, expõe o seguinte caso: Para estabelecer uma plataforma virtual abrangente, recomenda-se envolver várias empresas, em que a empresa X seja fabricante de artigos esportivos em que deseja ter um site de venda de produtos. A empresa A deverá ser contratada para a infraestrutura da plataforma, a empresa B para pagamentos e gestão de contas, a empresa C para logística e gestão de estoques e a empresa D para marketing e publicidade. Quando é efetuada uma encomenda, a plataforma (empresa A) capta os dados pessoais do cliente, que são depois transmitidos ao processador de pagamentos (empresa B) e simultaneamente incorporados na base de dados da empresa Y. Os dados pessoais são então encaminhados à empresa D para entrega de produtos e atividades promocionais. No referido acordo, todas as empresas terão a possibilidade de acessar os dados dos usuários do site. Porém, apenas a Empresa X tem a responsabilidade de ser a controladora. As empresas A, B, C e D são consideradas operadoras e estão vinculadas às diretrizes estabelecidas pela Empresa X. O controlador é responsável pela tomada de decisões sobre o tratamento dos dados, enquanto os operadores desempenham funções específicas conforme instruções do o controlador dentro do processamento. Resumindo, o controlador gerencia o processamento enquanto os operadores seguem as instruções do controlador.

Nesse sentido, conforme preconiza o artigo 37 da LGPD, o controlador e operador são conhecidos como agentes de tratamento de dados pessoais, assumindo, portanto, determinadas obrigações ao lidar com os dados pessoais do cliente, cabendo-lhe manter registradas as operações de tratamento de dados pessoais em que foram realizadas, principalmente quanto se tratar de interesse legítimo (artigo 10, da LGPD) (GODINHO; QUEIROGA NETO, *et. al.*, 2020).

Na sequência, de acordo com o artigo 38, caso haja necessidade, a autoridade nacional poderá vir a pedir relatório de impacto da proteção de dados[2]:

[2] De acordo com o artigo 5º, VII, da LGDP, o relatório de impacto à proteção de dados pessoais diz respeito à documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais, os quais podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismo de mitigação de risco.

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. (BRASIL, 2018)

A disposição específica a que se refere estipula que o relatório deve incluir determinadas informações, o que implica que esta lista não é exaustiva, servindo antes como amostra. Com isso, é necessário que o relatório contenha essas informações, mesmo que não se limite exclusivamente a esses itens (GODINHO; QUEIROGA NETO, *et. al.*, 2020).

Dispostas as breves questões concernentes ao regime jurídico prevista na LGPD, destaca-se, a partir de então, a responsabilidade civil prevista em tal norma jurídica.

À vista disso, o artigo 42 da Lei Geral de Proteção de Dados determina que o controlador ou o operador que, em razão do exercício de atividades 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 (BRASIL, 2018). Além disso, o referido dispositivo, notadamente, encontra respaldo nas regras do Código Civil sobre a responsabilidade civil, particularmente o que preconiza o artigo 927, o qual estabelece que aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo (BRASIL, 2002).

Nessa toada, Márcio Cots e Ricardo Oliveira (2019), a respeito da conduta que determinado à reparação da ofensa nos termos da LGPD, destacam que o nexo causal do dano se encontra intrinsicamente ligado à violação da LGPD, de forma que, se não houver violação, não é possível a aplicação do artigo 42 da mesma lei, logo, não se configurando ato ilícito.

Demais disso, o artigo 42, em seu §1º, prevê também a responsabilidade solidária pelo operador e pelo controlado, no intuito de assegurar a efetiva indenização ao titular dos dados, caso o operador venha a descumprir com as obrigações da legislação de proteção de dados ou caso não houver seguido as instruções lícitas d controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos previstos no artigo 43 da mesma lei. De mesmo modo, os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados,

respondem solidariamente, salvo também nos casos previstos no artigo 43 (BRASIL, 2018).

Assim sendo, não apenas o controlador pode ter acesso aos dados cedidos pelo titular, mas estando o operador também obrigado a indenizar caso, eventualmente, vir a ocorrer algum dano.

Desta feita, de acordo com o artigo 43 da LGPD, os agentes de tratamento não serão responsabilizados em processos cíveis se puderem fornecer provas de que não trataram os dados, se o dano tiver sido causado exclusivamente pelo titular dos dados ou por terceiro, ou se os termos da LGPD não foram violados. A lei estabelece as condições de exclusão de responsabilidade nesta matéria, pelo que se presume que os agentes em causa são responsáveis pelos danos causados, independentemente de culpa ou dolo. Portanto, não há exigência de verificação de culpa ou dolo para apurar a responsabilidade pela reparação dos danos causados (GODINHO; QUEIROGA NETO, *et. al.*, 2020).

