PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU
PROFISSIONAL EM DIREITO, SOCIEDADE E TECNOLOGIAS
DA ESCOLA DE DIREITO DAS FACULDADES LONDRINA

DANYLO FERNANDO ACIOLI MACHADO

A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS REFLEXOS SOBRE O PODER PÚBLICO

LONDRINA
2024

DANYLO FERNANDO ACIOLI MACHADO

A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS REFLEXOS SOBRE O PODER PÚBLICO

Dissertação apresentada ao Programa de Mestrado Profissional em Direito e Tecnologia das Faculdades Londrina para obtenção do título de Mestre em Direito.

Orientadora: Prof. Dra.: Jéssica Amanda Fachin

LONDRINA
2024

Ficha de identificação da obra

M149l Machado, Danylo Fernando Acioli.
A lei geral de proteção de dados e seus reflexos sobre o poder público / Danylo Fernando Acioli Machado. - Londrina, 2024.
101 f.

Orientador: Jéssica Amanda Fachin.
Dissertação (Mestrado Profissional em Direito, Sociedade e Tecnologias) –Escola de Direito das Faculdades Londrina, 2024.

Inclui bibliografia.

1. Lei Geral de Proteção de Dados. 2. Desafios. 3. Poder Público. 4. Adequação. I. Fachin, Jéssica Amanda. II.

Elaborado por: Fernanda Felite Teixeira
Bibliotecária CRB9 2165/O

DANYLO FERNANDO ACIOLI MACHADO

A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS REFLEXOS SOBRE O PODER PÚBLICO

Trabalho de conclusão de curso apresentado ao Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias" da Escola de Direito das Faculdades Londrina como requisito parcial para obtenção do título de Mestre em Direito.

Orientadora: Prof. Dra.: Jéssica Amanda Fachin

_____
Prof. Dra. Jéssica Amanda Fachin
Faculdades Londrina

_____
Prof. Dra. Renata Capriolli Zocatelli Queiroz
Faculdades Londrina

_____
Prof. Dr. Marcus Geandré Nakano Ramiro
Faculdades Londrina

Londrina, 10 de fevereiro de 2024.

MACHADO, Danylo Fernando Acioli. A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS REFLEXOS SOBRE O PODER PÚBLICO. 101 páginas. Dissertação de Mestrado apresentado ao Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias" da Escola de Direito das Faculdades Londrina, Londrina, 2024.

RESUMO

A dissertação apresentada tem o escopo de abordar a aplicação e reflexos da Lei Geral de Dados ao Estado, de modo que para cumprir a função inicial é abordada a sociedade da informação, discute-se a evolução dos dados pessoais para que chegasse até à função de protagonismo que carrega atualmente. Apresenta-se ao leitor preceitos e conceitos basilares acerca da proteção aos dados pessoais e, por meio de revisão bibliográfica, legislativa e jurisprudencial, demonstra-se que ao Estado é aplicável a Lei Geral de Proteção de Dados. O texto apresenta uma série de dificuldades, riscos e desafios que estão enraizados na Administração Pública e que impedem a real adequação e implementação da Lei Geral de Proteção de Dados ao Poder Público. São apresentas soluções e adequações viáveis para que o Estado possa de fato e de direito implementar e regulamentar a norma geral e salvaguardar o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais. A conclusão é a de que existem desafios latentes com o avanço tecnológico, um deles é a salvaguarda dos direitos fundamentais como a proteção aos dados pessoais, não obstante, as soluções se apresentam viáveis desde que a Administração Pública se afaste do estado de inércia em que se encontra e passe a agir com a proatividade necessária, de modo que sirva como um exemplo para a iniciativa privada e, assim, a evolução contínua seja possível sem esbarrar na inação estatal. Utiliza-se o método hipotético-dedutivo, por meio de pesquisa bibliográfica no modelo teórico-dogmático, valendo-se de axiomas de estudos científicos e doutrinas.

PALAVRAS-CHAVE: Lei Geral de Proteção de Dados; Desafios; Poder Público; Adequação.

MACHADO, Danylo Fernando Acioli. A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS REFLEXOS SOBRE O PODER PÚBLICO. 101 páginas. Dissertação de Mestrado apresentado ao Programa de Mestrado Profissional em “Direito, Sociedade e Tecnologias” da Escola de Direito das Faculdades Londrina, Londrina, 2024.

