FUNDAÇÃO EDUCACIONAL MACHADO DE ASSIS
FACULDADES INTEGRADAS MACHADO DE ASSIS
CURSO DE DIREITO

LEONARDO PIES BERGMANN

A (IN)EFICÁCIA DA RESPONSABILIZAÇÃO CIVIL DAS REDES SOCIAIS FRENTE AO VAZAMENTO DE DADOS PESSOAIS SENSÍVEIS

TRABALHO DE CURSO

Santa Rosa
2024

LEONARDO PIES BERGMANN

A (IN)EFICÁCIA DA RESPONSABILIZAÇÃO CIVIL DAS REDES SOCIAIS FRENTE AO VAZAMENTO DE DADOS PESSOAIS SENSÍVEIS
TRABALHO DE CURSO

Monografia apresentada às Faculdades Integradas Machado de Assis, como requisito parcial para obtenção do Título de Bacharel em Direito.

Orientador: Ms. Gabriel Henrique Hartmann

Santa Rosa
2024

LEONARDO PIES BERGMANN

A (IN)EFICÁCIA DA RESPONSABILIZAÇÃO CIVIL DAS REDES SOCIAIS FRENTE AO VAZAMENTO DE DADOS PESSOAIS SENSÍVEIS
TRABALHO DE CURSO

Monografia apresentada às Faculdades Integradas Machado de Assis, como requisito parcial para obtenção do Título de Bacharel em Direito.

Banca Examinadora

Prof. Ms. Gabriel Henrique Hartmann

Prof.ª Ms. Franciele Seger

Prof.ª Ms. Rosmeri Radke

Santa Rosa, 04 de julho de 2024.

DEDICATÓRIA

Dedico esta monografia aos meus pais, Arlindo Bergmann e Odete Catarina Pies, visto que minha oportunidade de estudo é fruto da dedicação deles.

AGRADECIMENTOS

Agradeço aos meus amigos, que contribuíram com comentários construtivos para a minha pesquisa.

Agradeço ao meu orientador, Gabriel H. Hartmann, que desempenhou um trabalho ímpar ao nortear a minha pesquisa.

Agradeço, especialmente, a Juíza de Direito, Miroslava do Carmo Mendonça, que oportunizou o meu contato com a profissão que almejo e proporcionou-me inúmeros aprendizados.

Mas, senhores, os que madrugam no ler, convém madrugarem também no pensar. Vulgar é o ler, raro o refletir. O saber não está na ciência alheia, que se absorve, mas principalmente, nas ideias próprias, que se geram dos conhecimentos absorvidos, mediante a transmutação, por que passam, no espírito que os assimila. Um sabedor não é armário de sabedoria armazenada, mas transformador reflexivo de aquisições digeridas.

Rui Barbosa, na obra Oração aos Moços.

RESUMO

Esta pesquisa tem como tema a responsabilização civil das redes sociais na proteção de dados pessoais. Tem como delimitação temática a busca por discorrer acerca da responsabilização civil das empresas administradoras das redes sociais, especialmente no cenário jurídico brasileiro. Com fins sociológicos e jurídicos, analisa-se a jurisprudência do STJ, entre os anos de 2019 e 2024, no que concerne a responsabilização civil das redes sociais. O problema norteador é: como a responsabilização civil das redes sociais frente ao vazamento de dados pessoais sensíveis poderá dirimir os danos aos seus usuários? Para isto, como objetivo geral analisa-se os impactos frente ao vazamento de dados pessoais sensíveis e a responsabilização civil das empresas administradoras das redes sociais. A relevância da pesquisa se encontra na era da informatização, onde o produto mais valioso não é algo físico, mas sim o digital e, por isso, é de grande importância compreender a responsabilização das empresas que realizam o tratamento de dados pessoais, visto estas informações possuem uma capacidade de dano muito grande aos indivíduos titulares das informações. Os principais autores são: Manuel Castells, Yuval Harari, Zygmunt Bauman, Danilo Doneda, Chiara Spadaccini de Teffé, Bruno Miragem, Bruno Bioni e Glenda Gondim. A pesquisa, em sua categorização, tem natureza teórica, com tratamento de dados de forma qualitativa, pois estuda a aplicação de uma hipótese pré-definida. A conduta a ser utilizada para a obtenção de fontes para a realização do estudo será através de pesquisas bibliográficas e documentais. A finalidade do trabalho de pesquisa será descritiva, pois após realizar as pesquisas, será descrito o que foi estudado. O plano de produção de dados é a partir de documentação indireta. Esta forma prática de obtenção de dados consiste em um levantamento de dados feito através de pesquisas documentais já realizadas, ou seja, livros e artigos científicos. Os dados obtidos através da pesquisa são analisados e interpretados utilizando o método hipotético-dedutivo, haja vista que há hipóteses preestabelecidas para a solução do problema apresentado. Destaca-se que, após a introdução, a pesquisa está dividida em três capítulos. O primeiro capítulo aborda o desenvolvimento do *homo sapiens* e o paradoxal desenvolvimento das redes sociais, onde é estudado o surgimento das redes sociais que presenciamos atualmente e os impactos e benefícios proporcionados por estas. No segundo capítulo há o estudo dos marcos legislativos que tratam da proteção de dados pessoais, nacionais e internacionais, e explana-se o que são os dados pessoais e a importância do tratamento correto deles. Por fim, o terceiro capítulo apresenta-se um panorama acerca da responsabilidade civil na Lei Geral de Proteção de Dados e, após, exploram-se os aspectos principais quanto à responsabilidade de tratamento correto de dados e quanto à dificuldade de quantificação do valor da indenização. Em seguida, apresenta-se uma pesquisa jurisprudencial, que tem o objetivo de abordar a responsabilização civil de empresas pelo vazamento de dados pessoais. As principais conclusões buscadas são atinentes à eficácia, ou não, da responsabilidade civil pelo vazamento de dados pessoais.

Palavras-chave: Rede social - Dados Pessoais Sensíveis - Responsabilidade Civil.

ABSTRACT

This research focuses on the civil liability of social networks in the protection of personal data. Its thematic delimitation is the search for disagreement about the civil liability of companies that manage social networks, especially in the Brazilian legal scenario. For sociological and legal purposes, the jurisdiction of the STJ is analyzed, between the years 2019 and 2024, with regard to the civil liability of social networks. The guiding problem is: how can the civil liability of social networks in the face of the leakage of sensitive personal data be able to resolve the damage to their users? To this end, the general objective is to analyze the impacts of personal data leaks and the civil liability of administrators of social media companies. The relevance of the research lies in the era of computerization, where the most important product is not something physical, but digital and, therefore, it is of great importance to understand the responsibility of companies that process personal data, given this information have a very high capacity for harm to the individuals holding the information. The main authors are: Manuel Castells, Yuval Harari, Zygmunt Bauman, Danilo Doneda, Chiara Spadaccini de Teffé, Bruno Miragem, Bruno Bioni and Glenda Gondim. The research, in its categorization, is theoretical in nature, with data processing in a qualitative way, as it studies the application of a pre-defined hypothesis. The conduct to be used to obtain sources to carry out the study will be through bibliographic and documentary research. The purpose of the research work will be descriptive, because after carrying out the research, what was studied will be described. The data production plan is based on indirect documentation. This practical way of obtaining data consists of a data collection carried out through documentary research already carried out, that is, books and scientific articles. The data obtained through the research are analyzed and interpreted using the hypothetical-deductive method, given that there are pre-established hypotheses for solving the problem presented. It is noteworthy that, after the introduction, the research is divided into three chapters. The first chapter addresses the development of homo sapiens and the paradoxical development of social networks, where the emergence of social networks that we currently witness and the impacts and benefits provided by them are studied. In the second chapter there is a study of the legislative frameworks that deal with the protection of personal data, national and international, and it explains what personal data are and the importance of their correct treatment. Finally, the third chapter presents an overview of civil liability in the General Data Protection Law and, after that, the main aspects are explored regarding the responsibility for correct data processing and the difficulty of quantifying the value of compensation. . Next, a jurisprudential research is presented, which aims to address the civil liability of companies for the leakage of personal data. The main conclusions sought are related to the effectiveness, or not, of civil liability for the leakage of personal data.

Keywords: Social Network – Sensitive Personal Data – Civil Responsability.

LISTA DE ABREVIAÇÕES, SIGLAS E SÍMBOLOS.

ARPA - Agência de Projetos de Pesquisa Avançada

art. – artigo

CDC - Código de Defesa do Consumidor

CoE - Conselho da Europa

EUA - Estados Unidos da América

GDPR - General Data Protection Regulation

LGPD - Lei Geral de Proteção de Dados

MG - Minas Gerais

n.p. - não paginado

nº - número

p. – página

PC - Computador pessoal

RG - Registro Geral

RGPD - Regulamento Geral Europeu sobre a Proteção de Dados

SP - São Paulo

STJ - Superior Tribunal de Justiça

TDAH - Transtorno do déficit de atenção com hiperatividade

UE - União Europeia

WWW - world wide web

§ - parágrafo

SUMÁRIO

INTRODUÇÃO

O crescimento do setor tecnológico, com o consequente advento da internet proporcionou ao indivíduo uma nova forma de realizar o seu convívio social, o que resultou no surgimento das redes sociais. Em razão disso, milhares de pessoas compartilham suas ideias, informações, sentimentos e outros dados em sites administrados por grandes empresas, o que acarreta um grande poder para estas detentoras das redes sociais.

Nesse contexto, a presente pesquisa tem como tema a responsabilização civil das redes sociais na proteção de dados pessoais. A delimitação temática centra-se na busca por discorrer acerca da responsabilização civil das empresas administradoras das redes sociais, especialmente no cenário jurídico brasileiro. Com fins sociológicos e jurídicos, analisa-se a jurisprudência do Superior Tribunal de Justiça, entre os anos de 2019 e 2024, no que concerne a responsabilização civil das redes sociais.

A fim de que se leve a efeito a pesquisa, tem-se como problema norteador: como a responsabilização civil das redes sociais frente ao vazamento de dados pessoais sensíveis poderá dirimir os danos aos seus usuários? No tocante às hipóteses desta pesquisa, têm-se: a) a responsabilização civil é suficiente para a contenção de comportamentos das empresas administradoras das redes sociais que não utilizam todos os meios possíveis de segurança para proteger a segurança de seus usuários; b) a responsabilização civil é insuficiente para a contenção de comportamentos das empresas administradoras das redes sociais que não utilizam todos os meios possíveis de segurança para proteger a segurança de seus usuários.

No que diz respeito aos objetivos da pesquisa, esta tem como objetivo geral, analisar os impactos frente ao vazamento de dados pessoais sensíveis e a responsabilização civil das empresas administradoras das redes sociais. Já nos objetivos específicos, estruturados em três: a) descrever historicamente o desenvolvimento do *homo sapiens* e o paradoxal desenvolvimento das redes sociais; b) verificar (inter)nacionalmente marcos legislativos dos dados pessoais sensíveis, privacidade e proteção na era do *big data*; c) é analisar jurisprudencialmente a (in)eficácia da responsabilização civil das redes sociais.

A relevância da pesquisa centra-se na era da informatização, onde o produto mais valioso não é algo físico, mas sim o digital. Com os dados pessoais, que são facilmente colhidos no meio online, a pesquisa enfatiza as redes sociais, tais como: Facebook, Instagram e WhatsApp. Justifica-se a escolha em razão de que são as maiores do segmento e consequentemente possuem mais poder de coleta de dados na era da *big data*.

Dessa forma, viabiliza-se a pesquisa com o estudo das legislações brasileiras e internacionais que impedem as redes sociais de utilizarem estes dados para fins unicamente financeiros, sem se preocupar com a segurança dos titulares dos dados, pois a falta de segurança acarreta vazamento de dados, que podem ser comercializados com outras empresas. O grande perigo deste comércio ilegal de dados centra-se nas empresas que utilizam essas informações para alavancar vendas ou até discriminar certos grupos de indivíduos. Esta discriminação pode ocorrer em razão da identidade de cada pessoa, que pode ser deduzida através dos seus dados que constam em redes sociais.

Apesar de não serem visíveis sem uma análise aprofundada, as redes sociais acumulam diversas informações valiosas dos indivíduos, capazes de informar características pessoais de cada cidadão. Com o advento da Web 4.0, inteligências artificiais podem traçar o perfil de cada pessoa, com base apenas informações que constam em bancos de dados de redes sociais. A pesquisa abordará os impactos que um vazamento de dados provoca ao indivíduo proprietário dos dados e as formas de responsabilizar as redes sociais em casos de violação dos seus sistemas de segurança com consequente vazamento de dados pessoais sensíveis.

Ademais, o assunto estudado é de grande importância, pois discorre sobre as ferramentas que o direito brasileiro dispõe para garantir o tratamento correto dos dados pessoais sensíveis, e assim oferecer maior proteção aos usuários das redes sociais.

Quanto à metodologia, a pesquisa, em sua categorização, terá natureza teórica, com tratamento de dados de forma qualitativa, pois estuda a aplicação de uma hipótese pré-definida. A conduta a ser utilizada para a obtenção de fontes para a realização do estudo será através de pesquisas bibliográficas e documentais. A finalidade do trabalho de pesquisa será descritiva, pois após realizar as pesquisas, será descrito o que foi estudado.

O plano de produção de dados, ou seja, a forma prática que será utilizada para a obtenção de dados que serão utilizados para embasar e fundamentar a pesquisa, ele será a partir de documentação indireta. Esta forma prática de obtenção de dados consiste em um levantamento de dados feito através de pesquisas documentais já realizadas, ou seja, livros e artigos científicos. Os dados obtidos através da pesquisa serão analisados e interpretados com o método hipotético-dedutivo, haja vista que há hipóteses preestabelecidas para a solução do problema apresentado.

A pesquisa divide-se em três capítulos: O primeiro aborda o desenvolvimento do homo sapiens e o paradoxal desenvolvimento das redes sociais. Em um primeiro momento, descreve-se o desenvolvimento do gênero homo, após estuda-se o desenvolvimento da internet e o consequente surgimento das redes sociais, o que é feito, principalmente, com apoio de obras escritas por Yuval Harari, Pierre Lévy e Manuel Castells. Após, com um teor predominantemente sociológico, expõe-se o paradoxo das redes sociais, onde são abordados aspectos positivos e negativos proporcionados por ela, o que será feito, principalmente, com apoio de obras escritas por Zygmunt Bauman e Byung-Chul Han.

O segundo capítulo aborda, em um primeiro momento, os marcos legislativos que tratam da proteção de dados pessoais, nacionais e internacionais, com uma base teórica baseada nas obras de Danilo Doneda, Bruno Ricardo Bioni e Têmis Limberger. Após, explana-se o que são os dados pessoais e a importância do tratamento correto deles, o que será feito com o apoio de obras de Danilo Doneda e Chiara Spadaccini de Teffé.

Por fim, o terceiro capítulo aborda como ocorre a responsabilização civil das redes sociais no ordenamento jurídico brasileiro. Inicialmente, apresenta-se um panorama acerca da responsabilidade civil na Lei Geral de Proteção de Dados, o que é feito com o apoio de obras de Bruno Ricardo Bioni e Bruno Miragem. Após, explora-se os aspectos principais quanto à responsabilidade de tratamento correto e quanto à dificuldade de quantificação do valor da indenização, o que é feito com o auxílio de obras de Ana Frazão, Walter Aranha Capanema e Glenda Gonçalves Gondim e, após, apresenta-se uma pesquisa jurisprudencial realizada no âmbito do Superior Tribunal de Justiça, que tem como principal objetivo abordar a responsabilização civil de empresas pelo vazamento de dados pessoais.

1 DO COLETIVO AO INDIVIDUAL: O PARADOXAL DESENVOLVIMENTO HISTÓRICO DAS REDES SOCIAIS.

O objetivo do capítulo é descrever historicamente o desenvolvimento do *homo sapiens* e o paradoxal desenvolvimento das redes sociais. Buscar-se-á, em um primeiro momento, descrever o desenvolvimento do gênero homo, o que será feito através de um panorama sobre as espécies que existiram durante a evolução *do homo sapiens* e como estas contribuíram para a evolução social destes. Após, será estudado o surgimento da internet e dos computadores, que viabilizaram o crescimento exponencial do círculo social do ser humano, através da criação de formas de conectar os humanos de diversas partes do mundo. Destaca-se que esta interligação mundial através da rede de computadores, que ocorreu mediante uma grande evolução tecnológica, que será tratada ao longo deste capítulo.