É fundamental observar o encarregado, mencionado anteriormente, uma vez que as disposições da LGPD não estabelecem nenhuma regulamentação específica quanto à sua responsabilização. O encarregado não responde perante o titular dos dados nem perante o agente nacional pelo tratamento dos dados efetuado pelo controlador, em que responsável pelo tratamento retém todo o poder de decisão sobre o tratamento dos dados, atuando o encarregado apenas como mediador para informar os terceiros interessados dessas decisões. Não obstante, o encarregado não pode fugir da responsabilidade por seus atos perante o controlador, ou na esfera criminal ou terceiros afetados, em razão de suas atribuições. Apesar desta omissão, ainda é possível exercer o direito de regresso. Embora o responsável não possua poder de decisão sobre o tratamento dos dados, poderá agir de má-fé e causar danos ao titular dos dados. Assim, devem cumprir o dever de reparação dos danos sofridos (COTS; OLIVEIRA, 2019).

Nessa esfera, em seu artigo 52, a LGPD prevê aplicação de sanções administrativas caso ocorra a violação aos termos de legislação:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último

> exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> [...]
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;
> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção. (BRASIL, 2018)

Com base na disposição dada, é notório que múltiplas sanções podem ser aplicadas, e um limite máximo de 50 milhões de reais é estabelecido para cada infração. Adicionalmente, a aplicação de sanções administrativas não exclui a responsabilidade civil, que exige a reparação de quaisquer danos causados às partes afetadas. Em última análise, o conceito de responsabilidade civil abrange uma variedade de funções (GODINHO; QUEIROGA NETO, *et. al.*, 2020).

Ainda para Godinho e Queiroga Neto (*et. al.*, 2020), de acordo com o ordenamento jurídico brasileiro, a utilização de determinadas funções não é consistentemente eficaz. Assim, a indenização concedida é muitas vezes desproporcional ao montante dos danos infligidos. Contudo, vale ressaltar que houve avanços em termos de sanções administrativas, uma vez que foi estabelecido um conjunto de critérios para determinar as penalidades adequadas. Com isso, espera-

se que a arbitragem de indenizações seja tratada com o mesmo nível de rigor que a lei determina para sanções administrativas.

2.3.1.1 Linhas interpretativas sobre a responsabilidade civil na LGPD

De acordo com Costa Neto (2018), para examinar completamente o campo da LGPD, é imperativo considerar as extensas progressões dentro do sistema de responsabilidade civil de direito privado. Especificamente, é fundamental reconhecer a importância e o peso dos princípios e normas delineados no Código Civil e no CDC. Essas regulamentações, por seu valor essencial e posicionamento estratégico no ordenamento jurídico, não podem ser desconsideradas na análise da disciplina LGPD.

Além do mais, os institutos de direito privado estão sujeitos a contínua construção e reconstrução. A sua interpretação é constantemente moldada para satisfazer as necessidades empíricas de uma sociedade em constante mudança, complexa, globalizada e altamente povoada. Este processo garante que o caráter ético, que é parte integrante do comportamento humano e das interações sociais, permaneça prestigiado (FACHIN, 1998).

Levado em conta a presente pauta, retomando a análise da LGPD, destaca-se que a partir dos artigos 42 a 45 da LGPD, surgiram duas linhas de interpretação sobre a natureza da responsabilidade civil dos agentes de tratamento de dados pessoais: parte da doutrina pensa que a responsabilidade civil nesses casos seria subjetiva, ao passo em que a posição divergente entende que a LGPD teria se filiado ao sistema de risco, ou seja, objetiva (NOVAKOSKI; NASPOLINI, 2020). Todavia, ambas as correntes possuem a premissa comum de que a LGPD sofre com uma grave “inexatidão terminológica” (TASSO, 2020, p. 104), visto a ausência de clareza suficiente no enunciado do artigo 42 da mesma lei.

À luz deste facto indiscutível, o direito moderno estabeleceu regulamentos para a responsabilidade civil com a intenção de erradicar o conceito de “custo social” de não resolver danos injustos. Este conceito mina a estabilidade jurídica e é uma fonte de injustiça incompatível com inúmeras teorias jurídicas utilizadas no direito privado, incluindo a análise económica do direito e a constitucionalização do direito civil (SCHREIBER, 2009).