ABSTRACT

The dissertation presented has the scope of addressing the application and consequences of the General Data Law to the State, so that to fulfill the initial function the information society is addressed, the evolution of personal data is discussed so that it reaches the function of protagonism it currently holds. The reader is presented with basic precepts and concepts regarding the protection of personal data and, through a bibliographical, legislative and jurisprudential review, it is demonstrated that the General Data Protection Law is applicable to the State. The text presents a series of difficulties, risks and challenges that are rooted in Public Administration and that prevent the real adaptation and implementation of the General Data Protection Law for Public Authorities. Viable solutions and adjustments are presented so that the State can in fact and legally implement and regulate the general rule and safeguard the fundamental right to the protection of personal data, including in digital media. The conclusion is that there are latent challenges with technological advancement, one of them is the safeguarding of fundamental rights such as the protection of personal data, however, the solutions are viable as long as the Public Administration moves away from the state of inertia in which it finds itself and begins to act with the necessary proactivity, so that it serves as an example for the private sector and, thus, continuous evolution is possible without running into state inaction. The hypothetical-deductive method is used, through bibliographical research in the theoretical-dogmatic model, using axioms from scientific studies and doctrines.

KEYWORDS: General Data Protection Law; Challenges; Public Power; Adequacy

SUMÁRIO

AGRADECIMENTOS

A gratidão é um dever que precisa ser cumprido como tarefa diária, de modo que após cerca de dois anos de estudo, compete a este momento ou a esta lauda a função a árdua função de não deixar que aqueles que foram relevantes estejam presentes, ainda que de forma simplória e concisa, sem tantas delongas ou devaneios. Rogo para que minha memória não me traia.

Cabe aqui o agradecimento primordial a Deus, pois sem Ele nada seria possível, a Deus reputo a glória, o louvor, a honra e a majestade, agradeço a Ele por ter me dado forças para até aqui chegar, sem a misericórdia e amor divinos seria impossível ante a tantas limitações que carrego.

A minha família merece todo o agradecimento, minha esposa Renata, meus filhos Lara e Heitor, vocês são a razão pela qual eu busco a capacitação e as formas necessárias para que, de algum modo, enquanto aqui estiver sirva de exemplo e, se um dia eu venha a faltar, tenha deixado um legado capaz de gerar mais orgulho do que decepção.

Meu avô, a quem carinhosamente chamo de meu velho, pois como autodidata me incentivou desde a tenra idade a estudar, de modo que durante toda minha criação ensinou que a capacitação e o estudo cabem em qualquer lugar. O senhor é um exemplo para mim, obrigado por me ajudar de todas as formas possíveis, tanto no ensino fundamental, médio, superior, nas especializações e agora no mestrado, espero poder honrá-lo onde quer que eu esteja.

Ao professor Zulmar Fachin que abriu as portas da Faculdades Londrina para mim e que, de tantas formas, me ajudou para que hoje tudo isto fosse possível, pessoa acessível que nos inspira no dia a dia, tanto no âmbito profissional como acadêmico.

Agradeço à professora Jéssica Fachin pela paciência, pela didática, pelo apoio, pelo incentivo e por acreditar que eu pudesse dar algum fruto, seja pelas publicações, pelas aulas, pelas orientações, sempre muito acessível e atenciosa, obrigado por me orientar até aqui.

Aos docentes do mestrado profissional, todos possuem um valor relevantíssimo em minha vida, cito, em especial, dois professores que serviram e servem para mim como inspiração e fizeram com que meus olhos brilhassem ainda mais durante o mestrado, professor Carlos Renato Cunha que consegue ser um referencial teórico e didático ao mesmo tempo, obrigado por ser um exemplo e a professora Renata Queiroz que fez com que despertasse meu interesse pela proteção aos dados pessoais, em especial no âmbito do poder público, ainda que de tenra idade, carrega consigo um conhecimento vasto, além do fato de que suas publicações sempre serviram para que pudesse enriquecer meus trabalhos. Obrigado a todos.

Sei estar abatido, e sei também ter abundância; em toda a maneira, e em todas as coisas estou instruído, tanto a ter fartura, como a ter fome; tanto a ter abundância, como a padecer necessidade. Posso todas as coisas em Cristo que me fortalece.

Filipenses 4:12,13.

INTRODUÇÃO

A presente dissertação tem o escopo de abordar novas tecnologias sob uma ótica jurídica, de modo a evitar a generalização, buscar-se-á no trabalho proposto apresentar uma análise sobre a proteção de dados pessoais, no Brasil, em especial sobre a Lei Geral de Proteção de Dados.