Ainda no primeiro momento do capítulo, será apresentado o contexto nacional do acesso à internet, e, para isso, será explicado como ocorreu o surgimento das Lan Houses no Brasil e a importância que elas possuem para a história das redes sociais no Brasil, visto que foram uma real representação de pontos de cultura, onde as pessoas residentes em locais mais periféricos tiveram acesso à rede.

Em suma, o primeiro momento deste capítulo será destinado à realização de uma pesquisa, com um teor principalmente histórico, acerca da evolução social do gênero homo, o que será feito através da contextualização sobre o surgimento de novas tecnologias de comunicação até a criação de uma rede de computadores que viabilizou o crescimento das redes sociais existentes atualmente.

O segundo momento conterá um teor predominantemente sociológico, visto que serão abordados aspectos específicos das redes sociais, a fim de viabilizar o estudo do teor paradoxal que elas apresentam, para, assim, proporcionar uma análise crítica da relação entre as benesses e os problemas que o surgimento e a disseminação das redes sociais provocaram nos indivíduos.

Ademais, será apresentada uma relação entre a obra distópica, 1984, de George Orwell que, apesar de ter sido escrita em 1948, tratou de fenômenos que podem ser observados atualmente, tais como a teletela. Também, será feita uma explanação acerca da busca pela eliminação da negatividade, aspecto frequente em grupos de indivíduos que utilizam as redes sociais para a comunicação.

Frisa-se que o presente capítulo realizará uma pesquisa que estudará sobre o surgimento do gênero homo, as formas de convívio social utilizadas por ele, sua evolução, criação de novas tecnologias até a interligação da comunicação através da internet e das redes sociais. Outrossim, será abordado alguns fatores que surgiram com o advento das novas tecnologias, tais como a fragilidade dos relacionamentos existentes no meio online, devido a facilidade da aquisição destes, e as consequências da velocidade proporcionada pelas redes sociais que gera o surgimento da comunicação rasa, sem essência.

Por fim, a ideia principal deste capítulo é a apresentação da evolução social dos antepassados gênero homo, a fim de contextualizar o surgimento das redes sociais. Ainda, as redes sociais serão sociologicamente estudadas, com o objetivo de discorrer sobre o paradoxo apresentado por estas.

1.1 O DESENVOLVIMENTO COLETIVO E SOCIAL DO *HOMO SAPIENS*

Ao longo da evolução humana, foram diversas as formas que os indivíduos utilizaram para socializar com seus semelhantes. Isto é, as redes sociais são ferramentas recentes na sociedade. Antes delas haviam outras formas que os indivíduos utilizavam para socializar. Para melhor compreender a evolução das redes sociais, faz-se necessário estudar como o *homo sapiens* se organizava em sociedade antes do surgimento desses meios.

Primordialmente, a fim de facilitar a compreensão do surgimento do *homo sapiens*, faz-se necessário discorrer acerca dos seus semelhantes. O surgimento do primeiro representante do gênero homo ocorreu em torno de 2,4 milhões de anos atrás e é chamado de *homo habilis*, este se organizava em pequenos grupos de vinte a cem indivíduos, não possuía distinções sociais marcantes em sua organização, eram nômades e sua forma de subsistência era a caça de pequenos animais e a coleta (Alves; Oliveira, 2015).

Posteriormente, por volta de 1,8 milhão e 143 mil anos atrás, há registros do *homo erectus*, o primeiro hominídeo que deixou a África e se espalhou para a Europa e Ásia. Este também se organizava em pequenos grupos sociais e deixou vestígios de cuidados realizados para ajudar os seus semelhantes mais fracos ou doentes (Alves; Oliveira, 2015).

Após esses, por volta de 300 mil e 35 mil anos atrás, encontra-se a espécie que coexistiu com o *homo sapiens*, trata-se do *homo neanderthalensis*, que possuía um cérebro mais desenvolvido, se organizava em pequenos bandos de caçadores-coletores e foi a primeira espécie a enterrar seus mortos (Alves; Oliveira, 2015).

Chega-se, então, na atual espécie, o *homo sapiens*, que se desenvolveu paralelamente com a espécie tratada anteriormente. As principais características desta espécie é a complexidade da sua organização social, marcada pela necessidade de uma cooperação entre os semelhantes em decorrência da caça de animais maiores e as migrações dos grupos para outras áreas (Alves; Oliveira, 2015).

Cabe destacar que o *homo sapiens* surgiu em um contexto demográfico único, ou seja, em uma região de lagos africanos onde se encontrava uma condição ecológica única. Apesar de todos terem nascido na mesma região, estes se dispersaram por toda região do globo terrestre, o que acarretou no surgimento de diversas culturas e línguas diferentes (Lévy, 1998).

Diante disso, os humanos, como os chimpanzés, possuem capacidade de construir amizades, porém esses instintos sociais possuem uma limitação. No momento em que o grupo fica muito grande o bando se divide em razão de uma desestabilização na ordem social do grupo, porém, após a revolução cognitiva, esses grupos aumentaram de tamanho. Ou seja, os instintos sociais sempre estiveram presentes no *homo sapiens* e, ao longo do tempo, estes aumentam cada vez mais (Harari, 2015). Nesse sentido, destaca-se a ampliação desses círculos sociais:

> **O Homo sapiens evoluiu para achar que as pessoas se dividiam entre "nós" e "eles"**. "Nós" era o grupo imediatamente à sua volta, independentemente de quem você fosse, e "eles" eram todos os outros. Na verdade, nenhum animal social jamais é guiado pelos interesses de toda a espécie à qual pertence. Nenhum chimpanzé se importa com os interesses da espécie chimpanzé, nenhuma lesma levantará um tentáculo em nome da comunidade global de lesmas, nenhum leão macho alfa tem intenção de se tornar o rei de todos os leões, e ninguém encontrará na entrada de uma colmeia o slogan "Abelhas-operárias do mundo, uni-vos!".
> Porém, **desde a Revolução Cognitiva, o Homo sapiens se tornou cada vez mais excepcional a esse respeito. As pessoas começaram a cooperar regularmente com completos estranhos, que elas imaginavam como "irmãos" ou "amigos"**. Mas essa irmandade não era universal. Em algum lugar no vale vizinho, ou depois de uma cadeia de montanhas, ainda era possível identificar quem eram "eles" (Harari, 2015, p. 179, grifo nosso).

Observa-se que, com o advento da revolução cognitiva, o *homo sapiens* passou a se diferenciar dos seus semelhantes, começou a apresentar comportamentos de

cooperação com indivíduos que viviam no mesmo ambiente que ele, mesmo que estes eram considerados estranhos, o que enseja o início a algo que pode ser chamado de meio de convívio social (Harari, 2015).

No mesmo sentido, ao analisar as culturas humanas sob uma perspectiva ampla, sob o enfoque de milênios e não séculos, a sociedade se encaminha para uma unicidade com relação à cultura, as civilizações estão cada vez mais complexas e maiores. Ademais, a sociedade teve diversos avanços na vida cotidiana das pessoas, que devido à grande relevância destes, podem até ser considerados como poderes “sobre-humanos”, dentre esses avanços se encontra a transformação da ordem social (Harari, 2015).

Ademais, após a explosão demográfica e o distanciamento acarretado por ela, surge a revolução neolítica, tratada como a segunda grande “ruptura”, que é baseada em uma mutação técnica, social, cultural e política, visto que proporcionou o surgimento da escrita, agricultura e das cidades e Estados. De certa forma, esta revolução possuiu como principal aspecto a substituição do método caçador e coletor por um modelo sedentário e fixo em um local (Lévy, 1998).

Por conseguinte, ocorreu, por volta do século XV, a considerada terceira ruptura, marcada pela interconexão entre os povos que anteriormente haviam se distanciado. Esta reaproximação foi proporcionada por indivíduos ávidos que se aventuraram em expedições e navegações a fim de buscar novas terras. Após, no século XX, momento em que a maioria dos indivíduos habitavam o campo, com a agricultura e a criação de animais, surge a revolução industrial, que acarreta no início da revolução informacional contemporânea, visto que, apesar de sempre haver pessoas que trabalham com a agricultura e com a transformação da matéria, a automatização destes trabalhos está cada vez mais presente na sociedade, o que se deve, principalmente, à informática (Lévy, 1998).

Diante disso, é indispensável discorrer sobre o surgimento da internet, que contribuiu para a ampliação do convívio humano, visto que as pessoas que inicialmente acessavam a Internet buscavam compartilhar experiências com outras pessoas, ou seja, saber os acontecimentos da vida de seus familiares, amigos e até de estranhos (Snowden, 2019). Nesse sentido, destaca-se a relação entre a comunicação e os transportes:

> O progresso das técnicas de transporte e de comunicação é, ao mesmo tempo, motor e manifestação desse relacionamento generalizado. Insisto com o paralelo entre transportes e comunicações, pois o efeito de influência mútua é constante, fundamental, verificado em toda parte, enquanto a substituição do transporte físico pela transmissão de mensagens é apenas local e temporário. A navegação de longo curso e a imprensa nascem juntas. O desenvolvimento dos correios estimula e utiliza a eficiência e a segurança das redes viárias. O telégrafo expande-se ao mesmo tempo que as ferrovias. O automóvel e o telefone avançam em paralelo. O rádio e a televisão são contemporâneos do desenvolvimento da aviação e da exploração espacial. Os satélites lançados pelos foguetes estão a serviço das comunicações. A aventura dos computadores e do ciberespaço acompanha a banalização das viagens e do turismo, o desenvolvimento dos transportes aéreos, a extensão das autoestradas e das linhas de trem de grande velocidade. O telefone móvel, o computador portátil, a conexão sem fio à Internet, em breve generalizados, mostram que o crescimento da mobilidade física é indissociável do aperfeiçoamento das comunicações. Um computador e uma conexão telefônica dão acesso a quase todas as informações do mundo, imediatamente ou recorrendo a redes de pessoas capazes de remeter a informação desejada. Essa presença virtual do todo em qualquer ponto encontra, talvez, o seu paralelo físico no fato de que um edifício qualquer de uma cidade grande contém elementos materiais vindos de todas as partes do mundo, concentrando conhecimentos, competências, processos de cooperação, uma inteligência coletiva acumulada ao longo dos séculos, com a participação, de alguma maneira, dos mais diversos povos (Lévy, 1998, p.39).

No tocante ao surgimento da internet, ele ocorreu na Agência de Projetos de Pesquisa Avançada (ARPA) do Departamento de pesquisa dos EUA, em 1950, momento em que ocorreu o lançamento do primeiro Sputnik, que assustou os centros americanos de alta tecnologia, e estes realizaram iniciativas ousadas, o que ocasionou o início a Era da Informação em grande escala (Castells, 2023). Quanto a estas iniciativas americanas, Castells discorre acerca de um sistema de comunicação invulnerável a ataques nucleares:

> Uma dessas estratégias, que desenvolvia um conceito criado por Paul Baran na Rand Corporation em 1960-4, foi criar um sistema de comunicação invulnerável a ataques nucleares. Com base na tecnologia de comunicação da troca de pacotes, o sistema tornava a rede independente de centros de comando e controle, para que a mensagem procurasse suas próprias rotas ao longo da rede, sendo remontada para voltar a ter sentido coerente em qualquer ponto da rede (Castells, 2023, p. 101).

Mediante este trecho é possível inferir que a troca de informações por meio de uma rede existe há tempos e, inicialmente, foi usada para fins militares. Castells explica que, apenas mais tarde, a tecnologia permitiu o empacotamento de todos os tipos de mensagens, tais como sons, imagens e dados e, por conta dessa universalidade da linguagem digital, surgiram condições tecnológicas para a

comunicação global (Castells, 2023). Ou seja, inicialmente as formas de mensagens trocadas eram muito limitadas e, com o passar do tempo, houve uma ampliação destas.

Quanto às maquinas que proporcionaram a utilização da internet pelo público geral, o surgimento destas foi possível devido a invenção de Ted Hoff, engenheiro da Intel, que desenvolveu o microprocessador. Esta invenção contribuiu para o avanço exponencial da microeletrônica, visto que se trata de um computador em um único chip, que proporciona a existência de pequenos aparelhos capazes de processar o grande número de informações dos aparelhos tecnológicos (Castells, 2023).

Visto isso, o processo de criação da internet passou por diversos acontecimentos desconhecidos pela maioria das pessoas. Inicialmente, conforme mencionado anteriormente, a internet era utilizada para fins militares e era sustentada pelo Departamento de Defesa dos EUA que, após, liberou o acesso à rede para cientistas que contribuíam para as pesquisas americanas e estes, por sua vez, começaram a utilizar os benefícios da rede para realizar a troca de mensagens pessoais com outros cientistas (Castells, 2023).

Em razão do aumento de cientistas que utilizavam as redes, tornou-se difícil a diferenciação do que se tratava de pesquisas militares e o que se referia a assuntos particulares tratados entre os pesquisadores. Pelo exposto, em 1980, houve a fragmentação das redes de internet, com o fim de diferenciar e organizar os dados tratados (Castells, 2023).

Simultaneamente a esses acontecimentos, houve o surgimento de um aparelho capaz de proporcionar a transferência de mensagens e pequenos arquivos pela rede sem que fosse necessária a passagem por um sistema principal. Esse aparelho é o modem, visto como um símbolo da contracultura, pois foi desenvolvido por dois estudantes de Chicago e distribuído gratuitamente como forma de ampliar o acesso das pessoas a esse meio de comunicação, o que representa uma forma de afastar a centralização do acesso à rede decorrente do fato de apenas grandes pesquisadores e militares possuírem acesso a esse meio de comunicação (Castells, 2023).

Ademais, o modem proporcionou a ampliação do alcance das redes e, mediante o recorte a seguir, será possível desenvolver a compreensão de como o acesso à internet se tornou possível aos civis, o que ampliou o acesso do público presente nos meios eletrônicos (Castells, 2023).

> Em 1983, Tom Jennings criou um sistema para publicação de quadros de avisos em PCs, por intermédio da instalação de um *modem* e de um *software* especial que permitia aos computadores se comunicarem com um PC equipado com essa tecnologia de interface. Essa foi a origem de uma das redes mais originais, de base, a Fidonet, que em 1990, já conectava 2.500 computadores nos EUA (Castells, 2023, p. 105).

Ainda, nessa época, Castells afirma que os indivíduos que tinham acesso aos meios tecnológicos eram aqueles que possuíam conhecimento do meio eletrônico, porém, com o surgimento, por volta do ano de 1990, do world wide web (WWW), forma que possibilitou uma maior facilidade de pesquisa no meio online, visto que organizou os sítios existentes na internet por tipo de informação e não mais por localização. Diante disso, contatou-se um grande salto tecnológico, pois viabilizou a organização dos sítios da internet por informação, o que facilitou a forma de pesquisa para os usuários que não detinham um conhecimento mais aprofundado da utilização dos dispositivos eletrônicos de pesquisa (Castells, 2023). Após estes acontecimentos, há ainda outro grande momento que possibilitou a ampliação da interconexão das redes, observável no seguinte trecho:

> Em fins da década de 1990, o poder de comunicação da Internet, juntamente com os novos progressos em telecomunicações e computação provocaram mais uma grande mudança tecnológica, dos microcomputadores e dos *mainframes* descentralizados e autônomos à computação universal por meio da interconexão de dispositivos de processamento de dados, existentes em diversos formatos. Nesse novo sistema tecnológico o poder de computação é distribuído numa rede montada ao redor de servidores da *web* que usam os mesmos protocolos da Internet, e equipados com capacidade de acesso a servidores em megacomputadores, em geral diferenciados entre servidores de bases de dados e servidores de aplicativos (Castells, 2023, p. 107).

Diante do acontecimento do trecho, tornou-se possível o surgimento de aparelhos com finalidades únicas, focados em áreas especificas da vida, seja atividades de casa, transportes, compras, entre outras. Essa especialização tornou-se possível devido ao poder de armazenamento das redes em seus servidores. Dessa forma, a inteligência e os dados são armazenados em um local onde os aparelhos que dispõem de um software específico conseguem ter acesso ao conteúdo armazenado, o que possibilitou a comunicação entre os aparelhos que tratam das diversas áreas da vida (Castells, 2023). Cumpre destacar que esta interligação provocada pela Internet contribuiu para o desenvolvimento das redes sociais online, pois, conforme Castells, “A comunicação mediada por computadores gera uma gama enorme de comunidades virtuais (Castells, 2023, p. 77).