De acordo com Novakoski e Naspolini, o artigo 42 da LGPD não pode ser interpretado no sentido privado como sugerem os defensores da teoria subjetivista, visto que:

> O art. 42 da LGPD reconhece, naquela expressão e ainda que de forma implícita, que a atividade de tratamento de dados pessoais envolve risco potenciais, os quais, registre-se, são explicitamente admitidos, em maior ou menor grau, em diversos outros dispositivos da norma (art. 5º, XVII; art. 38, § único; art. 44, II; art. 48, caput c/c § 1º, IV; art. 50, caput c/c § 1º; art. 55, XIII). Sendo o Código Civil a fonte última irradiadora de princípios e regras de direito privado, a interpretação do art. 42 da LGPD deve ser realizada de forma coerente e sistemática ao disposto no art. 927, § único, do Código Civil, que adotou a teoria da responsabilidade objetiva fundada no risco da atividade exercida pelo agente da atividade potencialmente lesiva, eliminando a situação de socialização do prejuízo na qual a vítima era forçada a suportar o dano em razão da dificuldade (prática, financeira, probatória) de provar a culpa. (NOVAKOSKI; NASPOLINI, 2020, p. 167-168)

De acordo com Barreto Júnior e Cavalcanti (*et. al.*, 2018), a criação de um sistema de proteção de dados pessoais pela LGPD ficaria sem sentido se a implementação do sistema fosse ineficaz ou funcionalmente inútil. Tal resultado só levaria à violação contínua do direito de um indivíduo à privacidade pessoal.

Nessa toada, reflete ainda o seguinte:

> Aponta-se ainda que o art. 43 da LGPD evidenciaria que a responsabilidade civil prevista na norma teria cunho subjetivo por envolveria a necessidade de demonstração de culpa do agente de tratamento de dados pessoais, o que não é verdadeiro. As hipóteses descritas nos incisos I a III do art. 43 da LGPD não guardam qualquer vínculo com a exigência de culpa, mas se relacionam a hipóteses de ruptura do nexo de causalidade. O art. 44 da LGPD, por sua vez, impõe padrões comportamentais ao agente de tratamento de dados pessoais, ou seja, estabelece deveres de resultado (e não se simples diligência), cujo descumprimento implica, per se, a responsabilização do causador do dano independentemente de prova de culpa. Um óbice usualmente levantado pelos defensores da tese da responsabilidade civil subjetiva da LGPD se escorra no fato de que a adoção da teoria do risco da atividade inibiria a competição e o desenvolvimento de novas tecnologias. A afirmação, que parece ter um tom de novidade, foi exaustivamente examinada quando da promulgação do CDC e do próprio Código Civil em vigor; ao contrário dos partidários da tese, a imputação da responsabilidade objetiva nas hipóteses estabelecidas nestes diplomas não inibiu a inovação e o desenvolvimento de novas tecnologias, mas certamente as tornou mais seguras e impediu a socialização dos riscos de desenvolvimento (e dos danos a eles relacionados), imputando o dever de reparar àquele que exerce a atividade e assegurando a efetiva proteção das vítimas de danos injustos, a ponto de não surpreender a descoberta (ou desenvolvimento) de um ―princípio da proteção da vítima‖ na interpretação do sistema civil-constitucional vigente. (NOVAKOSKI; NASPOLINI, 2020, p. 168-169)

De acordo como destaca Maria Celina Bodin de Moraes (2019), a noção de “responsabilidade” refere-se a uma nova abordagem à responsabilidade, muitas vezes referida como responsabilidade “ativa” ou “proativa”. Isto fica evidente na Secção X

do Artigo 6, onde se estipula que as empresas devem não só cumprir os requisitos legais, mas também demonstrar que tomaram medidas eficazes para garantir o cumprimento das normas de proteção de dados pessoais. Na verdade, devem ir além, provando que as suas medidas são eficazes na prevenção de qualquer dano potencial. Assim, evitar violações legais já não é suficiente; agora é necessário prevenir proativamente a ocorrência de qualquer dano.

À luz destas premissas, parece ilógico que a legislação implemente mecanismos de responsabilidade preventiva que visam impedir a ocorrência de danos, ao mesmo tempo que submete a compensação de danos resultantes de violações de dados pessoais - um direito humano fundamental - ao domínio subjetivo da responsabilidade civil. Esta abordagem não é apenas contraditória, mas também apresenta dificuldades inerentes, como evidenciado pelo debate histórico entre Saleilles e Josserand no final do século XIX, que acabou por resultar na transformação da responsabilidade civil aquiliana de subjetiva para objetiva através de mecanismos como a culpa presumida e teorias de risco (NOVAKOSKI; NASPOLINI, 2020).