Assim, dentro da proposta apresentada, como dito, será feita análise sobre a Lei Geral de Proteção de Dados e, buscando afunilar o tema, será discutida a aplicação da proteção aos dados pessoais e sua aplicação ao Poder Público, enquanto agente que trata e angaria de forma massificada dados pessoais e que não pode se furtar ao cuidado com os dados pessoais, ainda que no exercício da função estatal.

O capítulo inicial do trabalho proposto abordará a sociedade da informação, fazendo análise, inclusive, no âmbito da União Europeia, partindo da premissa de que fatos históricos e mudanças sociais foram capazes de impactar o direito, ou seja, o universo jurídico, de modo tal que há necessidade de estudo sobre os temas para que seja possível o discernimento, posterior, da temática acerca da proteção de dados pessoais junto ao Poder Público.

Por meio de revisão bibliográfica será discutida a formação da sociedade da informação, o modo como a sociedade se porta com o advento e implementação de novas tecnologias, bem como em qual contexto se dá a mudança social, após, serão abordados os desafios existentes na sociedade informacional.

No segundo capítulo serão apresentados os apontamentos iniciais que permeiam a proteção de dados pessoais, com análise sobre os conceitos basilares do tema, em especial, possui o escopo de discutir em qual o contexto em que se insere a proteção aos dados pessoais, o que os dados pessoais representam no presente século, a evolução histórica que permeia o tema e demais apontamentos que sejam necessários para introduzir o leitor ao tema. Ressalta-se que o segundo capítulo tem a finalidade de apresentar uma real evolução histórica da análise sobre a temática dados pessoais, sem deixar de, posteriormente, tratar acerca dos dados pessoais na atualidade e o seu regramento.

O capítulo seguinte terá a função de discutir a aplicabilidade da proteção de dados pessoais, ou seja, da Lei Geral de Proteção de Dados ao Poder Público, posto que este, como susodito, acaba por tratar e angariar dados pessoais de forma massificada, uma vez que em vários âmbitos da Administração Pública há o cadastro com os dados pessoais, inclusive dados sensíveis, sob a detenção da Administração, fator que faz com que seja necessária uma análise

técnica sobre medidas a serem tomadas e até penalidades possíveis em caso de desrespeito à norma geral e direito fundamental, qual seja, a proteção de dados pessoais, inclusive nos meios digitais.

O terceiro capítulo ainda terá a finalidade de abordar a responsabilidade da Administração Pública quando do desrespeito à proteção aos dados pessoais, inclusive nos meios digitais, de modo que será abordada, inicialmente, a responsabilidade civil, se objetiva ou subjetiva e, em seguida, com uma análise fundamentada na Constituição Federal, será discutida a responsabilidade administrativa do Poder Público, temas como o direito de regresso em face dos agentes públicos terão apresentação para que o leitor entenda a seriedade e preocupação do legislador e dos tribunais acerca da proteção aos dados pessoais, apresentando-se, até mesmo, hipóteses de condenação por improbidade administrativa em algumas condutas praticadas pelos agentes públicos e agentes políticos.

Em seguida, no último capítulo, ou seja, no capítulo quatro, após ter sido ultrapassada a análise teórica sobre a proteção de dados pessoais, seu regramento geral e a aplicabilidade da tutela, inclusive ao Estado, bem como a responsabilidade civil e administrativa pelo descumprimento da Lei Geral de Proteção de Dados e eventual desrespeito ao direito fundamental à proteção de dados, inclusive nos meios digitais, será feita a análise de casos práticos em que o Poder Público faz o tratamento, colheita e até divulgação dos dados pessoais, sendo demonstrado se há, ou não, cumprimento à norma que estabelece as diretrizes sobre a proteção de dados pessoais.

Será promovida a análise de processos judiciais, alguns em controle concentrado de constitucionalidade, no qual o Supremo Tribunal Federal teve a tarefa de fazer o julgamento envolvendo o Estado, seja em hipóteses de ação ou inação Estatal, ou ainda, pela criação de legislação que desrespeitava o direito fundamental abordado na dissertação. Além de processos que tramitaram no Supremo Tribunal Federal, será abordado caso que foi discutido pelo Tribunal Superior Eleitoral em que foi feita contraponto entre o princípio da transparência e a proteção aos dados pessoais. Ademais, buscar-se-á demonstrar não somente qual a dor, ou seja, qual a problemática, mas será apontado, dentro do Poder Público, situações em que se apresentam soluções para a implementação da Lei Geral de Proteção de Dados, seja por meio de cartilhas e manuais de aplicação, ou até mesmo, em caso no âmbito municipal em que se promoveu a implementação, quais as fases adotadas e a forma para que a Lei Geral de Proteção de Dados fosse de fato e de direito implementada no poder público.