No contexto nacional, a presença dos computadores se difundiu, por volta de 2003, com o programa Computador para Todos, do Governo Federal, que concedeu incentivos nas linhas de crédito ao varejo, o que proporcionou a aquisição de computadores por um maior número de pessoas. Devido a esse incentivo, de maneira inesperada, indivíduos passaram a comprar computadores com o objetivo de empreender, o que deu início às Lan Houses (Ferraz; Lemos, 2011).

O surgimento desses locais, na década de 2000, foi determinante para conceder à população um novo espaço público de acesso a fontes de conhecimento e cultura, ele tornou possível que os indivíduos usufruíssem do “viver em rede” por um valor muito inferior ao custo de um computador (Ferraz; Lemos, 2011).

Dessa forma, as Lan Houses podem ser consideradas como um “florescimento espontâneo” do que pretendiam os Pontos de Cultura idealizados pelo Governo, visto que estes pontos buscavam exatamente a criação de uma disseminação e criação de uma cultura própria do povo, cujo público principal era aquelas pessoas que se encontram em situações mais periféricas da sociedade (Ferraz; Lemos, 2011).

Cabe destacar que, em virtude desta evolução tecnológica tratada anteriormente, surgiu o denominado ciberespaço, uma espécie de dispositivo de comunicação qualitativamente original, que se demonstra ímpar quanto à outras formas de comunicação que o precederam. Isso porque os meios de comunicação anteriores ao ciberespaço apresentavam características especificas, como por exemplo o grupo que abrange a imprensa, o rádio e a televisão, este possui como caraterística a capacidade de transmitir uma mensagem para um grande grupo de pessoas, porém estas não têm a possibilidade de interagir diretamente com a mensagem recebida, apenas recebe e não responde. O outro meio de comunicação anterior ao ciberespaço é o grupo abrangido pelo correio e o telefone, que possui um esquema de troca de mensagens ponto a ponto, o que permite a reciprocidade entre as trocas de informações, porém não possui a capacidade de criação de uma comunidade, visto que a troca de mensagens em grande escala é difícil neste método (Lévy, 1998).

Visto isso, o ciberespaço se demonstra ímpar em relação aos outros meios de comunicação, visto que combina as vantagens das formas de comunicação apresentadas anteriormente, ou seja, ele é um dispositivo de comunicação que permite que uma pessoa envie uma mensagem para dezenas de outras pessoas e essas pessoas possuem a opção de apresentar resposta sobre esta mensagem e

interagir com as outras pessoas que receberam a referida mensagem inicial. De certa forma, já que o ciberespaço armazena estas mensagens enviadas, é possível observar o surgimento de grupos de discussão, denominados fóruns eletrônicos, que consistem na reunião de várias pessoas que compartilham de um mesmo interesse e, nestes fóruns, trocam ideias sobre estes assuntos (Lévy, 1998).

Realizada esta breve exposição acerca da evolução do homo sapiens desde a sua organização social primitiva até a criação dos meios eletrônicos para a troca de informações e experiências com os seus semelhantes, por meio da internet, dando início à virtualização do convívio social, é de suma importância discorrer acerca do paradoxo das redes sociais disponíveis na internet.

1.2 O PARADOXO DAS REDES SOCIAIS: A LIQUIDEZ DOS RELACIONAMENTOS SOCIAIS NAS REDES

Feitas tais considerações acerca do ciberespaço, é inegável que as características apresentadas por ele se assemelham com as redes sociais[1] existentes na atualidade, visto que estas proporcionam uma comunicação interligada entre vários indivíduos, que podem enviar e responder mensagens, o que torna possível a criação de grupos online, semelhantes aos fóruns eletrônicos que foram explicados no momento anterior. Diante disso, faz-se necessário discorrer acerca das redes sociais e o paradoxo apresentado por estas, ou seja, a presente seção possui como objetivo discorrer acerca de problemas e benesses que decorreram do surgimento e crescimento das redes sociais. Serão abordados diversos aspectos que podem ser constatados na sociedade contemporânea, mediante uma análise crítica de algumas obras relevantes para o estudo do crescimento da nova forma de conectar as pessoas.

O surgimento da Internet provocou a “morte do anonimato”, pois os indivíduos submeteram os seus direitos de privacidade à matança, por vontade própria, ou ao menos apenas consentiram em perder a privacidade como preço razoável pelas maravilhas proporcionadas por ela (Bauman; Lyon, 2013).

Na obra Vigilância Liquida, produzida em formato de entrevista, onde David Lyon questiona Zygmunt Bauman acerca de diversos fatores atinentes ao meio

[1] A Meta, empresa detentora da grande maioria dos aplicativos de rede social, afirma, em seu site, que suas tecnologias promovem a conexão de pessoas do mundo todo e dão voz à bilhões de pessoas. Disponível em: https://about.meta.com/br/actions/. Acesso em 30/11/2023.

tecnológico, Lyon, em um de seus questionamentos, aufere que “São tantos os relacionamentos em parte - ou na totalidade - vivenciados online que uma sociologia sem o Facebook é inadequada” (Bauman; Lyon, 2013, p. 40).

No mesmo sentido, Bauman defende que “Nossa vida divide-se (e cada vez mais, quando passamos das gerações mais velhas para as mais jovens) entre dois universos, “on-line” e “off-line”, e é irreparavelmente bicentrada” (Bauman; Lyon, 2013, p. 42).

> Reconhecidamente, Rose estava preocupado em fazer avaliações inequívocas - Como de fato se deveria estar no caso de uma transação seminal, porém arriscada, como a troca de esparsos incidentes de “proximidade” off-line pela volumosa variedade on-line. A “proximidade” trocada talvez fosse mais satisfatória, porém consumia tempo e energia e era cercada de riscos; a “proximidade” adotada sem dúvida é mais rápida, quase não exige esforço e é praticamente livre de riscos, mas muitos a consideram muito menos capaz de aplacar a sede de companhia plena. Ganha-se uma coisa, perde-se outra - e é terrivelmente difícil decidir se os ganhos compensam as perdas; além disso, uma decisão está de uma vez por todas fora de questão - você vai achar a opção tão frágil e provisória quanto a “proximidade” que obteve (Bauman; Lyon, 2013, p.43).

Diante disso, as redes proporcionam uma nova forma de proximidade, onde não se exige tanto esforço para a realização de um contato com outro indivíduo, uma das diferenças entre o meio on-line e o off-line é a facilidade e agilidade proporcionada pelo primeiro, porém, por consequência disso, ele se demonstra mais ineficiente no que concerne a relação entre os indivíduos, visto que torna a relação mais frágil diante da facilidade de obtenção (Bauman; Lyon, 2013).

No âmbito das redes sociais e aparelhos digitais, é indispensável discorrer acerca da obra distópica de George Orwell, intitulada 1984, visto que a leitura desta proporciona uma visão detalhada de como seria uma sociedade onde um dos pilares principais é o controle e a vigilância. Escrito em 1948, o livro retrata a vida de Winston Smith em uma sociedade regida por um governo totalitário representado pelo “Grande Irmão”, personificação da idealização do partido que detém o poder (Orwell, 2009).

Além disso, a obra possui uma figura que se enquadra diretamente com o objeto de estudo desta pesquisa: as teletelas. As teletelas são instrumentos utilizados pelo Partido existente no livro de Orwell e servem para vigiar e evitar qualquer pensamento contrário às ideias dos governantes, o que possibilitava uma detecção antecipada de conspirações e acarretava na resolução destas “ameaças” antes do seu agravamento (Orwell, 2009). A respeito desse instrumento:

> A teletela recebia e transmitia simultaneamente. Todo som produzido por Winston que ultrapassasse o nível de um sussurro muito discreto seria captado por ela; mais: enquanto Winston permanecesse no campo de visão enquadrado pela placa de metal, além de ouvido também poderia ser visto. Claro, não havia como saber se você estava sendo observado num momento específico. Tentar adivinhar o sistema utilizado pela Polícia das Ideias para conectar-se a cada aparelho individual ou a frequência com que o fazia não passava de especulação. Era possível inclusive que ela controlasse todo mundo o tempo todo. Fosse como fosse, uma coisa era certa: tinha meios de conectar-se a seu aparelho sempre que quisesse. Você era obrigado a viver – e vivia, em decorrência do hábito transformado em instinto – acreditando que todo som que fizesse seria ouvido e se a escuridão não fosse completa, todo movimento examinado meticulosamente (Orwell, 2009, p.13).

Diante disso, apesar da obra ter sido escrita em 1948, percebe-se a existência de uma nítida relação entre o instrumento Teletela utilizado pelo partido, com os tablets, notebooks e celulares existentes atualmente, que possibilitam o acesso às redes sociais, porém se diferem no fato de que, na obra de Orwell, os cidadãos evitavam a Teletela e agiam de maneira controlada perante ela, pois temiam a vaporização[2] (Orwell, 2009).

Outro aspecto observado no advento das redes sociais é a cadeia do igual, decorrente da busca por extinguir a negatividade do que é diferente, visto que o diferente proporciona desconforto e reduz a alta velocidade do diálogo e da troca de experiências dos iguais. Em outras palavras, os indivíduos que possuem percepções de mundo iguais utilizam-se das redes sociais para trocar informações apenas com seus semelhantes, visto que o diálogo entre eles possui uma alta velocidade, decorrente de sua rasa comunicação. Esta rasa comunicação é ocasionada pela busca por ausência de negatividade, ou seja, no momento em que o outro não manifesta objeções contra as ideias explanadas, não há negatividade, o que resulta em um diálogo tranquilo entre os indivíduos que compartilham da mesma linha de pensamento (Han, 2017).

Esse isolamento dos indivíduos com pensamentos semelhantes em grupos fechados proporciona a descarga de instintos humanos maléficos ou simplesmente a supressão destes grupos. Isso porque a formação destes grupos gera uma manipulação daqueles que os compõem, o que ocasiona no surgimento de modelos de ordem, ou seja, aqueles que buscam uma ordem total, inquestionável, uma ordem

[2] Vaporização, na obra 1984 de George Orwell, é quando a pessoa simplesmente some da sociedade, seu nome é esquecido e todos os indícios de sua existência são apagados, o indivíduo é eliminado da sociedade em questão de pouco tempo (Orwell, 2009).

invencível da razão, ordem detentora da ideia de que toda divergência deve se afastar do caminho mediante uma manipulação habilidosa. Basicamente ela entende que tudo que causa infelicidade deve ser retirado do caminho (Bauman; Lyon, 2013).

Nessa toada, a convicção de que a proeza de eliminar toda a negatividade é factível também foi presenciada pela humanidade durante o nazismo, que buscava erradicar de uma vez por todas qualquer condição humana que consideravam ser irregular. Possuía uma ideia de colocar ordem na sociedade mediante uma queima de suas impurezas. Embora de forma menos repulsiva, é isso que presenciamos nas redes sociais, porém sem a utilização dos métodos primitivos como a lavagem cerebral, o extermínio e a força (Bauman; Lyon, 2013).

Estima-se que o surgimento de doenças neuronais, tais como depressão, TDAH, síndrome do burnout e outras, como uma consequência do excesso de positividade proporcionado pelos meios eletrônicos. Essa constatação ocorre devido à substituição da alteridade, fator determinante para o funcionamento dos meios de defesa imunológicos, pela diferença, que por sua vez não acarreta em nenhuma reação imunológica. Isso deve principalmente pela ausência da necessidade de fortalecimento imunológico em um sistema onde há apenas o igual, ou seja, aquele que não apresenta riscos visíveis ao sistema não é tratado como uma ameaça a ser neutralizada (Han, 2015).

O esgotamento e a exaustão, sintomas comuns das doenças neurológicas, não são indícios da existência de reações imunológicas, são consequências do excesso de informação que provoca o sufocamento do indivíduo. Salienta-se que a violência provocada pela positividade se desenvolve de maneira silenciosa, sem a existência direta de uma inimizade, como era o caso das grandes guerras do século passado. Atualmente, presencia-se uma forma de violência diferente da primitiva, ela é saturante, exaustiva e provocada pelo sistema (Han, 2015).

Enfatiza-se que o excesso de transparência proporcionado pelas redes sociais causa a perda da vivacidade, haja vista que o indivíduo busca a todo custo a eliminação da negatividade em prol da velocidade na troca de informações, a satisfação momentânea, que é proporcionada pela cegueira quanto ao mundo exterior gerada pela reafirmação do que já existe. O efeito disso é a perda do conhecimento de como lidar com um determinado acontecimento negativo, o que gera uma regressão na forma como o indivíduo trabalha a sua dor (Han, 2017).

Noutro vértice, as redes sociais também contribuíram para a transformação das coisas em mercadoria, isso porque criou-se a cultura da necessidade de exposição para ser real. Frente a isso, o semblante humano tornou-se uma simples superfície transparente, pois a face se esgota totalmente em seu valor expositivo (Han, 2017).

Ademais, a coação expositiva presenciada atualmente, reforçada por redes sociais como o Facebook, leva a alienação do próprio corpo, fator determinante para a transformação do corpo humano em objeto expositivo que deve ser sempre aprimorado, isso porque as imagens apresentadas na rede são feitas de uma forma especial, voltada para beirar a perfeição, com o auxílio de ângulos e aplicativos de edição de imagem para maximizar cada vez mais o valor expositivo. Dessa forma, o valor expositivo rouba a verdadeira face dos indivíduos, visto que a verdadeira imagem possui negatividade, não é perfeita e por isso não agrada a sociedade da transparência, que busca a todo custo a aniquilação da negatividade (Han, 2017).

Outra consequência da sociedade da transparência é a eliminação das cerimônias em prol da aceleração na circulação de informações, fator que incide diretamente na geração de conhecimento dos indivíduos, isso porque o conhecimento necessita da negatividade oferecida pelos rituais, visto que estes se apresentam como um processo de transformação do conhecimento. A aquisição de conhecimento depende do âmbito imaginativo que é retirado pelo imediatismo das informações (Han, 2017). Nesse sentido, Han afirma que “A coação por transparência aniquila o odor das coisas, o perfume do tempo; a transparência não tem perfume. A comunicação transparente, que já não admite nada indefinido, é obscena” (Han, 2017, p. 76).

Realizada esta explanação acerca das redes sociais e suas consequências, verifica-se que as redes sociais trazem consigo uma realidade paradoxal, visto que, ao passo que aproximam os indivíduos, também o distanciam. Isso se deve principalmente ao fator negatividade abordado por Han, os indivíduos buscam se relacionar apenas com pessoas que compartilham das mesmas ideias, o que impossibilita a realização de um diálogo (Han, 2017).

Enfatiza-se, também, que os usuários das redes sociais geram uma grande quantidade de informações durante o uso deste meio de comunicação, o que ocorre devido aos rastros deixados no meio online, informação esta que, apesar de não poder ser aproveitada por pessoas físicas, é utilizada pelas empresas de tecnologia e donas das redes sociais, visto que possuem métodos desenvolvidos para interpretar este excedente de dados deixados pelas pessoas (Hartmann; Piaia, 2021).

Apresentado o aspecto paradoxal das redes sociais, ou seja, a relação entre os pontos positivos e negativos existentes nela, o próximo capítulo será utilizado para a realização de explanações acerca de legislações aplicáveis ao tratamento de dados pessoais, bem como para o desenvolvimento de pesquisa sobre os dados sensíveis na era *big data*. Destaca-se a importância do capítulo seguinte, que tratará dos dados pessoais sensíveis que, com o exposto anteriormente, são amplamente produzidos durante a relação dos indivíduos no meio online.

2 DADOS PESSOAIS SENSÍVEIS, PRIVACIDADE E PROTEÇÃO NA ERA DO *BIG DATA*

O presente momento da pesquisa realizará explanações acerca dos marcos legislativos que tratam da proteção de dados pessoais, tanto nacionais como internacionais. No âmbito nacional será estudado, além da Lei Geral de Proteção de Dados, o Código de Defesa do Consumidor e o Marco Civil da Internet, visto que, apesar de não se demonstrarem como legislações específicas do assunto, possuem dispositivos normativos que tratam sobre a privacidade. Já, no âmbito internacional, serão estudadas as primeiras legislações na previsão e proteção dos dados pessoais. Ademais, será feito um enfoque específico no direito europeu, devido à sua importância neste assunto e ao fato de que inspirou o Brasil na criação da LGPD.