2.3.2 O ilícito lucrativo no tratamento de dados pessoais e o não atendimento dos direitos do titular

De acordo com Nelson Rosenvald (2019), os ilícitos lucrativos são aqueles que produzem resultados lucrativos para os perpetradores, proporcionando ganhos financeiros que compensem a ilegalidade das ações. No que diz respeito ao tratamento de dados pessoais, conforme mencionado anteriormente, a monetização desta informação pode resultar em lucros substanciais que tornam a prática valiosa para quem a realiza.

De acordo com Maimone (2022), para que o sistema jurídico brasileiro possa enfrentar eficazmente esta questão, é necessário que haja um consenso sobre dois aspectos cruciais. Em primeiro lugar, o reconhecimento de que existe efetivamente um problema - especificamente, que o perpetrador não pode beneficiar das suas ações ilícitas. Em segundo lugar, o entendimento de que é imperativo exigir o reembolso de quaisquer lucros obtidos com essas ações ao legítimo proprietário.

O desafio que se coloca é a reparação dos danos causados ao titular dos dados nos casos em que o tratamento irregular beneficia quem o pratica. A dificuldade particular desta questão é que, embora haja uma violação de um direito fundamental,

o que aumenta a necessidade de punição adequada, o desconhecimento do autor do delito torna difícil penalizar o responsável (MAIMONE, 2022).

Santana sustenta que o conceito de dano moral não depende necessariamente do sofrimento da vítima, mas sim da violação ou negação de um direito fundamental da personalidade. Consequentemente, embora a avaliação do dano possa servir para quantificar a indenização, não pode servir como único critério para determinar a sua existência (MAIMONE, 2022).

Nesse sentido, em análise à decisão monocrática do Superior Tribunal de Justiça em Recurso Especial (SP 2019/0234788-6), de relatoria do Ministro Luís Felipe Salomão entendeu pela condenação ao réu sobre a reparação de danos morais causados pelo dano, na tentativa de combater a prática ao utilizar a coibição do ilícito lucrativo, como forma de determinação à indenização.

A conversa em torno desta questão serve para sublinhar que, embora o sistema de responsabilidade civil aplicável aos incidentes que envolvam tratamento de dados pessoais seja objetivo, a determinação do montante da indenização para casos de ganhos ilícitos exige mais do que apenas avaliar a extensão dos danos da vítima. É importante levar em conta também o lucro obtido pela empresa responsável pela infração, pois a aplicação da responsabilidade civil tem caráter punitivo (SANTOS, 2022).

3 CONSIDERAÇÕES GERAIS

O conceito de privacidade abrange não apenas o direito à solidão, mas também salvaguarda a capacidade dos indivíduos de limitar o acesso de terceiros a informações que dizem respeito exclusivamente à sua vida pessoal. A progressão das leis relativas à proteção de dados ao longo da história é uma prova da correlação entre o direito à privacidade e a sua salvaguarda. É por isso que é considerado um direito fundamental.

A evolução legislativa foi subdivida em quatro gerações: i) na década de 70, com a preocupação pela administração pública sobre as bases de dados e poder, passaram a regulamentar através da necessidade de permissão por escrito; ii) regulamentações de proteção de dados pessoais e privacidade com preocupação voltada ao procedimento; iii) na década de 80 surgiu a autonomia informacional, onde há participação de pessoas nos tratamentos de dados; iv) incorporação dos dados sensíveis, positivado pela Lei do Cadastro Positivo (Lei n. 12.414/11).

Após tais gerações, no ano de 2018, restou criada a Lei Geral de Proteção de Dados, onde a privacidade adquiriu novo significado com os avanços tecnológicos. Nesse sentido, as redes sociais são uma forma única de sociedades virtuais, onde os indivíduos interagem utilizando as suas informações pessoais.

No entanto, os avanços tecnológicos podem muitas vezes entrar em conflito com o direito fundamental à privacidade. Estes avanços podem expandir drasticamente a recolha de dados, exigindo que os indivíduos mantenham o controle e a consciência das suas preferências, hábitos e interesses. No mundo de hoje, onde a maioria das informações pessoais é digitalizada, certas informações que deveriam permanecer confidenciais podem tornar-se perigosas. Assim, salvaguardar a privacidade online torna-se um bem valioso, mas que requer proteção.

Neste quadro específico, a privacidade dos cidadãos é violada e os seus direitos individuais são transgredidos. A intimidade foi reduzida a uma mera mercadoria numa sociedade que coloca grande ênfase no consumismo, e tornou-se uma forma omnipresente de moeda, com uma multidão de indivíduos dispostos a pagar pela sua disseminação.

Diante desse cenário, no ano de 2014, nasceu com a aprovação do Congresso Nacional, no dia 25 de março, a Lei n. 12.965/2014, conhecida popularmente como Marco Civil da Internet, com o objetivo de finalmente regulamentar o uso da Internet

no Brasil. Em paralelo ao Marco Civil da Internet, surgiu a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), vindo a disciplinar o uso da internet no Brasil, justamente para quem faz uso de tal rede, vindo a delimitar, inclusive, a própria atuação do Estado nesse âmbito.

As regulamentações abrangidas pela Lei Geral de Proteção de Dados estão estruturadas para proteger os direitos fundamentais à privacidade. Uma dessas disposições requer consentimento informado. Isto implica que a recolha de dados deve ser conduzida de forma transparente e que os indivíduos devem ser informados sobre como os seus dados serão utilizados antes de os fornecerem.

Com a criação da LGPD, restou estabelecida também a ANPD, órgão este que visa maior sensibilidade à proteção de dados, incluindo o monitoramento das regulamentações previstas na legislação, bem como sendo responsável por criar padrões de segurança para armazenamento de dados e avaliar a gravidade de quaisquer violações de segurança de dados que ocorram.

Como já foi referido, a comercialização dos dados pessoais tornou-se mais frequente na sociedade atual. Nesse sentido, fica evidente a associação entre a salvaguarda desses dados e as relações de consumo, que é regida pelo Código de Defesa do Consumidor no Brasil. É fundamental compreender que os consumidores que detêm dados pessoais estão em posição vulnerável, conforme destacado explicitamente no Código de Defesa do Consumidor e amparado implicitamente na Lei Geral de Proteção de Dados.

É cediço que os artigos 18, 42 e 43 faz intenso paralelo a determinados pontos ao CDC, isto é, ao tratamento da responsabilidade civil em ambas leis. Como é perceptível, a evidente ligação entre os dois diplomas legais cria uma influência robusta do Código de Defesa do Consumidor como referência complementar na determinação da responsabilidade civil que se aplica à Lei Geral de Proteção de Dados.

O artigo 42 da Lei Geral de Proteção de Dados estabelece que o operador ou controlador que causar dano à propriedade, à moral ou às pessoas, bem como dano coletivo a terceiros em decorrência de atividades de tratamento de dados pessoais, e em violação às leis de proteção de dados pessoais, deve reparar o dano. Esta disposição é apoiada pelas regras do Código Civil sobre responsabilidade civil, especificamente o artigo 927, que determina que qualquer pessoa que cause

ilegalmente danos a outra pessoa, conforme definido nos artigos 186 e 187, deve assumir a responsabilidade pelos seus atos e reparar os danos causados.

O artigo 43 da LGPD determina que os agentes de tratamento não serão responsabilizados em processos cíveis se puderem provar que não trataram os dados, se o dano tiver sido causado exclusivamente pelo titular dos dados ou por terceiro, ou se os termos do A LGPD não foi violada. A lei define os pré-requisitos para a absolvição da responsabilidade, o que implica que os agentes em causa sejam inicialmente considerados responsáveis pelos danos causados, independentemente de qualquer culpa ou dolo. Como resultado, não há necessidade de investigação de culpabilidade ou intenção para estabelecer responsabilidade pela reparação de danos.

Levado em conta a presente pauta, retomando a análise da LGPD, destaca-se que a partir dos artigos 42 a 45 da LGPD, surgiram duas linhas de interpretação sobre a natureza da responsabilidade civil dos agentes de tratamento de dados pessoais: parte da doutrina pensa que a responsabilidade civil nesses casos seria subjetiva, ao passo em que a posição divergente entende que a LGPD teria se filiado ao sistema de risco, ou seja, objetiva.

Todavia, o STJ, no julgamento do Recurso Especial (SP 2019/0234788-6) entendeu pela condenação ao réu sobre a reparação de danos morais causados pelo dano, na tentativa de combater a prática ao utilizar a coibição do ilícito lucrativo, como forma de determinação à indenização.

O discurso sobre esta matéria sublinha que, embora o sistema de responsabilidade civil relativo aos incidentes que envolvam o tratamento de dados pessoais permaneça imparcial, a determinação da indenização para os casos de ganhos ilícitos exige mais do que apenas avaliar a extensão do dano sofrido pela parte lesada. É fundamental considerar os lucros auferidos pela empresa responsável pela infração, pois a execução da responsabilidade civil funciona de forma punitiva.