Em prosseguimento, buscará elucidar o que são os dados pessoais e a importância do tratamento correto deles, visto que, no cenário da *big data*, o direito à intimidade corre risco, devido à alta concentração de informações nos bancos de dados e os métodos de processamento avançados. Para isto, buscar-se-á explicar o conceito da *big data*, os métodos de coleta e tratamento de dados, bem como casos onde o direito à privacidade foi violado.

Diante disso, o objetivo desta sessão será dissertar acerca de legislações internacionais e nacionais que tratam, ou já trataram, sobre o tema dos dados pessoais, com o enfoque principal no cenário europeu e no brasileiro. Após isso, será o momento de discorrer sobre os dados pessoais e os dados pessoais sensíveis, onde serão explicadas as possibilidades de coleta destes por dispositivos móveis, bem como o tratamento das informações obtidas com a utilização de *softwares* avançados. Também será explicado como os dados pessoais que, em um primeiro momento não apresentam características sensíveis, podem apresentar, após o tratamento, uma determinada carga sensível.

2.1 MARCOS LEGISLATIVOS (INTER)NACIONAIS DA PRIVACIDADE E DA PROTEÇÃO DE DADOS PESSOAIS

Buscar-se-á abordar a privacidade e proteção dos dados pessoais sensíveis na era *big data*, com o intuito de discorrer acerca dos marcos legislativos internacionais e nacionais que proporcionaram o início e a evolução da proteção dos dados dos indivíduos no meio digital. Inicialmente, um aspecto a ser destacado é a existência de uma tendência a ocorrer uma convergência entre as legislações que tratam do tema

proteção de dados, visto que há características específicas que impossibilitam a criação de uma solução isolada em um determinado país (Doneda, 2021).

No cenário internacional, os modelos norte-americano e europeu são os principais, visto que são frequentemente tratados como indutores de soluções adotadas por ordenamentos jurídicos de outros países (Doneda, 2021). Porém, diante do fato do Brasil adotar o mesmo sistema utilizado pela Europa, o Civil Law[3], esta pesquisa se deterá à análise do modelo europeu, com o intuito de realizar apenas breves menções ao norte-americano.

No que concerne ao tema da proteção de dados, existe uma tendência de ocorrer uma convergência entre as legislações que tratam deste tema, visto que há características específicas e até intrínsecas no tema, que impossibilitam a criação de uma solução isolada em um determinado país (Doneda, 2021).

Cabe destacar a existência, neste tema, de uma dissensão entre os países que adotam o sistema Common Law[4] e o Civil Law. Essa tensão entre os países que utilizam esses sistemas, ocorre, principalmente, em razão da resistência apresentada por países adeptos ao modelo Common Law em vincular diretamente a matéria da proteção de dados aos direitos fundamentais ou a algum modelo de tutela da dignidade. Importante destacar a existência de países que, mesmo vinculados a esse modelo, apresentam características mistas, com elementos do modelo europeu, que aplica o modelo Civil Law. São exemplos de países que apresentam a divergência mencionada, a Austrália, Nova Zelândia e Canadá (Doneda, 2021).

No cenário europeu, as tratativas acerca da proteção de dados iniciaram no ano de 1970, por meio da Lei de Proteção de Dados Pessoais do Lande de Hesse, na Alemanha, que era composta por apenas 17 artigos. A referida legislação sintética possuía como objetivo principal disciplinar as atividades dos centros de processamento de dados de instituições e sujeitos submetidos à autoridade do território. Em prosseguimento, surgiu a lei sueca, em 1973, classificada como a primeira lei nacional que trata sobre a proteção de dados pessoais e, em 1978 surge, na França, a lei 78-17, que passou a regular a matéria. Cabe destacar que as legislações tratadas neste parágrafo estavam de acordo com a resolução europeia de

[3] Civil Law é o sistema que o direito brasileiro é filiado, onde "a lei é a fonte primária do sistema jurídico" (Tartuce, 2020, p. 2).

[4] Common Law é o sistema em que "os precedentes jurisprudenciais constituem a principal fonte do direito" (Tartuce, 2020, p. 2).

1973, que tinha como objetivo o incentivar os países europeus a adotar princípios mínimos na matéria, para que no futuro possibilitasse a criação de uma convenção aprofundada nos aspectos comuns no direito interno (Doneda, 2021).

Ademais, a Alemanha é um dos países que apresenta maior desenvolvimento doutrinário na proteção de dados, visto que essa área é classificada como um instituto autônomo (Menke, 2019). O direito alemão desempenhou um grande papel para o início do desenvolvimento da área dos dados pessoais, como pode-se observar no seguinte trecho:

> A primeira lei no mundo sobre o assunto foi editada em 1970 pelo estado alemão de Hessen. No ano de 1977, o Parlamento alemão aprovou lei federal de proteção de dados (Bundesdatenschutzgesetz). Toda-via, o ápice do reconhecimento da proteção de dados ocorreu com a decisão do Tribunal Constitucional Federal sobre a questão do censo demográfico que se realizava na Alemanha no ano de 1983 (Volkszählungsurteil). Esta decisão estabeleceu o direito fundamental à autodeterminação informativa (Grundrecht auf informationelle Selbstbestimmung) (Menke, 2019, p. 781).

A Volkszählungsurteil[5] foi um caso que tratou de reclamações constitucionais feitas pelos cidadãos da Alemanha, que eram contrários a uma lei alemã que previa um novo censo demográfico, que não se limitaria apenas a realizar a contagem dos indivíduos, mas também faria o levantamento de diversos outros dados pessoais da população, dentre eles estaria o sexo, estado civil, religião e outras formas especificas de identificar uma pessoa (Menke, 2019).

No mesmo sentido, a Volkszählungsurteil é uma decisão que se tornou um marco da proteção de dados, pois fixou diretrizes desta matéria que influenciaram tanto a doutrina como a jurisprudência de outros países além da Alemanha, visto que o teor da decisão foi além do caso concreto e fixou afirmações programáticas da disciplina (Menke, 2019).

Importante destacar que as iniciativas do cenário europeu foram fundamentais para, no cenário internacional, proporcionar a consciência de que um foco exclusivo no direito interno não é suficientemente eficaz para a proteção de dados pessoais, visto que a coleta e tratamento dos dados pessoais podem ocorrer fora do território de um Estado. Por conta disso, o Conselho da Europa decidiu abordar a questão da proteção dos dados pessoais em uma convenção, o que deu vida, em 1981, à Convenção 108 do CoE (Conselho da Europa), também conhecida como “Convenção

[5] Em tradução livre, caso do censo demográfico (Menke, 2019).

de Estrasburgo", que teve como objetivo incentivar os Estados-Membros do Conselho da Europa a adotar determinadas normas específicas para o tratamento dos dados pessoais. Um dos aspectos mais importantes desta convenção, e que vai diretamente de encontro com o fato tratado no início deste parágrafo, foi a adoção de um prisma universalista, visto que a convenção não foi projetada para ser pura e exclusivamente europeia, pois ela foi aberta para adesões de outros países que não compõe a União Europeia (Doneda, 2021).

No ano de 1984 o Reino Unido, em decorrência da adoção da Convenção 108, promulgou o seu *Data Protection Act*, que tratava a matéria da proteção de dados de uma forma peculiar, visto que o direito à privacidade não era propriamente reconhecido, era visto apenas como uma tutela contra a intromissão não autorizada na vida privada pelo abuso de dados pessoais. Porém foi no ano de 1995 que ocorreu o surgimento de um documento capaz de padronizar, de maneira efetiva, a proteção de dados pessoais na União Europeia, a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho Europeu. A Diretiva[6] se demonstrou mais ambiciosa que os outros marcos legais anteriores. Isso se deve, principalmente, à imposição feita aos legisladores dos estados-membros, no sentido de que estes deveriam confeccionar e aprovar normas com um conteúdo normativo que vá de encontro com o conteúdo estabelecido na Diretiva, conteúdo este que se demonstra bem detalhado e definido (Doneda, 2021).

Cumpre destacar que a Convenção 108 do CoE e a Diretiva 95/46/CE possuem algumas diferenças quanto ao objetivo e abordagem do tema proteção de dados pessoais. Enquanto a Convenção deixa evidente, em seu preâmbulo, que a proteção de dados pessoais se refere à proteção dos direitos humanos e das liberdades fundamentais, através do entendimento de que a matéria é um pressuposto do estado democrático, o que apresenta uma consideração à Convenção Europeia para os Direitos do Homem (Doneda, 2021).

A Diretiva, por outro lado, apresenta uma visão voltada à proteção dos dados pessoais no cenário comercial, ao induzir o comércio por meio da criação de regras comuns para a proteção destes em uma determinada região. Porém, a Diretiva não deixa de mencionar a existência dos direitos fundamentais, o que torna possível

[6] As Diretivas são diplomas legais da União Europeia, que visam a promoção de uma harmonia entre as legislações nacionais, também estabelecem objetivos que os Estados-Membros deverão alcançar. Quanto à incorporação deste diploma legal no direito interno de cada país, isso fica a critério deste (Teffé, 2022).

observar a estruturação desta com a presença de dois eixos principais que disciplinam o tema. O primeiro é a proteção da pessoa e o objetivo de proporcionar a livre circulação de pessoas e aspectos atinentes ao comércio no espaço comum, o que está intimamente ligado à circulação de dados. Quanto ao segundo eixo, este é a referência aos direitos fundamentais do homem, que é adotado como base e fundamento para a disciplina (Doneda, 2021).

Importante destacar, no contexto da Diretiva, a adoção de uma prática frequente em legislações que tratam de temas relacionados à tecnologia, que é a vinculação da matéria a princípios, ou seja, na coleta, o tratamento e o uso dos dados pessoais são regidos pela observância de determinados princípios. Frisa-se que, apesar de inexistir um apontamento direto de garantias e limites diretamente ligados aos direitos, a Diretiva apresenta diversos princípios que os estados-membros devem prever em suas legislações internas, além de prever limites e exceções ao tratamento dos dados pessoais. No tocante ao fluxo de dados entre as fronteiras, o diploma legal se demonstra preocupado com este assunto e estipulou que a circulação dos dados será livre entre os estados-membros e, quanto aos outros países, a circulação será regida pelo princípio da equivalência, ou seja, só será possível a transmissão de dados caso o outro país possua um nível de proteção de dados adequado aos padrões estabelecidos pela Diretiva, em caso negativo, a circulação dos dados será cerceada (Doneda, 2021).

Dentre os países europeus que legislaram acerca da proteção de dados, merece destaque a Itália, visto que seu processo de formação de um direito voltado à privacidade ocorreu mediante uma atuação conjunta entre a doutrina e a jurisprudência, que, diante da evolução da matéria em outros países, buscaram juntas a elaboração de contornos e fundamentos acerca desta. Inicialmente, o Código Civil de 1865, que estava em vigor no momento em que as discussões se iniciaram, não previa o assunto da privacidade e, por isso, naquele momento, este direito foi ignorado pela doutrina (Doneda, 2021).

Foi após a entrada em vigor do Código Civil Italiano de 1942 que houve o surgimento do direito à imagem, que foi utilizado pela doutrina como fundamentação para o direito à privacidade, porém, por ser uma tese fundamentada em analogia, houve muita resistência por parte daqueles que consideravam que a matéria do direito à imagem deveria ser interpretada apenas de acordo com a sua ideia específica, o que torna inviável a aplicação de analogia. Na década de 1950 que entram em cena

os tribunais italianos que, gradualmente, passaram a reconhecer a existência de um direito denominada *diritto alla riservatezza*[7] (Doneda, 2021).

Ainda no contexto dos tribunais italianos, cabe ressaltar o “caso Petacci”, importante episódio para a consolidação do direito à privacidade nos tribunais, visto que foi por meio dele que a Corte d’Appello de Milão entendeu que o ato de publicar fatos atinentes à vida íntima de um indivíduo gera uma violação ao direito subjetivo à privacidade, o que acarreta no enquadramento disto em uma categoria específica dos direitos da personalidade. No julgado, destaca-se também que não foi necessária a demonstração de um efetivo prejuízo econômico para a parte. Após isso, foi apenas em 1970 que as altas cortes italianas reconheceram a existência de um *diritto alla riservatezza*, o que resultou, em prosseguimento, na criação legislativa da lei nº 300, que trata do direito à privacidade (Doneda, 2021).

Quanto ao contexto europeu geral, merece considerações o Regulamento nº 2016/679, conhecido como Regulamento Geral Europeu sobre a Proteção de Dados ou, em espanhol, *General Data Protection Regulation* (GDPR). Este marco legislativo foi muito importante para a proteção de dados em toda a Europa, visto que proporcionou uma uniformidade legislativa sobre a matéria em todo território europeu. Isso se deve principalmente ao fato de que as Diretivas, utilizadas anteriormente, eram aplicadas em via de exceção, no momento em que as leis nacionais não possuíam aplicabilidade (Doneda, 2021). Nesse sentido, destaco o seguinte trecho, que explica a carga trazida pela GDPR ao cenário europeu:

> O Regulamento Geral Europeu sobre a Proteção de Dados (RGPD – Regulamento (UE) nº 2016/679) traz uma lista de “categorias especiais de dados pessoais”, conferindo proteção específica para os dados sensíveis. Entende-se que a utilização do Regulamento trouxe mais segurança para o tema, ao estabelecer, precisamente, quais dados deveriam ser de natureza sensível e oferecer definições claras para algumas espécies assim consideradas (Teffé, 2022, p. 50).

No tocante ao aspecto territorial da GDPR, a legislação é aplicável tanto para os países que se encontram no âmbito da União Europeia, quanto para países que não são comunitários, e, para estes, a legislação é aplicada nos momentos em que possuem uma relação comercial ou jurídica capaz de afetar os europeus ou alguma empresa que possua sede lá. Este fenômeno se deve, principalmente, ao fato de que

[7] Em tradução livre: direito à privacidade.

os dados circulam livremente, o que impossibilita a limitação territorial da transmissão deles. Cabe destacar a existência de um órgão regulador no diploma legislativo, aspecto que garante mais segurança para os dados nas relações comerciais internacionais (Limberger, 2020). Nesse sentido, destaca-se o seguinte trecho:

> Este, por sua vez, ocasionou um “efeito dominó”, visto que passou a exigir que os demais países e as empresas que buscassem manter relações comerciais com a UE também deveriam ter uma legislação de mesmo nível que o GDPR. Isso porque o Estado que não possuísse lei de mesmo nível passaria a poder sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da UE. Considerando o contexto econômico atual, esse é um luxo que a maioria das nações, especialmente as da América Latina, não poderia se dar (Garrido, 2023, p.10).

A relevância da GDPR ocorre pois obrigou os demais países a adotar suas medidas de segurança de dados, sob a pena de sofrer barreiras econômicas (Garrido, 2023). Para melhor exemplificar a aplicação da GDPR em território distinto do europeu, colaciono o seguinte trecho:

> Apenas a título ilustrativo, uma instituição brasileira que capture dados no Brasil, em território nacional, mas que tenha um aplicativo que permita que o cliente seja de qualquer cidadania, nacionalidade, residência, e, portanto, o usuário do serviço, titular dos dados, pode ser um europeu, que mantém sua vida em um país da União Europeia, mas está temporariamente a trabalho no Brasil, utiliza cartão de crédito internacional, acaba por atrair, em termos de aplicação de leis e jurisdição para a sua operação, tanto a regulamentação nacional (LGPD) como também a regulamentação europeia (GDPR). Se essa instituição brasileira utilizar recursos na nuvem e fizer a guarda internacional dos dados pessoais em outro país, poderá atrair ainda outras regulamentações (como o Cloud Act, dos EUA) (Garrido, 223, p.27).

No cenário brasileiro, o Código de Defesa do Consumidor, Lei nº 8.078/90, já trouxe, no ano de 1990, em seus artigos 43 e 44, disposições acerca dos dados pessoais dos consumidores. Isso porque os artigos acima mencionados determinam que os consumidores possuem o direito de acesso às informações contidas em seus cadastros, e que estes dados devem ser expostos ao consumidor de maneira clara, objetiva e verdadeira. Cabe destacar que o artigo 43 §2º ainda prevê a obrigação de comunicar o consumidor sobre o registro de seus dados, com ressalva das hipóteses onde este solicita o registro dos dados (Brasil, 1990).