4 CONCLUSÃO

Nos dois grandes momentos em que é exposto o tema central deste trabalho, houve ocasião para uma exposição inicial que ilustrou como a introdução da LGPD no Brasil foi resultado direto de um movimento. Este movimento teve como objetivo reconhecer a importância da salvaguarda dos dados pessoais como um campo jurídico independente, o que por sua vez exigiu a criação de legislação pertinente para regulamentá-los.

Observou-se ao longo do trabalho que o aumento da importância econômica dos dados pessoais para a sociedade moderna é a causa profunda de uma tendência discernível. Este fenómeno é acompanhado pelo aumento das atividades de tratamento, que passaram a ser objeto de escrutínio devido a possíveis violações dos interesses individuais dos titulares dos dados, bem como por problemas políticos que podem surgir do potencial destes instrumentos para influenciar e moldar comportamentos, apesar de a capacidade dos alvos de exercerem autodeterminação.

O Poder Legislativo aprovou a LGPD como legislação especial neste contexto específico. O objetivo principal da LGPD é fornecer ampla proteção aos dados pessoais dos indivíduos. Esta legislação aplica-se também aos atos de tratamento que ocorram no contexto das relações de consumo. Portanto, requer um exercício hermenêutico compatível e harmonização com o CDC.

A respeito da responsabilidade civil, mister que a mesma se baseia nos conceitos de equilíbrio na distribuição dos riscos, no tratamento justo das vítimas e dos perpetradores e no princípio da solidariedade social. Preocupa-se principalmente em remediar os danos injustos infligidos à vítima, um princípio crucial na sociedade atual, onde a informação e o risco são altamente valorizados.

A partir desse ponto, retoma-se o problema de pesquisa do presente trabalho, onde se discute a responsabilidade civil a esses sujeitos, buscando saber se na modalidade objetiva ou subjetiva, bem como quais as consequências de sua incidência.

Para galgar a presente resposta, destaca-se que ao discutir a responsabilidade civil, é fundamental levar em consideração as regulamentações previstas tanto no CDC quanto na LGPD. A combinação destas regras resulta numa expansão do escudo de proteção conferido pelo CDC, aumentando assim as responsabilidades dos fornecedores em relação à boa-fé contratual, precaução e divulgação.

Além de suas responsabilidades gerais, a LGPD está comprometida com a regulamentação abrangente de assuntos que se relacionem especificamente com a salvaguarda dos dados pessoais dos consumidores. Isto inclui alargar o alcance da responsabilidade civil aos fornecedores, bem como facilitar a identificação de deveres de compensação nos casos em que os operadores de dados que não são classificados como fornecedores ao abrigo do CDC cometem atos ilícitos que infringem os direitos de proteção de dados pessoais.

Apesar dos argumentos convincentes, a obrigação de fornecer provas de culpabilidade como meio de definir a obrigação de reparar as violações dos princípios e regulamentos delineados na LGPD desconsidera a consistência lógica intrínseca do sistema de responsabilidade civil do Brasil, bem como a evolução histórica da a este quadro ao longo do século XX, que se afastou do conceito de culpabilidade para o dos perigos potenciais das atividades.

O tratamento de dados pessoais é uma prática que acarreta riscos inerentes, pois envolve o direito fundamental à privacidade. Esses riscos são abordados pela LGPD, que defende uma interpretação que abarca a teoria da responsabilidade civil objetiva. Essa teoria sustenta que quem descumprir as obrigações previstas em lei será responsabilizado pelos danos resultantes, a menos que consiga comprovar que o nexo de causalidade foi rompido nos termos da LGPD.

Doravante, pode-se deduzir que o conceito de comunicação entre CDC e LGPD amplia a compreensão e amplia a salvaguarda de um indivíduo em seu estado suscetível quando se trata da manipulação de suas informações pessoais por um fornecedor, que agora funciona como processador de dados.

Em conclusão, é vital reconhecer que a investigação realizada não se restringe às conclusões apresentadas, mas sim a um ponto de partida sujeito a possíveis modificações na sequência de debates políticos e jurídicos. Não pretende ser uma solução abrangente, mas sim uma contemplação de aspectos específicos da mudança que podem ter impacto sobre os indivíduos que utilizam a tecnologia e podem ser vulneráveis a fraudes financeiras. No entanto, espera-se que a Autoridade Nacional de Proteção de Dados (ANPD) estabeleça regulamentos para normas técnicas até 2024, o que sem dúvida desencadeará novas disputas políticas e jurídicas.

REFERÊNCIAS

ASSIS, José Francisco de. **Direito à privacidade no uso da internet: omissão da legislação vigente e violação ao princípio fundamental da privacidade**. In: E-Gov. Disponível em: <https://encurtador.com.br/agNPS>. Acesso em: 26 set 2023.

BARRETO JUNIOR, Irineu Francisco; NASPOLINI, Samyra Haydêe Dal Farra. **Proteção de informações no mundo virtual: a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais**. Cadernos Adenauer: Proteção de dados pessoais: privacidade versus avanço tecnológico, ano XX, n. 3. Rio de Janeiro: Fundação Konrad Adenauer, 2019.

_____; WANDERLEY, Ana Elizabeth Lapa; LEITE, Beatriz Salles Ferreira. **Sistemas de responsabilidade civil dos provedores de aplicações da internet por ato de terceiros: Brasil, União Europeia e Estados Unidos da América**. In: Revista Eletrônica do Curso de Direito da UFSM, v. 13, n. 2, Santa Maria, 2018.

BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 2 ed. São Paulo, 2000.

BRASIL. **Constituição Federal de 1988**. Brasília: Senado Federal, 1988. Disponível em: <https://encurtador.com.br/tAHJ2>. Acesso em: 27 set. 2023.

_____. **Lei 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da República Federativa do Brasil. Brasília, DF: 10 jan 2002. Disponível em: < https://encurtador.com.br/aoKM6>. Acesso em: 27 set. 2023.

_____. **Lei. 13.709, de 14 de agosto de 2018**. Diário Oficial da República Federativa do Brasil. Brasília, DF: 14 ago 2018. Disponível em: <https://encurtador.com.br/iGHLZ>. Acesso em: 27 set. 2023.

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. 7 ed. Coimbra: Almedina. 2003

CAPURRO, Rafael; ELDRED, Michael; NAGEL, Daniel. It and privacy from an ethical perspective digital whoness: identity, privacy and freedom in the cyberworld. In: BUCHMANN, Johannes. **Internet Privacy: a multidisciplinary analysis**. München: Acatech, 2012. [tradução livre].

COOKIES, WEB BEACONS E TECNOLOGIAS SEMELHANTES. In: **Sumup**. 2020. Disponível em: <https://www.sumup.com/pt-br/transparencia/cookies/> Acesso em: 29 set. 2023.

COSTA NETO, Moacyr da. **A autonomia privada e a prevalência do negociado**. In: Revista Univap, v. 24, n. 45, edição especial. São José dos Campos, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Comentada**. 2 ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2019.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 30 ed. Rio de Janeiro: Forense, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FACHIN, Luiz Edson. Virada de Copérnico: um convite à reflexão sobre o direito civil brasileiro contemporâneo. In: FACHIN, Luiz Edson (coord.). **Repensando fundamentos do direito civil brasileiro contemporâneo**. Rio de Janeiro: Renovar, 1998.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson; BRAGA NETTO, Felipe Peixoto. **Curso de Direito Civil: Responsabilidade Civil**. 5 ed. Salvador: Juspodivm, 2018.

FERREIRA, Rubens da Silva. **A sociedade de vigilância como sociedade de disciplina, vigilância e controle**. In: Información, cultura y sociedad. Buenos Aires, n. 31, 2014.

FRAZÃO, Ana; OLIVEA, Milena Donato; ABÍLIO, Vivianne da Silveira. *Compliance* de danos pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.). **A Lei Geral de Proteção de dados pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.

FUGAZZA, Grace Quaresma; SALDANHA, Gustavo Silva. **Privacidade, ética e informação: uma reflexão filosófica sobre os dilemas no contexto das redes sociais**. Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, v. 22, n. 50, p. 91-101, 2017.

GODINHO, Adriano Marteleto; QUEIROGA NETO, Genésio Rodrigues de; TOLÊDO, Rita de Cássia de Morais. **A responsabilidade civil pela violação a dados pessoais**. In: Revista IBERC, v. 3, n. 1, p. 1-23, 2020.

GRAIEB, Carlos. **Quando não há mais segredos**. Revista Veja, n. 32, p. 81, 2009.

GUIMARÃES FILHO, Pedro Andrade; FERNEDA, Ariê Scherreier; FERRAZ, Miriam Olivia Knopik. **A proteção de dados e a defesa do consumidor: autonomia privada frente à privacidade**. Revista Meritum, Belo Horizonte, vol. 15, n. 2, p. 38-52, 2020.

KELSEN, Hans. **Teoria pura do direito**. 6 ed. São Paulo: Martins Fontes, 1998.