Outrossim, o artigo 5º, LXXII, da Constituição da República Federativa do Brasil prevê o direito de o indivíduo ter acesso às suas informações existentes em registros ou bancos de dados das entidades governamentais ou de caráter público e, se

necessário, permite a retificação dos dados (Brasil, 1988). Em decorrência deste dispositivo constitucional, surge a Lei nº 9.507/97, responsável por disciplinar o procedimento de habeas data. Quanto a este diploma legislativo, destaca-se o parágrafo único do artigo 8º, que prevê o esgotamento da via administrativa como requisito para o ajuizamento da ação, o que é uma exceção ao artigo 5º, XXXV da Constituição, responsável por determinar que o Poder Judiciário deve examinar toda lesão ou ameaça a direito (Brasil, 1997).

Porém foi a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, que trouxe ao Brasil a previsão da proteção dos dados pessoais. Esta legislação estipulou, em seu artigo 3º, os princípios do uso da internet no Brasil e, dentre eles, se encontra a proteção da privacidade e dos dados pessoais. Ainda, destaca-se o artigo 7º deste diploma legal, o qual elenca os direitos dos usuários durante o acesso à Internet, tais como o sigilo de comunicações privadas, consentimento expresso para a coleta e tratamento de dados pessoais, possibilidade de indenização em casos de violação da intimidade (Brasil, 2014).

No mesmo sentido, o Marco Civil da Internet estabeleceu, no artigo 19, disposições acerca da responsabilidade civil dos provedores de aplicações de internet em casos de conteúdo produzido por terceiros. No entanto, esta responsabilidade ficou condicionada a dois aspectos: o primeiro relaciona-se a necessidade de uma ordem específica para a retirada do conteúdo do meio online, e o segundo a necessidade das providências estipuladas se encontrarem dentro dos limites técnicos do provedor. Cabe destacar que, de acordo com o próprio dispositivo legal, estas condições foram introduzidas com o intuito de impedir a censura e assegurar a liberdade de expressão (Brasil, 2014). Cabe destacar que a legislação sofreu críticas quanto à maneira como trata o tema:

> O Marco Civil possui esse erro conceitual de que todo direito é atribuído e não empoderado. Os direitos à liberdade de expressão, privacidade, vida privada, de acesso à informação, por exemplo, são universais e já dados anteriormente a entendimento a todos os cidadãos e usuários de internet. Não há nova contextualização desses direitos. Não há tentativa alguma de explicá-los ou de relacioná-los com as práticas de internet atualmente existentes. Eles são direitos históricos e acabou, que os juízes nos digam o que eles são atualmente. Aliás, há uma fé desmesurada no Marco Civil acerca da participação do Poder Judiciário e do juiz. Até que ponto isso é relevante para o desenvolvimento da internet? (Gonçalves, 2016, p. 06).

Por fim, no ano de 2018 foi sancionada a Lei Geral de Proteção de Dados (LGPD), marco legislativo de grande relevância para a integração da economia digital, responsável por tratar a proteção dos dados pessoais de forma sistemática e coerente, estipulando procedimentos estruturantes e regras específicas acerca desse ramo do direito (Bioni, 2021). Para melhor esclarecer:

> Com a aprovação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709/2018, o Brasil inaugura o que se pode denominar “sistema protetivo dos dados pessoais”. Essa lei deve ser entendida como tal, pois estabelece princípios que devem nortear a coleta, o compartilhamento e o tratamento dos dados pessoais, direitos básicos dos titulares dos dados pessoais, obrigações impostas aos controladores e responsáveis pelo tratamento de dados pessoais. Portanto, a LGPD não afasta a aplicação dos dispositivos legais supramencionados, o que se comprova pelo art. 45 ao estabelecer a aplicação do Código de Defesa do Consumidor. (Teixeira; Guerreiro, 2022, p.07).

Nesse sentido, a LGPD foi um marco crucial para a proteção de dados, pois estabeleceu princípios capazes de nortear desde a coleta dos dados pessoais, até o compartilhamento e tratamento destes, o que proporciona direitos básicos aos indivíduos titulares dos dados coletados (Teixeira; Guerreiro, 2022).

Cabe destacar a dificuldade de criar uma legislação sobre a proteção de dados, visto que a envergadura desses marcos regulatórios específicos é complexa, isso se deve ao fato de que o objeto em discussão não é um setor específico do país, mas sim todas as atividades econômicas, sejam elas públicas ou privadas, que utilizem, de alguma forma, os dados pessoais para proporcionar o seu desenvolvimento (Bioni, 2021).

Ademais, a necessidade da criação da LGPD resta evidenciada no fato de que, em julho de 2018, a Brasscom lançou um Manifesto que buscava pressionar o Senado Federal a aprovar o Projeto de Lei da Câmara nº 53, que atualmente é a LGPD. Ressalta-se que este ato contou com o apoio de diferentes grupos econômicos que tradicionalmente não possuem afinidade, porém se reuniram para um objetivo específico (Bioni, 2021). Acerca da importância da criação desta legislação:

> O Brasil, até agosto de 2018, não dispunha de lei específica para a proteção de dados pessoais. Sua tutela era pleiteada com base em determinadas previsões estabelecidas na Constituição Federal e algumas normas setoriais, que direta ou indiretamente tratam de questões relacionadas à privacidade e aos dados pessoais, como, por exemplo, o Código de Defesa do Consumidor (Lei nº 8.078/90), o Marco Civil da Internet (Lei nº 12.965/14), a Lei de Acesso à Informação (Lei nº 12.527/11) e a Lei do Cadastro Positivo (Lei nº

> 12.414/11). Todavia, esse arcabouço regulatório mostrava-se pouco preciso e não oferecia garantias adequadas às pessoas, o que, além de gerar insegurança jurídica e de deixar informações pessoais mais vulneráveis, acabava tornando o País menos competitivo frente ao cenário externo. (Teffé, 2022, p.04)

No mesmo sentido, para o momento em que a sociedade se encontra, a LGPD e a GDPR possuem um grande papel, visto que atuam como instrumentos capazes de proporcionar uma maior proteção e consequentemente uma garantia da pessoa humana. Isso porque promovem um notável controle dos dados que são tratados, estipulam deveres e responsabilidades para os indivíduos ou empresas que desempenham a atividade de tratamento dos dados, o que proporciona uma maior segurança para as informações que circulam na rede (Teffé, 2022).

Infere-se também que, diferentemente das legislações brasileiras anteriores sobre o assunto, a LGPD cumpre com um dos desejos do legislador, que é o alinhamento com o padrão europeu, representado pelo Regulamento Geral Europeu de Proteção de Dados, tornando-se um marco legislativo muito importante para o direito digital brasileiro (Teffé, 2022).

Com isso, observa-se que as legislações que tratam acerca da proteção de dados pessoais se encontram em avanço constante, tanto no cenário nacional, quanto no cenário internacional. Por este motivo, é indispensável tecer explanações sobre os dados pessoais sensíveis na era do processamento de informações em grande escala.

2.2 OS DADOS PESSOAIS SENSÍVEIS NA ERA DO *BIG DATA*

Inicialmente, antes de adentrar no contexto específico dos dados pessoais sensíveis, é necessário tecer esclarecimentos acerca da *big data*, que é um grande conjunto de dados que possuem um grande volume e formatos de dados estruturados, que acarreta na dificuldade de processamento destes dados por um software tradicional. Destaca-se, também, que a *big data* possui três características especiais, que são, o alto volume de dados, alta velocidade de processamento e atualização destes e a grande variedade de tipos e formatos de dados disponíveis (Cavique, 2014). Quanto a esse grande volume de dados, destaca-se o seguinte trecho acerca da captação destes:

> Na economia digital, o valor dos dados encontra-se relacionado à captura e à mobilização da atenção dos usuários nas plataformas. O ideal é que eles passem o máximo de tempo nesses ambientes, pois, quanto mais engajados, maior será a quantidade de dados acumulados e a acuidade preditiva dos mecanismos algorítmicos, o que, consequentemente, aumentará o valor das receitas dos serviços. Por tal razão, muitas estratégias deste mercado vêm sendo voltadas a desenvolver mecanismos para capturar a atenção de seus usuários, para que eles sejam ativos nas plataformas e para que alimentem o ambiente com informações que, mais tarde, serão tratadas e monetizadas a curto, médio e longo prazo (Teffé, 2022, p.06).

Ademais, "[...] Através do oferecimento de serviços aparentemente gratuitos para bilhões de pessoas, os provedores responsáveis por esses serviços monitoram o comportamento dos usuários, obtendo detalhes surpreendentes [...]" (Teffé, 2022, p. 07). Importante destacar a dependência dos indivíduos para com os meios de internet, que é assim explicada:

> No contexto atual, verifica-se o quão difícil se tornou evitar as estruturas estabelecidas por grandes agentes de tecnologia e pelos Estados, seja pela utilidade e pela qualidade dos serviços oferecidos, seja em razão da sua essencialidade para o exercício de direitos e deveres como cidadão. Isso pode se tornar ainda mais difícil, inclusive, se as pessoas começarem a depender de redes e algoritmos tanto para tomarem grande parte de suas decisões quanto para contratarem e utilizarem bens e serviços (Teffé, 2022, p. 07).

Para exemplificar o risco da falta de segurança com os dados pessoais, em 2016, na Austrália, a empresa Red Cross Blood Service, responsável pela prestação de serviços de coleta de sangue, sofreu um ataque em seus sistemas de segurança, que resultaram no vazamento de informações atinentes a 550.000 doadores de sangue. Dentre as informações disponibilizadas na internet havia uma que se destacou, pois era sigilosa, visto que ela especificava se determinado doador seria uma pessoa com comportamento sexual de risco. O desfecho desta história, é que a empresa percebeu a gravidade da situação após tomar ciência do ocorrido e, diante disso, pediu desculpas formais aos doadores e forneceu todo apoio para as pessoas que tiveram seus dados violados (Mulholland, 2018).

Nesse contexto, é de suma importância compreender a importância da privacidade no âmbito tecnológico vivenciado pela sociedade, isso porque as consequências trazidas pelo excesso de transparência dos indivíduos possuem uma grande complexidade. Enfatiza-se, principalmente, o perigo que o controle social apresenta para as pessoas, visto que, em decorrência dele, a individualidade de cada cidadão será anulada, aspecto que inviabiliza o livre desenvolvimento da

personalidade. Isso posto, a privacidade é um pilar importante para garantir, ao cidadão, uma esfera privada livre de interferências e manipulações externas, de forma a possibilitar a autonomia das pessoas para a tomada de suas decisões (Doneda, 2021).

No tocante aos dados pessoais, é indispensável tratar sobre a figura dos bancos de dados, haja vista que se encontram no cerne desta matéria. Ao conjunto de informações organizadas seguindo um padrão, é dado o nome de banco de dados, e ele pode ser organizado e administrado com ou sem o auxílio dos meios eletrônicos, porém merece destaque a ampliação inimaginável da potência destes em caso de utilização da tecnologia para realizar a administração. Isto ocorre, pois a tecnologia possibilita o armazenamento e processamento maior e mais rápido das informações, aspecto que possibilita a combinação de dados de várias formas diferentes em pouco tempo, o que seria muito diferente em caso de administração manual (Doneda, 2021).

Assim, se tornou possível o agrupamento das informações em subcategorias, o que torna viável o armazenamento de informações pessoais em grupos delimitados a determinados aspectos da vida do indivíduo em sociedade. Em consequência desse agrupamento, há dois apontamentos a serem considerados, o primeiro é o enfraquecimento da tutela da pessoa, visto que ela ficou submetida a interpretação de contextos setoriais, e o segundo, que é criação de uma categoria específica de dados, denominada dados sensíveis (Doneda, 2021).

Quanto aos dados sensíveis, eles possuem como característica a grande possibilidade de utilização para fins de discriminação ou realização de condutas lesivas ao titular destes, ou seja, esta classificação se demonstra fundamental em razão da existência de um risco maior na utilização deste tipo de informação. Convém destacar que, em determinadas condições, mesmo os dados que não se enquadram na categoria de sensíveis, podem, a depender da forma de processamento adotada, revelar questões consideradas sensíveis (Doneda, 2021).

Nesse sentido, percebe-se que as informações, no meio digital, possuem a característica de um elemento jurídico multifacetado em razão da imprevisibilidade das consequências de sua utilização. Por conta disso, a tutela aplicada deve ser dinâmica, para que seja possível o acompanhamento dos dados durante a circulação, visto que a informação pessoal é considerada uma extensão da personalidade do indivíduo (Doneda, 2021). Quanto a isso, colaciono:

> Torna-se então necessária uma tutela dinâmica, que acompanhe os dados em sua circulação, sem se concentrar no sujeito e nas suas características eminentemente subjetivas (como ocorre geralmente quando se trata do direito à privacidade). A informação pessoal, em um certo sentido, pode ser desvinculada da pessoa: ela pode circular, submeter-se a um tratamento, ser comunicada etc. Contudo, até o ponto em que continua sendo uma informação “pessoal”, isto é, identificando a pessoa a qual se refere, a informação mantém um vínculo indissolúvel com a pessoa, e sua valoração específica tem, como fundamento o fato dela ser uma representação direta da pessoa. Por força deste regime privilegiado de vinculação entre a informação pessoal e a pessoa à qual ela se refere – como representação direta de sua personalidade –, tal informação deve ser entendida, portanto, como uma extensão da sua personalidade (Doneda, 2021, p. 152).

Visto isso, é de suma importância compreender os métodos de processamento das informações, que pode ocorrer de maneira quantitativa e qualitativa, o primeiro é baseado em um processamento de um grande número de dados em menos tempo e, o segundo, este é baseado no uso de técnicas avançadas para a obtenção de resultados mais valiosos com os dados obtidos. Cumpre destacar que, com o desenvolvimento tecnológico, tornou-se possível a combinação dos dois métodos de processamento, o que gera uma base técnica que pode ser aplicada em toda coleta de dados pessoais (Doneda, 2021).

No tocante ao método qualitativo, há diversas técnicas que são aplicadas para tornar cada vez mais efetivo o processamento dos dados. Dentre as técnicas se encontra o *profiling*, que possibilita a criação de uma representação virtual da pessoa, o que gera um grande risco de confusão entre o perfil virtual e a própria pessoa (Doneda, 2021). Quanto a essa técnica:

> Entre estas técnicas, está a elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas. Esta técnica, conhecida como *profiling*, pode ser aplicada a indivíduos, bem como estendida a grupos. Com ela, os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma “metainformação”, que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo. A técnica pode ter várias aplicações desde o controle de entrada de pessoas em um determinado país pela alfândega, que selecionaria para um exame acurado as pessoas às quais é atribuída maior possibilidade de realizar atos contra o interesse nacional, até para finalidades privadas, como o envio seletivo de mensagens publicitárias de um produto apenas para seus potenciais compradores, entre inumeráveis outras (Doneda, 2021, p. 154).

Outra técnica amplamente utilizada é o *data mining*, que se baseia na utilização de instrumentos estatísticos e matemáticos que, através de padrões significativos e

correlações, resultam na busca por um número maior de informações a partir de um material bruto, que é uma grande quantidade de dados. Através desta técnica, torna-se possível a transformação de um grande número de informações brutas e desorganizadas em materiais que apresentam interesse. Cumpre destacar que, em razão da utilização das informações em estado bruto, a possibilidade de obtenção de informações cada vez mais valiosas cresce juntamente com a capacidade de obtenção destas informações utilizadas como base, e esta captação está diretamente ligada ao crescimento tecnológico (Doneda, 2021).

Nesse sentido, tanto essas técnicas mencionadas, quanto outras utilizadas no tratamento de informações, possuem um elemento em comum que merece atenção. Este fator em comum é o distanciamento entre a informação obtida com a anuência da pessoa proprietária do dado e a informação obtida através do cruzamento destes dados. Ou seja, a possibilidade de afastamento, no que diz respeito ao conteúdo, entre a informação inicial e a informação resultado pode ser muito grande e, por vezes, acarretar na diminuição da liberdade do indivíduo em sociedade, visto que os dados pessoais são, em diversas ocasiões, intermediários entre a sociedade e a pessoa. Isso se deve, principalmente, porque os dados obtidos mediante a aplicação das técnicas de processamento acarretam, algumas vezes, na obtenção de informações que não foram autorizadas pelo indivíduo, o que gera, para ele, um descontrole quanto ao que a sociedade sabe sobre ele (Doneda, 2021).