LIMBERGER, Têmis. **Cibertransparência informação pública em rede: a virtualidade e suas repercussões na realidade**. Porto Alegre: Livraria do Advogado, 2016.

LISBOA, Roberto Senise. **Boa-fé e confiança na Lei Geral de Proteção de Dados brasileira**. In: Revista do Advogado, n. 144, São Paulo, p. 6-11, 2019.

MACEIRA, Irma Pereira. **A proteção do direito à privacidade familiar na internet**. Tese (Doutorado em Ciências Sociais). Pontifícia Universidade Católica de São Paulo. São Paulo, 2012.

MAIMONE, Flávio Henrique Caetano de Paula. **Responsabilidade civil na LGPD: efetividade na proteção de dados pessoais**. Indaiatuba: Editora Foco, 2022.

MARQUES, Andréa Neves Gonzaga. **Direito à intimidade e privacidade**. In: Jus TJDFT. 2008. Disponível em: <https://encurtador.com.br/iD059>. Acesso em: 15 out 2023.

MATTOS FILHO, VEIGA FILHO, MARREY JR. E QUIROGA ADVOGADOS. **Guia para a Lei Geral de Proteção de Dados**. São Paulo. 2018. Disponível em: <https://encurtador.com.br/iyGJ1>. Acesso em: 15 out 2023.

MENDES, Hugo Rocha. A proteção de dados pessoais: diálogos entre o CDC e a Lei Geral de Proteção de Dados. SOARES, Márcia Santana del et al. (Coord.). **Estudos sobre o Direito Civil**. Goiânia: UNIGOIÁS, 2023.

MENDES, Laura Schertel. **O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor**. In: Revista de Direito do Consumidor, v. 106, 2016.

_____. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MIRAGEM, Bruno. **Curso de direito do consumidor**. 4 ed. São Paulo: Editora Revista dos Tribunais, 2013.

MONTEIRO, Renato Leite. Da Proteção aos Registros, aos dados pessoais e às comunicações privadas. In: MASSO, Fabiano del et al. (Coord.). **Marco Civil da Internet**. São Paulo: Revista dos Tribunais, 2014.

MORAES, Maria Celina Bodin de. **LGPD: um novo regime de responsabilização civil dito proativo**. Revista Civilistica, ano 8, n. 3, Rio de Janeiro, 2019

NETO VASCONCELOS, Waldomiro de. **Privacidade e redes sociais: uma análise de adequação da legislação atual frente ao dinamismo das relações cibernéticas**. Trabalho de Conclusão de Curso (Faculdade de Direito do Recife) Universidade Federal de Pernambuco. Recife, 2022.

NOVAKOSKI, André Luis Mota; NASPOLINI, Samyra Haydêe Dal Farra. **Responsabilidade civil na LGPD: problemas e soluções**. In: CONPEDI LAW REVIEW, v. 6, n. 1, p. 158-174, 2020.

PAESANI, Liliana Minardi. **Direito e internet: liberdade de informação, privacidade e responsabilidade civil**. 7 ed. São Paulo: Atlas, 2014.

PARISER, Eli. **O filtro invisível: o que a internet está escondendo de você**. Rio de Janeiro: Zahar, 2012.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4 ed. São Paulo: SaraivaJur, 2018.

ROSENVALD, Nelson. **A responsabilidade civil pelo ilícito lucrativo**. Salvador: Editora JusPodivm, 2019.

SANTOS, Gabriel Cardoso dos. **Regime de responsabilidade civil aplicável ao tratamento de dados pessoais: uma análise sob a ótica da Lei Geral de Proteção de Dados**. Trabalho de Conclusão de Curso. (Centro de Ciências Sociais Aplicadas) Universidade Federal do Rio Grande do Norte. Natal, 2022.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil: da erosão dos filtros à diluição dos danos**. 2 ed. São Paulo: Atlas, 2009.

SLAVOV, BÁRBARA. **Os limites do uso do desenvolvimento tecnológico frente aos direitos de privacidade**. Dissertação (Mestrado em Direito). Centro Universitário Fieo, Osasco, 2009.

TASSO, Fernando Antônio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. In: Cadernos Jurídicos: Direito Digital e proteção de dados pessoais. São Paulo, ano 21, n. 53, São Paulo, 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. In: Revista Civilistica, ano 9, n. 1, Rio de Janeiro, p. 1-38, 2020.

VIEIRA, Waleska Duque Estada. **A privacidade no ambiente cibernético: direito fundamental do usuário**. In: Revista da ESMESC, v. 24, n. 30, p. 197-217, 2017.