Quanto aos dados efetivamente sensíveis, cabe destacar que a classificação e identificação dos dados que podem ser considerados sensíveis depende de fatores diretamente relacionados à cultura e legislação de cada local. Por conta disso, é de grande importância levar em consideração, para a classificação, parâmetros como a natureza e as características de uma determinada informação, bem como o contexto onde ela está inserida. Também é importante observar as consequências da utilização destas informações, tais como a potencialidade de discriminação ou utilização destas informações para fins ilícitos contra a pessoa que se refere os dados (Teffé, 2022).

Outro aspecto a ser considerado são as intenções do agente que realiza o tratamento dos dados, visto que seus objetivos influenciam diretamente na obtenção destes dados, que, inclusive, podem ser armazenados para utilização futura, com o auxílio de técnicas mais avançadas, para obter dados que podem ser considerados valiosos e sensíveis (Teffé, 2022). Para melhor elucidar este aspecto:

> Intenções são, em geral, importantes no processo de decisão se os dados que estão sendo tratados podem ser considerados sensíveis. Para se analisar a questão, mostra-se relevante verificar, entre outros aspectos, o histórico do agente, o potencial de ganho comercial ou financeiro com o tratamento e se a intenção declarada é, de fato, objetivamente verificável. Imagine, por exemplo, um controlador que coletou grandes quantidades de dados pessoais relativos a certas características comportamentais de determinadas pessoas, na esperança de que alguma forma de tratamento de dados possa estar disponível no futuro, permitindo tirar conclusões sobre o estado de saúde dos titulares dos dados. Usar uma definição muito restrita para os dados sensíveis pode significar que o referido tratamento não será considerado de caráter sensível, visto que, no momento, não se pode tirar tais conclusões. Essa maneira de definir os dados pessoais pode ser insuficiente, dada a probabilidade de que futuras evoluções tecnológicas tornem esses dados sensíveis. Diante disso, uma definição que ignore completamente o propósito do agente não parece ser adequada, uma vez que ele poderá reunir dados não sensíveis esperando que futuras evoluções tecnológicas permitam acessar conclusões sensíveis sobre seus titulares (Teffé, 2022, p.37).

Cabe destacar que as informações sensíveis sobre as pessoas podem ser obtidas através de metadados, que são gerados por praticamente todos os dispositivos tecnológicos, tais como *smartphones*. Isso ocorre devido ao uso cada vez mais frequente destes dispositivos por crianças e adultos e, principalmente, pela capacidade de armazenamento presente neles. Um exemplo disso são as fotografias, além de ficar armazenada a imagem capturada, dados como o modelo da câmera, data de criação, localização, e outros, ficam registrados no armazenamento do aparelho (Teffé, 2022).

No mesmo sentido, os conteúdos captados por *smartphones* durante seu uso podem revelar diversos aspectos sensíveis, tais como experiências de vida, emoções, condições médicas, orientações sexuais, condições financeiras, entre outros aspectos, tudo isso obtido através de comunicações realizadas durante o uso desse aparelho. Ainda que não haja uma efetiva comunicação entre pessoas durante o uso, também é possível que o dispositivo colete informações relacionadas a atividades da vida cotidiana, localizações frequentadas pelo indivíduo e gostos pessoais apresentados por ele (Teffé, 2022).

Diante dessa vasta possibilidade de captação de informações, mostra-se difícil pensar em um dado pessoal que não seja potencialmente sensível, isso se deve aos conjuntos informacionais que se encontram em grande evolução. Eles permitem que, a partir dos dados pessoais coletados, os agentes de tratamento encontrem conclusões sensíveis em um ritmo cada vez mais acelerado (Teffé, 2022).

Realizadas estas explanações, é possível inferir a capacidade de dano do vazamento e processamento irregular de dados pessoais, visto que a captação e processamento de dados se encontra em constante evolução, o que torna cada vez mais fácil a violação do direito à privacidade de um indivíduo mediante o processamento irregular de dados.

3 A RESPONSABILIDADE CIVIL DA REDE SOCIAL NOS VAZAMENTOS DOS DADOS PESSOAIS

Este capítulo visa estudar como ocorre a responsabilização civil das redes sociais no ordenamento jurídico brasileiro. Para que isso se torne possível, será apresentada uma construção acerca da responsabilização civil na Lei Geral de Proteção de Dados, a fim de abordar as peculiaridades apresentadas pela referida legislação, visto que, apesar desta possuir diversos aspectos que se assemelham com a legislação consumerista, também há alguns pontos que são característicos dela, os quais devem ser analisados para que o estudo se demonstre completo.

Após este estudo, será apresentada a responsabilização civil das empresas por vazamentos de dados pessoais sensíveis, momento em que serão explorados os aspectos principais quanto à responsabilidade de tratamento correto e quanto à dificuldade de quantificação do valor da indenização. No segundo momento, será feita uma pesquisa jurisprudencial realizada no âmbito do Superior Tribunal de Justiça, que tem como principal objetivo, abordar a responsabilização civil de empresas pelo vazamento de dados pessoais na prática, a fim de avaliar a eficácia desta.

3.1 A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

Esta passagem da pesquisa possui como objetivo discorrer como ocorre a responsabilidade civil na Lei Geral de Proteção de Dados, Lei nº 13.709/18, explicará a responsabilidade civil de um modo geral e, em prosseguimento, analisará os dispositivos legais atinentes à responsabilidade civil existentes no referido diploma legal.

Antes de adentrar na responsabilidade civil na LGPD, é de suma importância compreender que a responsabilidade civil busca restaurar o equilíbrio moral e patrimonial que foi afetado pelo dano causado, por meio de uma redistribuição de riqueza condizente com as previsões legais (Diniz, 2023).

Visto isso, a responsabilidade civil, de um modo geral, possui divergências quanto a sua definição, visto que há autores que a classificam com base na culpa, no sentido de uma resposta pelas consequências das ações realizadas, caracterizada pela obrigação de reparar o dano causado a determinado indivíduo. Outros doutrinadores, que compõem a vertente moderna, sustentam que a responsabilidade civil não se detém apenas à questão da culpabilidade, visto que é mais ampla, pois

deve visar uma repartição de prejuízos, que deve proporcionar um equilíbrio entre os interesses e os direitos. Em razão desta vertente moderna, surgem os dois polos da responsabilidade civil, o polo objetivo e o subjetivo, onde o primeiro aborda a questão do risco criado e o segundo se fundamenta na culpa (Diniz, 2023). Diante disso, o conceito que melhor define a responsabilidade civil é:

> Com base nessas considerações poder-se-á definir a responsabilidade civil como a aplicação de medidas que obriguem alguém a reparar dano moral ou patrimonial causado a terceiros em razão de ato do próprio imputado, de pessoa por quem ele responde, ou de fato de coisa ou animal sob sua guarda ou, ainda, de simples imposição legal. Definição esta que guarda, em sua estrutura, a ideia da culpa quando se cogita da existência de ilícito (responsabilidade subjetiva), e a do risco, ou seja, da responsabilidade sem culpa (responsabilidade objetiva) (Diniz, 2023, p. 20).

Cumpre salientar que a responsabilidade civil possui requisitos que devem ser observados, que são a existência de uma ação, seja ela omissiva ou comissiva, qualificada juridicamente como um ato licito ou ilícito, a ocorrência de um dano, seja ele moral ou patrimonial, à vítima do ocorrido, e o nexo de causalidade entre o dano e a ação (Diniz, 2023).

Nesse sentido, é de muita importância discorrer, pormenorizadamente, acerca desses requisitos. Inicialmente, a ação omissiva ou comissiva possui como aspecto principal a previsão legal de um ato lícito ou ilícito, visto que, no fundamento da responsabilidade há, além da culpa, o risco. Diante disso, além da ideia básica advinda da culpa, que é a existência de um dever de indenizar pela prática de um ato ilícito, há também o dever de reparar em razão do risco, que ocorre em situações específicas quando o indivíduo age de acordo com a lei, porém acontece determinada situação indesejada e este possui o dever de indenizar por ter assumido o risco do ato. (Diniz, 2023).

Ademais, ressalta-se que o artigo 927 do Código Civil prevê, além da responsabilidade de indenizar em casos de ato ilícito previsto nos artigos 186 e 187 da mesma legislação, o dever de indenizar em casos onde o indivíduo assume o risco, o que se depreende do parágrafo único do referido artigo: “Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem” (Brasil, 2002, n.p).

Destaca-se que a culpa anteriormente mencionada é em sentido amplo, ou seja, compreende tanto o dolo – violação intencional –, quanto a culpa em sentido estrito – imprudência, imperícia e negligência – e, diante disso, infere-se que, mesmo em casos onde o agente causador do dano não possuía a vontade de causar determinada situação, deve haver a responsabilização civil (Diniz, 2023). Ainda, cumpre ressaltar o duplo fundamento do ato ilícito:

> É mister esclarecer, ainda, que o ilícito tem duplo fundamento: a infração de um dever preexistente e a imputação do resultado à consciência do agente. Portanto, para sua caracterização, é necessário que haja uma ação ou omissão voluntária, que viole norma jurídica protetora de interesses alheios ou um direito subjetivo individual, e que o infrator tenha conhecimento da ilicitude de seu ato, agindo com dolo, se intencionalmente procura lesar outrem, ou culpa, se consciente dos prejuízos que advêm de seu ato, assume o risco de provocar evento danoso. Assim, a ação contrária ao direito, praticada sem que o agente saiba que é ilícita, não é ato ilícito, embora seja antijurídica. P. ex.: se alguém se apossa de um objeto pertencente a outrem, na crença de que é seu; se A não paga o que deve a B porque, por equívoco, considera cancelada sua dívida. Dever-se-á, então, verificar se o agente é imputável, para efeitos de responsabilidade civil e se, em face da situação, podia ou devia ter agido de outra maneira. Fácil é denotar que a ilicitude e a culpa são conceitos distintos, embora em certo sentido complementares do comportamento do agente (Diniz, 2023, p. 22).

Nesse mesmo sentido, o ato ilícito é previsto nos artigos 186 e 187 do Código Civil, que prenunciam as possibilidades de ocorrência de um ato ilícito civil. O primeiro artigo prevê os principais requisitos para a configuração do ato ilícito e o segundo preconiza que, nos casos onde um indivíduo titular de direito, ao exercer esta capacidade, age contra os limites da boa-fé, fins econômicos, sociais e bons costumes, também pratica ato ilícito (Brasil, 2002).

No tocante ao dano, este se trata de um prejuízo, tanto patrimonial quanto extrapatrimonial, causado à vítima do ocorrido, e que deve ocorrer em decorrência do ato comissivo ou omissivo do agente praticante da ação ou, também, por fato de coisa a ele vinculada. Salienta-se que o dano é um elemento indispensável para a responsabilidade civil, visto que esta inexiste sem ele (Diniz, 2023).

Outro requisito é o nexo de causalidade, elemento que interliga a ação e o dano, responsável por estabelecer a necessidade de existir um vínculo entre a ação realizada pelo réu e o dano sofrido pelo autor. Ressalta-se que, caso não exista este requisito, não haverá responsabilidade civil, como exemplo disso destaca-se a causas de caso fortuito e força maior (Diniz, 2023).

No tocante à responsabilidade civil especificamente da LGPD, faz-se necessário discorrer acerca da criação da referida legislação, que surgiu em decorrência de diversos debates que proporcionaram a chegada da sua redação. Um deles é a definição do modelo de regime de responsabilidade civil que, na primeira versão do anteprojeto, era objetiva, visto que apresentava o tratamento de dados como uma atividade de risco (Bioni; Dias, 2020).

Nesta linha, a proposta da LGPD como lei foi ao Senado Federal com a previsão de que os agentes da cadeia de tratamento de dados respondem independentemente de culpa pelos danos causados. Destaca-se que esta previsão, que eliminava a culpa como um pressuposto para a responsabilidade civil, foi retirada da redação final da Lei Geral de Proteção de Dados (Bioni; Dias, 2020).

No entanto, a responsabilidade civil que é prevista na LGPD em vigor, prevê a responsabilidade civil em seu artigo 42, onde determina que o controlador ou operador terá a obrigação de reparar o dano causado a outrem, desde que aqueles estejam desempenhando uma atividade de tratamento de dados pessoais sensíveis. Cabe destacar que o mesmo dispositivo legal fixa que o dano pode ser tanto patrimonial, quanto extrapatrimonial, o que torna visível a possibilidade de dano coletivo ou individual (Brasil, 2018).

Em razão disso, detecta-se a existência de um dever imputado ao controlador ou operador de dados, que é o dever de segurança esperada daqueles que trabalham profissionalmente com o tratamento de dados, visto que a expertise para tratar corretamente os dados e preservar a privacidade dos titulares é presumida (Miragem, 2021).

Nesse sentido, constata-se que o nexo de causalidade da responsabilidade civil na LGPD, se encontra na falha do agente de tratamento de dados. Ademais, é desnecessária a discussão acerca da existência de dolo ou culpa na conduta do agente, visto que a mera constatação do tratamento irregular já é suficiente para a existência do dever de indenizar, portanto, é possível até a inversão do ônus da prova em favor do titular dos dados (Miragem, 2021).

Cumpre salientar que esta inversão do ônus da prova é prevista no artigo 42, §2º da LGPD, que prevê a ocorrência desta inversão em casos onde “for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa” (Brasil, 2018, n.p).

No tocante ao tratamento irregular dos dados pessoais, este é previsto no artigo 44 da LGPD e leva em consideração a velocidade de atualização e crescimento das formas de tratamento de dados e os riscos que são intrínsecos à atividade de tratamento, como por exemplo, acesso de terceiros não autorizados aos dados pessoais armazenados (Miragem, 2021). Nesse sentido, destaca-se o referido artigo:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (Brasil, 2018, n.p.).

Diante disso, é necessário analisar se o controlador ou operador de dados teria a capacidade de identificar a necessidade de implementação de uma atualização na técnica utilizada para tratar os dados, visto que, a depender da técnica implementada como forma de atualização, pode acarretar na abertura de um novo risco para a utilização irregular dos dados, o que seria caracterizado como um fortuito interno, um risco inerente da atividade desempenhada, que não afasta a responsabilidade do agente responsável pelos danos causados aos titulares dos dados (Miragem, 2021).

Um dos aspectos principais da responsabilidade civil na LGPD são as técnicas aplicadas ao tratamento disponíveis na época do evento danoso, visto que são capazes de excluir a responsabilidade do controlador ou operador, visto que o dano ocorreu em decorrência do desenvolvimento tecnológico, que possibilitou a obtenção dos dados de forma irregular, bem como seu tratamento indevido, o que gera um desvio da finalidade prevista inicialmente. Isso ocorre, principalmente, em razão do rápido desenvolvimento da tecnologia que, por ser mais veloz, não é acompanhada pelas outras áreas da economia (Miragem, 2021).

No que diz respeito aos agentes de tratamento de dados que respondem pelos danos causados, estes são o controlador e o operador. O controlador é o profissional que decide o que será feito, visto que o artigo 5º, VI da LGPD o define como “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (Brasil, 2018, n.p). Quanto ao operador, ele é o profissional que executa os comandos decididos pelo controlador, já que o artigo 5º, VII da LGPD o descreve como “pessoa natural ou jurídica, de direito público

ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Brasil, 2018, n.p.). Dessa forma, infere-se que, basicamente, o controlador toma as decisões de como os dados devem ser tratados e o controlador executa estes comandos (Miragem, 2021).

Cabe destacar que o artigo 42, em seus incisos I e II prevê a responsabilização solidária do operador e do controlador, respectivamente. O operador, conforme o inciso I, é responsabilizado solidariamente pelos danos no momento em que ele não observar a legislação de proteção de dados ou no momento em que ele descumprir as ordens e decisões proferidas pelo controlador, tendo como requisito fundamental a licitude dessas decisões. No que diz respeito ao controlador, o inciso II estabelece que este agente deve responder solidariamente quando estiver diretamente ligado ao tratamento de dados, restando ressalvados os casos de exclusão de responsabilidade, o que também vale para o operador (Brasil, 2018). A fim de complementar, destaca-se:

> As condições de imputação de responsabilidade do controlador e do operador pelos danos decorrentes do tratamento indevido dos dados serão: a) a identificação de uma violação às normas que disciplinam o tratamento de dados pessoais; e b) a existência de um dano patrimonial ou extrapatrimonial (moral) ao titular dos dados. Para a imputação de responsabilidade de ambos não se exigirá a demonstração de dolo ou culpa (é responsabilidade objetiva). Da mesma forma, é correto compreender da exegese da lei, e em razão da própria essência das atividades desenvolvidas, que responderão solidariamente, de modo que o titular dos dados que sofrer o dano poderá demandar a qualquer um deles, operador ou controlador, individualmente ou em conjunto (Miragem, 2021, p. 496).

Visto isso, torna-se essencial discorrer acerca dos casos de exclusão da responsabilidade dos agentes de tratamento, estas são elencadas no artigo 43 da LGPD, que elenca três hipóteses que, no momento em que provadas pelo controlador ou operador de dados, implicam na exclusão da responsabilidade (Brasil, 2018).

Cumpre destacar que as três possibilidades apresentam duas formas de excluir a responsabilidade, a primeira é o rompimento do nexo de causalidade entre a o ato de tratamento dos dados e o dano experimentado pelo titular, o que pode ser verificado nos incisos I e III do referido artigo. Quanto à segunda possibilidade, esta é a exclusão da ilicitude da conduta, visto que o inciso II do artigo 43 determina que o agente não será responsabilizado no momento em que comprovar que não violou a legislação (Miragem, 2021). Ademais, cabe destacar o seguinte trecho, a fim de

melhor elucidar a exclusão da responsabilidade do agente com base no fato de não ter realizado o tratamento dos dados pessoais:

> A hipótese de demonstrar que não realizaram o tratamento de dados que lhes é atribuído compreende o afastamento daquele determinado controlador ou operador de qualquer atividade de coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de dados, que tenha dado causa ao dano sofrido pelo titular (Miragem, 2021, p. 497).

Dessa forma, é de suma importância destacar que o previsto no artigo 43, inciso II, que prevê a exclusão da responsabilidade por estar de acordo com a legislação, deve ser aplicado em conjunto com os artigos 7º e 6º da LGPD, visto que estes elencam como os dados pessoais devem ser tratados, ou seja, há no primeiro dispositivo, hipóteses de permissão legal para a realização do tratamento dos dados pessoais e, no segundo, os princípios que o tratamento de dados deve observar (Miragem, 2021).

Nos casos de culpa exclusiva do titular dos dados ou de terceiros, hipótese de exclusão prevista no inciso III do artigo 43, é fundamental destacar que o motivo para a realização do dano deve ser dominantemente atribuído ao titular ou ao terceiro, portanto, o agente de tratamento não pode ter contribuição direta ou indireta no dano, ou seja, o controlador ou operador não pode ter participado no tratamento de dados que resultou no dano (Miragem, 2021).

Ademais, salienta-se que, com forte no artigo 45 da LGPD, o tratamento de dados que violam direitos relacionados com relações de consumo, a responsabilização será regida pelas regras previstas no Código de Defesa do Consumidor (Brasil, 2018).

Dessa forma, é possível observar que, apesar de todas as preocupações previstas em favor do titular dos dados, a responsabilidade civil na Lei Geral de Proteção de Dados busca responsabilizar apenas o controlador e operador que participam diretamente no tratamento dos dados pessoais, o que representa alguns aspectos relevantes sobre a eficácia da responsabilização civil no contexto dos vazamentos de dados pessoais sensíveis, que serão analisados posteriormente.

3.2 A (IN)EFICÁCIA DA RESPONSABILIZAÇÃO CIVIL DAS EMPRESAS FRENTE AO VAZAMENTO DOS DADOS PESSOAIS

Diante das explanações realizadas anteriormente, infere-se que a responsabilização das empresas por vazamentos de dados pessoais sensíveis se demonstra como um desafio para a jurisprudência brasileira, visto que, além de ser um tema novo para os tribunais, carrega uma alta carga de volatilidade, o que se deve, principalmente, à característica mais latente da era da informação, que é a rápida evolução dos métodos de utilização do meio *online*. É justamente esta questão que será abordada nesta altura da pesquisa, ou seja, como os tribunais estão decidindo a temática da responsabilidade civil por vazamentos de dados pessoais. Também serão feitos apontamentos sobre formas de ampliar a eficácia da proteção de dados.

Antes de adentar no contexto jurisprudencial, é necessário expor o enquadramento das redes sociais nas espécies de provedores de internet, visto que as redes sociais, como o Facebook e o Instagram, são encaixadas no grupo dos provedores de hospedagem, pois possuem a finalidade principal de divulgar conteúdos produzidos por terceiros, eles são os intermediários entre os criadores e o público geral, oferecem um espaço próprio de armazenamento de arquivos para as pessoas (Colaço, 2015). No tocante ao conceito deste grupo denominado provedores de hospedagem, este é explicado no seguinte trecho:

> Os provedores de hospedagem, do inglês hosting providers, são responsáveis por garantir o armazenamento de arquivos em servidores remotos, possibilitando acesso de usuário contratante, nos termos pactuados. Assim, a função principal dessa espécie de provedores é hospedar páginas ou arquivos de terceiros e disponibilizá-los aos outros internautas, conforme regras de privacidade escolhidas pelo titular dos arquivos (Colaço, 2015, p.10).

Os provedores de hospedagem possuem responsabilidade de empregar as tecnologias adequadas para a prestação de serviços e a resolução eficiente dos problemas que são decorrentes da segurança e da qualidade da prestação, ponto em que se enquadra a defesa contra *malwares* (Colaço, 2015).

É justamente neste sentido que se deve destacar o dever de diligência dos responsáveis pelo tratamento dos dados pessoais, que é caracterizado pela necessidade de cuidado do agente encarregado com os sistemas de tratamento de dados utilizados. O profissional deve analisar criteriosamente o sistema utilizado para

armazenar e tratar os dados pessoais, de forma a se atentar para o possível resultado razoavelmente confiável do tratamento, o que deve afastar, de qualquer forma, a confiança cega no sistema (Frazão, 2019).

Aponta-se que esse dever de diligência impõe ao agente um dever de meio, e não de resultado, visto que o agente só será responsabilizado em casos onde não se demonstrar cuidadoso na escolha do melhor método de tratamento de dados, e não acompanhar o processo de tratamento dos dados (Frazão, 2019).

Ademais, o dever de diligência apresenta uma notável relevância no estudo do tratamento de dados, visto que demonstra capacidade de assegurar que os agentes encarregados do tratamento e da segurança dos dados pessoais tenham uma obrigação compatível com o risco que assumem o que, consequentemente, estimula a busca pelo aperfeiçoamento da segurança dos dados pessoais (Frazão, 2019).

Em linhas gerais, a responsabilidade deve recair sobre o agente encarregado pelo tratamento de dados, pois este é o responsável pela escolha do melhor método de tratamento de dados possível e disponível no momento e, em casos de aplicação do sistema escolhido, também deve acompanhar o processo continuamente, como forma de solucionar o mais rápido possível eventuais imprevistos. Dessa forma, é possível equilibrar a o poder e a responsabilidade encontrados nesta atividade (Frazão, 2019).

No que se refere às vulnerabilidades de um sistema, estas possuem como ponto principal em seu conceito a existência de uma condição que permite que um atacante explore uma falha e viole a segurança. Elas, quando descobertas, são catalogadas em sites, o que permite que o agente responsável pela segurança tome as devidas providências para mitigar os danos que eventualmente possam ser provocados pela falha. Por esse motivo, deve-se compreender que o agente só será responsabilizado se a vulnerabilidade for documentada previamente, o que retoma a ideia de que a responsabilidade decorre de uma obrigação de meio, e não de resultado (Capanema, 2020).

Outro ponto a ser destacado, agora na LGPD, é o fato de que o legislador omitiu um detalhe muito importante quanto a responsabilidade civil, que é a definição da responsabilidade em subjetiva, que depende de comprovação da culpa, ou objetiva, que independe da comprovação da culpa. Apesar do entendimento predominante ser aliado à responsabilidade objetiva, esta lacuna contribui para um possível impedimento de reparação integral dos danos (Gondim, 2021).

No tocante ao dano, os casos onde ocorre o vazamento de dados pessoais são marcados, na maioria das vezes, por um dano extrapatrimonial, visto que atinge um bem imaterial, com exceção dos casos onde o vazamento de dados acarreta em lesões ao patrimônio da vítima, que deverão ser encarados como dano material. Diante disso, surge a necessidade de valoração dos danos extrapatrimoniais, visto que sua quantificação não é uma tarefa simples, pois depende da análise de alguns pontos (Gondim, 2021).

Para que a valoração do dano seja efetiva, ela deve levar em consideração o poder econômico daquele que realizou indevidamente o tratamento dos dados. O valor deve apresentar um desestímulo ao ofensor e, para que isso seja possível, deve ser considerado, ainda que presumidamente, o valor das informações violadas, sob pena de acarretar em um ilícito lucrativo, ou seja, aquele em que é mais lucrativo violar um direito do que investir em formas de evitar a ocorrência de danos (Gondim, 2021).

Uma forma de evitar o ilícito lucrativo, responsabilizar efetivamente as empresas pelos vazamentos de dados e não esbarrar no enriquecimento ilícito, ocasionado por uma quantificação desproporcional, seria a utilização de uma espécie de tutela coletiva, a fim de responsabilizar as empresas a altura dos danos causados, onde haveria duas indenizações, uma destinada ao titular dos dados e a outra destinada a fundos de defesa de direitos difusos (Gondim, 2021).

A fim de estudar a responsabilidade civil das empresas quanto ao armazenamento adequado dos dados pessoais, é de suma importância compreender o posicionamento do Superior Tribunal de Justiça acerca do tema, que, embora recente, já foi tema de debate no referido tribunal. Com isso, a primeira jurisprudência a ser explorada é o Recurso Especial n. 2.077.278/SP, proferido pela Terceira Turma do STJ, da relatora a Ministra Nancy Andrighi, onde foi discutido o vazamento de dados pessoais que ensejaram em uma facilitação para a aplicação do golpe do boleto por terceiros contra o consumidor (Brasil, 2023).

O Recurso Especial n. 2.077.278/SP possui aspectos relevantes para o tema da responsabilização civil por vazamentos de dados pessoais. É de se destacar, primeiramente, que a comprovação de que os dados vazados estavam armazenados no sistema da empresa e, para que isso seja possível, é imprescindível quais dados foram obtidos ilicitamente por terceiros. Ou seja, em casos de responsabilização civil de empresas pela facilitação do vazamento de dados pessoais deve-se analisar pormenorizadamente os fatos concretos devidamente comprovados, visto que o nexo

de causalidade é comprovado pelo fato dos dados vazados estarem armazenados no sistema da empresa (Brasil, 2023).

Ademais, caso não reste comprovado, por elementos objetivos, que determinados dados foram obtidos mediante vazamento de dados ocorrido no sistema da empresa, não haverá responsabilização civil desta. Isso ocorre em casos onde o terceiro utiliza dados que podem ser obtidos por fontes alternativas que não são o sistema da empresa, tais como nome, prenome, estado civil, profissão. Destaca-se, também, que o mesmo pode ocorrer com os dados pessoais sensíveis, visto que podem ser obtidos de outras empresas que o indivíduo possa ter consentido em fornecer estes dados (Brasil, 2023).

Além do mais, o diferencial desta decisão proferida no Recurso Especial se encontra na conclusão de que, em razão da instituição financeira ser a única empresa que possui acesso aos dados relativos às operações bancárias, presumiu-se que estes tenham advindo de uma falha na prestação de serviço que competia a ela, visto que não obteve êxito em cumprir com o seu dever de sigilo (Brasil, 2023). Isso pode ser melhor compreendido no seguinte trecho do julgado:

> [...] 5. Os dados sobre operações bancárias são, em regra, de tratamento exclusivo pelas instituições financeiras. No ponto, a Lei Complementar 105/2001 estabelece que as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados (art. 1º), constituindo dever jurídico dessas entidades não revelar informações que venham a obter em razão de sua atividade profissional, salvo em situações excepcionais. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento de informações sigilosas e causem prejuízos ao consumidor, configura defeito na prestação do serviço (art. 14 do CDC e art. 44 da LGPD). 6. No particular, não há como se afastar a responsabilidade da instituição financeira pela reparação dos danos decorrentes do famigerado "golpe do boleto", uma vez que os criminosos têm conhecimento de informações e dados sigilosos a respeito das atividades bancárias do consumidor. Isto é, os estelionatários sabem que o consumidor é cliente da instituição e que encaminhou e-mail à entidade com a finalidade de quitar sua dívida, bem como possuem dados relativos ao próprio financiamento obtido (quantidade de parcelas em aberto e saldo devedor do financiamento). 7. O tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor [...] (Brasil, 2023, p.1).

Cumpre destacar, também, o Recurso Especial n.º 1.758.799/MG, proferido pela Terceira Turma do STJ, tendo como relatora a Ministra Nancy Andrighi. Este julgado apresenta um entendimento sobre a possibilidade de presunção do dano moral causado ao titular dos dados, em casos onde ocorre a disponibilização ou

comercialização de dados sem o conhecimento do consumidor titular destes dados (Brasil, 2019). Nesse sentido, colaciono:

> [...] 6. O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas. 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor - dentre os quais se inclui o dever de informar - faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa [...] (Brasil, 2019, p.1).

Diante disso, compreende-se que o agente tratador de dados possui o dever de comunicar o consumidor e titular dos dados sobre todas as atividades realizadas com os seus dados quando não solicitadas pelo titular e, por consequência disso, deve haver a comunicação ao titular sobre as informações que são comercializadas com terceiros. Destaca-se que é em razão do descumprimento dos deveres inerentes à atividade de tratamento de informações que o referido julgado visualizou o nascimento do dever de indenizar pelos danos causados ao indivíduo (Brasil, 2019).

Também merece destaque o importante esclarecimento feito nesta jurisprudência, que vai de encontro com o objetivo principal desta pesquisa. Foi dissertado que as informações publicadas por determinado indivíduo em rede social não carregam uma carga de consentimento que possibilite a utilização destas informações para outros fins por terceiros e, por isso, inexiste possibilidade de afastamento da responsabilidade civil daqueles que a utilizarem de maneira indevida sem o consentimento do titular. O mesmo se aplica aos casos em que os

consumidores fornecem dados para a realização de determinada compra com uma empresa, o responsável pelo tratamento das informações deve compreender que o consumidor não anuiu com a divulgação destas informações no mercado, visto que esta deve ser uma anuência expressa, jamais implícita em alguma relação (Brasil, 2019).

Enfatiza-se que, no que concerne à comprovação do dano, no referido Recurso Especial foi entendido que independe de comprovação o dano causado pela comercialização de dados entre empresas sem a anuência do titular dos dados, visto que se trata de um dano moral *in re ipsa*, aspecto muito importante, visto que o titular dos dados naturalmente é a parte hipossuficiente da relação processual (Brasil, 2019).

Cumpre salientar que a responsabilização civil pelo comércio de dados se apresenta como fundamental para a segurança dos indivíduos, visto que as informações de cunho pessoal são muito valiosas no mercado de consumo, apresentam uma utilidade ímpar para todas as partes da relação de consumo, porém, em determinadas situações, pode apresentar situações ofensivas ou desconfortáveis para o titular dos dados (Brasil, 2019).

No cenário da comprovação dos danos morais sofridos pelo vazamento de dados pessoais, é de suma importância destacar que a presunção do dano não é um consenso entre a jurisprudência do Superior Tribunal de Justiça, ela se aplica conforme a realidade do caso concreto, visto que foi entendido, em decisão proferida no Agravo em Recurso Especial nº 2.130.619, que o vazamento de dados pessoais, apesar de ser um acontecimento indesejável no processo de tratamento de informações, não possui a força de, sozinho, acarretar no dever de indenizar, visto que é indispensável a comprovação do dano. No entanto, o caso seria diferente se os dados fossem considerados sensíveis, ou seja, quando se refere à intimidade de uma pessoa. Destaca-se que esse julgado se refere ao vazamento do nome completo, RG, data de nascimento, idade, telefone e informações sobre a contratação de serviço de fornecimento de energia elétrica, os quais foram considerados apenas dados pessoais não sensíveis (Brasil, 2023). Para melhor compreensão:

> [...] O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. Diferente seria

> se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural [...] (Brasil, 2023, p.10).

Dessa forma, a responsabilização das empresas pelo vazamento de dados depende da análise concreta de cada caso, e ser observada a natureza dos dados para a determinação se estes dados possuem aspectos sensíveis ou não. Isso se deve, principalmente ao fato de que, conforme anteriormente exposto, o condão sensível das informações atrai a possibilidade de tornar o dano moral *in re ipsa*, ou seja, que independe da comprovação de dano (Brasil, 2019).

Em suma, verifica-se um atraso da legislação quanto a efetividade da responsabilidade civil no âmbito do tratamento indevido dos dados pessoais sensíveis. Isso se deve, principalmente ao fato de que a atual quantificação do valor de indenização não é capaz de coibir o ilícito lucrativo, pois não apresenta uma forma de reparação paritária com os danos causados.

CONCLUSÃO

O advento das novas tecnologias, gerado pelo crescimento do setor tecnológico, acarretou no surgimento da internet, que proporcionou ao indivíduo uma nova forma de realizar o seu convívio social, o que resultou no surgimento das redes sociais. Em razão disso, o compartilhamento de informações de toda natureza, por milhares de pessoas, tornou-se uma prática comum no meio online. Ocorre que este compartilhamento é feito em sites administrados por grandes empresas, o que acarreta em um grande poder para estas detentoras das redes sociais, visto que o valor econômico das informações pessoais está em crescimento acelerado, o que gera um maior interesse das empresas na captação e tratamento destas informações. Cumpre salientar que as informações pessoais, no momento em que tratadas indevidamente, possuem uma capacidade de dano ao titular significativa, visto que viola a privacidade deste. Com isso em mente, a presente pesquisa tratou sobre a responsabilização civil das redes sociais na proteção de dados pessoais.

No decorrer deste trabalho, buscou-se abordar detalhadamente a problemática da responsabilidade civil das empresas em casos de vazamento de dados pessoais sensíveis e não sensíveis, com especial enfoque no ordenamento jurídico brasileiro e na aplicação da Lei Geral de Proteção de Dados. Além disso, esta pesquisa possibilitou tanto a identificação de diversos aspectos críticos que influenciam na responsabilização das empresas, quanto as nuances legais e práticas envolvidas na proteção dos dados pessoais dos indivíduos.

No primeiro capítulo, foi realizada, em um primeiro momento, uma explanação acerca do desenvolvimento do *homo sapiens* e o paradoxal desenvolvimento das redes sociais. Em um primeiro momento, foi descrito o desenvolvimento do gênero homo, após foi estudado o desenvolvimento da internet e o consequente surgimento das redes sociais, o que foi feito, principalmente, com apoio de obras escritas por Yuval Harari, Pierre Lévy e Manuel Castells. Após, com um teor predominantemente sociológico, foi exposto o paradoxo das redes sociais, onde foram abordados aspectos positivos e negativos proporcionados por ela, o que foi feito, principalmente, com apoio de obras escritas por Zygmunt Bauman e Byung-Chul Han.

O segundo abordou, em um primeiro momento, os marcos legislativos que tratam da proteção de dados pessoais, nacionais e internacionais, com uma base teórica baseada nas obras de Danilo Doneda, Bruno Ricardo Bioni e Têmis Limberger. Após, foi explanado o que são os dados pessoais e a importância do tratamento correto deles, o que foi feito com o apoio de obras de Danilo Doneda e Chiara Spadaccini de Teffé.

O terceiro abordou a responsabilização civil das redes sociais no ordenamento jurídico brasileiro. Em um primeiro momento, foi apresentado um panorama acerca da responsabilidade civil na Lei Geral de Proteção de Dados, o que foi feito com o apoio de obras de Bruno Ricardo Bioni e Bruno Miragem. Após, foram explorados os aspectos principais quanto à responsabilidade de tratamento correto e a dificuldade de quantificação do valor da indenização, o que foi feito com o auxílio de obras de Ana Frazão, Walter Aranha Capanema e Glenda Gonçalves Gondim e, em seguida, foi apresentada uma pesquisa jurisprudencial realizada no âmbito do Superior Tribunal de Justiça, que teve como principal objetivo abordar a responsabilização civil de empresas pelo vazamento de dados pessoais.

Buscou-se responder o seguinte problema de pesquisa: como a responsabilização civil das redes sociais frente ao vazamento de dados pessoais sensíveis poderá dirimir os danos aos seus usuários? Para tanto, construíram-se as seguintes hipóteses: a) a primeira conclusiva que a responsabilização civil é suficiente para a contenção de comportamentos das empresas administradoras das redes sociais que não utilizam todos os meios possíveis de segurança para proteger a segurança de seus usuários; b) a responsabilização civil é insuficiente para a contenção de comportamentos das empresas administradoras das redes sociais que não utilizam todos os meios possíveis de segurança para proteger a segurança de seus usuários.

Dessa forma, refuta-se a primeira hipótese e confirma-se a segunda hipótese, ou seja, verifica-se que a responsabilização civil é insuficiente para a contenção de comportamentos das empresas administradoras das redes sociais que não utilizam todos os meios possíveis de segurança para proteger a segurança de seus usuários. Isso porque ao longo do estudo constatou-se que a aplicação prática da LGPD ainda se encontra em desenvolvimento. Ademais, este cenário carece de decisões que apresentem um real risco para as grandes empresas de tratamento de dados, o que acarretaria em uma maior atenção para o sigilo dos dados pessoais sensíveis.

Cumpre salientar que, apesar de haver presunção do dano moral em casos de vazamentos de dados pessoais sensíveis, diante do entendimento do STJ, há ainda um ponto que dificulta a efetiva responsabilização das empresas: a inexistência da quantificação de um valor indenizatório capaz de desestimular o tratamento irregular dos dados pessoais sensíveis. Isso porque a avaliação do valor dos dados pessoais é uma tarefa difícil, que atualmente padece de parâmetros, o que abre margem para a fixação de valores que não tenham a força de desestimular o tratamento indevido e, ao mesmo tempo, indenizar o titular dos dados.

Cumpre destacar que as empresas responsáveis pelo armazenamento e tratamento dos dados pessoais possuem uma grande quantidade de recursos financeiros, o que torna necessária uma responsabilização civil rígida, capaz de desestimular qualquer forma de facilitação de vazamento de dados, aspecto que pode ser desenvolvido com o avanço do tema nas pautas dos Tribunais Superiores e, principalmente, com a utilização da modalidade de dano coletivo para a responsabilização das empresas, visto que é uma forma de atribuir um valor capaz de desestimular a prática do tratamento irregular, sem esbarrar nos empecilhos apresentados pela indenização individual, tais como enriquecimento ilícito, visto que o valor arrecadado seria revertido para a coletividade.

Ademais, outro aspecto que dificulta a responsabilização das empresas é a vasta possibilidade de disseminação das informações pessoais, visto que um dado pessoal pode ser obtido por diversas fontes diferentes, o que torna excessivamente onerosa a comprovação do responsável pelo vazamento das informações. Isso se deve, principalmente, ao fato de que a coleta de dados no meio *online* é constante, e o armazenamento ocorre em diversas empresas diferentes, sujeitos a várias formas de processamento de dados, capazes de obter várias informações diferentes, como bem apontado na segunda parte do segundo capítulo desta pesquisa.

Dessa forma, é possível concluir que a responsabilização civil atual é insuficiente para a contenção de comportamentos das empresas administradoras das redes sociais que não utilizam todos os meios possíveis de segurança para proteger a segurança de seus usuários, visto que se trata de um tema complexo e multifacetado, que requer uma análise detalhada e específica dos casos concretos. É evidente que a LGPD trouxe avanços para este tema, porém a aplicação prática continua em processo de consolidação. Decisões judiciais recentes mostram uma tendência à proteção dos direitos dos titulares, mas também evidenciam uma

necessidade de criação de uma forma eficaz de quantificação do valor indenizatório, capaz de coibir o ilícito lucrativo.

O papel da quantificação da indenização demonstra-se fundamental, pois, em casos onde o montante indenizatório é superior aos custos de implantação das medidas necessárias para a proteção, há o estímulo da observação do dever de diligência, em razão do afastamento do ilícito lucrativo. Com isso, de modo geral, as empresas serão compelidas indiretamente a agir conforme os ditames da legislação de proteção de dados, e não pouparão esforços e investimentos para garantir a proteção dos dados pessoais sensíveis.

É de extrema importância esclarecer que a indenização deverá observar o tamanho da empresa responsável pelo tratamento dos dados, o valor dos dados, ainda que presumido, e o número de pessoas afetadas. Ademais, a indenização deve ser dividida em dois valores, o primeiro destinado à reparação do dano causado ao indivíduo, e o segundo destinado à sociedade, que será maior e apresentará a característica desestimuladora, pois seu montante será grande o suficiente para superar o valor que seria necessário para tornar seguro o tratamento de dados da empresa. A destinação do segundo valor à sociedade possui um aspecto muito importante, que é a impossibilidade de acarretar enriquecimento ilícito de um pequeno grupo de pessoas que teve seus direitos violados.

Em suma, a responsabilização civil se demonstra insuficiente no afastamento dos ilícitos lucrativos, porém não deve ser compreendida como algo completamente ruim, visto que as possibilidades de evolução são inúmeras, pois se trata de um assunto novo no Direito, que chega aos poucos nos Tribunais Superiores e na Doutrina. Além disso, as redes sociais e a tecnologia no geral se apresentam como uma área muito próspera no Direito, o que abre grandes possibilidades para o desenvolvimento de estudos futuros, bem como o dano coletivo, que poderá ser estudado para fins de aplicação na responsabilidade civil por vazamentos de dados pessoais sensíveis.

REFERÊNCIAS

ALVES, Alexandre; OLIVEIRA, Letícia Fagundes de. **Conexões com a História**. 2. ed. São Paulo: Moderna, 2015.

BAUMAN, Zygmunt; LYON, David. **Vigilância Liquida**. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

BIONI, Bruno Ricardo. Et al. **Proteção de dados: contexto, narrativas e elementos fundantes**. São Paulo: B. R. Bioni Sociedade individual de Advocacia, 2021.

_____, Bruno; DIAS, D. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **civilistica.com**, v. 9, n. 3, p. 1-23, 22 dez. 2020.

BRASIL. **Agravo em Recurso Especial n. 2.130.619/SP**. Relator Ministro Francisco Falcão, Segunda Turma, Superior Tribunal de Justiça, julgado em 07/03/2023, Publicado: 10/03/2023. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023>. Acesso em 19 mai. 2024.

_____. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 02 de abril de 2024.

_____. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 11 de set. 1990. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 2 de abril de 2024.

_____. **Lei nº 9.507, de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Diário Oficial da União, Brasília, DF, 12 de nov. 1997. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l9507.htm>. Acesso em: 2 de abril de 2024.

_____. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União, Brasília, DF, 10 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 19 de maio de 2024.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília,

DF, 23 de abr. 2014. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 3 de abril de 2024.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 28 de setembro de 2023.

_____. **Recurso Especial n. 1.758.799/MG.** Relatora Ministra Nancy Andrighi, Terceira Turma, Superior Tribunal de Justiça, julgado em 12/11/2019, Publicado: 19/11/2019. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700652199&dt_publicacao=19/11/2019>. Acesso em: 16 mai. 2024.

_____. **Recurso Especial n. 2.077.278/SP**. Relatora Ministra Nancy Andrighi, Terceira Turma, Superior Tribunal de Justiça, julgado em 3/10/2023, Publicado: 09/10/2023. Disponível em: <https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202301909798&dt_publicacao=09/10/2023>. Acesso em: 15 out. 2023.

CAPANEMA, Walter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. São Paulo: Escola Paulista da Magistratura (EPM). v. 21, n. 53, p. 163-170, jan./mar. 2020. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/142288. Acesso em: 06/06/2024.

CASTELLS, Manuel. **A sociedade em rede**. Tradução Roneide Venancio Majer. 25ª. Ed. Rio de Janeiro: Paz e Terra, 2023. (A era da informação: economia, sociedade e cultura, v.1).

CAVIQUE, Luís. **Big data e data science**. Boletim da APDIO. Nº 51 (2014), p. 11-14. Disponível em: http://hdl.handle.net/10400.2/3918.

COLAÇO, Hian Silva. Responsabilidade Civil dos Provedores de Internet: Diálogo Entre a Jurisprudência e o Marco Civil da Internet. **Revista dos Tribunais**, v.104, n. 957, jul. 2015.

DINIZ, Maria H. **Curso de direito civil brasileiro: responsabilidade civil. v.7**.: Editora Saraiva, 2023. *E-book.* ISBN 9786553627765. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553627765/. Acesso em: 03 out. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais** [livro eletrônico]. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

FERRAZ, Joana Varon; LEMOS, Ronaldo. **Pontos de cultura e lan houses: estruturas para inovação na base da pirâmide social**. Rio de Janeiro: Escola de Direito do Rio de Janeiro da Fundação Getulio Vargas, 2011.

FRAZÃO, Ana. **Inteligência artificial e direito: ética, regulação e responsabilidade**. Coordenação Ana Frazão e Caitlin Mulholland. São Paulo: Thomson Reuters Brasil, 2019.

GARRIDO, Patricia P. **Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD)**. Editora Saraiva, 2023. *E-book.* ISBN 9786555599480. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599480/. Acesso em: 25 set. 2023.

GONDIM, G. G. A responsabilidade civil no uso indevido dos dados pessoais. **Revista IBERC**, Belo Horizonte, v. 4, n. 1, p. 19–34, 2021. DOI: 10.37963/iberc.v4i1.140. Disponível em: https://revistaiberc.responsabilidadecivil.org/iberc/article/view/140. Acesso em: 6 jun. 2024.

GONÇALVES, Victor Hugo P. **Marco Civil da Internet Comentado**. Grupo GEN, 2016. *E-book.* ISBN 9788597009514. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597009514/. Acesso em: 26 set. 2023.

HAN, Byung-Chul. **Sociedade da Transparência**. Tradução Enio Paulo Giachini. Petrópolis, RJ: Editora Vozes, 2017.

_____.. **Sociedade do Cansaço**. Tradução Enio Paulo Giachini. Petrópolis, RJ: Editora Vozes, 2015.

HARARI, Yuval Noah. **Sapiens Uma Breve História da Humanidade**. Tradução Janaína Marcoantonio. Porto Alegre, RS: L&PM, 2015.

HARTMANN, Fabiano Peixoto (Org.). **Inteligência artificial: estudos de inteligência artificial**. 1. Ed. Curitiba, PR: Alteridade, 2021.

LÉVY, Pierre. A revolução contemporânea em matéria de comunicação. **Revista FAMECOS**, [S. l.], v. 5, n. 9, p. 37–49, 2008. DOI: 10.15448/1980-3729.1998.9.3009. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/3009. Acesso em: 1 maio. 2024.

LIMBERGER, Têmis. Informação e internet: apontamentos para um estudo comparado entre o regulamento geral de proteção de dados europeu e lei de proteção de dados brasileira. Itajaí: **Novos Estudos Jurídicos**. 25. Ed. 2020.

MASCARO, Alysson L. **Filosofia do Direito**. Grupo GEN, 2021. E-book. ISBN 9786559771042. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771042/. Acesso em: 25 nov. 2023.

MENKE, Fabiano. A Proteção de Dados e o Direito Fundamental à Garantia da Confidencialidade e da Integridade dos Sistemas Técnico-Informacionais no Direito

Alemão. **Revista Jurídica Luso-Brasileira**, Lisboa, Portugal, 01, 01, p. (781 à 809), 2019.

MIRAGEM, Bruno. **Responsabilidade Civil**. [Digite o Local da Editora]: Grupo GEN, 2021. *E-book.* ISBN 9788530994228. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530994228/. Acesso em: 09 mai. 2024.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, *[S. l.]*, v. 19, n. 3, p. 159–180, 2018. DOI: 10.18759/rdgf.v19i3.1603. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 28 set. 2023.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

PAIVA, Eduardo de Azevedo. Princípios Gerais de Direito e Princípios Constitucionais. **Normatividade Jurídica**, Rio de Janeiro, 11, p. 51 a 59, 2013.

SNOWDEN, Edward J. **Eterna Vigilância**. Tradução Sandra Martha Dolinsky. São Paulo: Planeta do Brasil, 2019.

TARTUCE, Flávio. **Manual de direito civil: volume único**. 10. ed. Rio de Janeiro: Forense; São Paulo: Método, 2020.

TEFFÉ, Chiara Spadaccini de. **Dados Pessoais Sensíveis: Qualificação, Tratamento e Boas Práticas**. Indaiatuba, SP: Editora Foco, 2022.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. Editora Saraiva, 2022. *E-book.* ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 26 set. 2023.