Em seguida, cumprir-se-á a função de apresentar a conclusão acerca de toda a revisão bibliográfica promovida durante a dissertação, de modo a fazer o contraponto entre as dores apresentadas, bem como as soluções discutidas.

Por fim, utiliza-se, a título de metodologia, o método hipotético-dedutivo, por meio de pesquisa bibliográfica no modelo teórico-dogmático, valendo-se de axiomas de estudos científicos e doutrinas.

1 SOCIEDADE DA INFORMAÇÃO E UMA RELEITURA SOBRE OS DADOS PESSOAIS

1.1 A NECESÁRIA RELEITURA SOBRE OS DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO

O mundo vive em constante evolução nas relações sociais e governamentais, ainda que em alguns momentos, neste último caso citado, tem-se um movimento pendular. Em razão disto, verifica-se que com o advento de novas tecnologias, em razão do grau evolutivo que se alcança o avanço tecnológico, há uma necessidade de prestação de tutela para relações antes não existentes ou, ainda que existentes, irrelevantes em dado momento histórico.

Vislumbra-se, destarte, a proteção de dados estar contextualizada no avanço tecnológico advindo com o decorrer da evolução. Dentre o avanço tecnológico, de todas as épocas, existem marcos históricos relevantes, desde o domínio do fogo, a roda, o avanço na medicina, as comunicações, capacidade de navegação e muitas outras, cita-se aqui um dos avanços mais relevantes para o presente trabalho, qual seja, o serviço da *internet,* o qual decorre ainda de outro avanço, qual seja, a criação e utilização de computadores e *smartphones* – ou outros correlatos que possam ser instrumento para a utilização da navegação em rede - *internet*.

Obviamente o avanço de tecnologias acarreta uma verdadeira revolução, a qual impacta diretamente nas sociedades, Klaus Schwab (2016, p. 15) ensina que o termo revolução é uma forma de expressão para uma mudança radical e abrupta, de modo tal que em nossa história as revoluções advindas de novas tecnologias acabam por desencadear uma alteração considerável nas estruturas sociais, bem como nos sistemas econômicos, fala-se ainda que vive-se a Era Digital, a qual só é possível em decorrência das revoluções agrícola e industrial.

Nas palavras do autor:

> "A primeira revolução ocorreu aproximadamente entre 1760 e 1840. Provocada pela construção das ferrovias e pela invenção da máquina a vapor, ela deu início à produção mecânica. A segunda revolução industrial, iniciada no final do século XIX, entrou no século XX e, pelo advento da eletricidade e da linha de montagem, possibilitou a produção em massa. A terceira revolução industrial começou na década de 1960. Ela costuma ser chamada de revolução industrial ou do computador, pois foi impulsionada pelo desenvolvimento dos semicondutores, da computação em *mainframe* (década de 1960), da computação pessoal (década de 1970 e 1980) e da *internet* (década de 1990)".

Após a última revolução citada pelo autor no texto que foi reproduzido, cita-se a existência da quarta revolução industrial, também conhecida como Era Digital. Dessarte, é possível afirmar que o contexto no qual se insere o tema proposto, qual seja, da proteção de dados, está na quarta revolução industrial, ou seja, na Era Digital, a qual, conforme será demonstrado, acaba por elevar a importância dos dados pessoais, seja por questões econômicas ou outras, gerando necessidade de proteção do Estado aos titulares dos dados pessoais em face dos detentores destes.

Ademais, importa salientar que a humanidade tem experimentado um período de mudanças tecnológicas sem precedentes, uma das principais evoluções se faz notar com maior intensidade, qual seja, a comunicação. A *internet* causou uma revolução no compartilhamento de informações e dados, bem como no modo de se relacionar das pessoas. Vive-se num momento em que as tecnologias, como a internet, acarretam um efeito favorável, sendo este a democratização do acesso a dados, serviços, informações, gerando, inclusive, encurtamento entre culturas. (Marineli, 2019, p. 19).

Ora, é possível afirmar que a coleta de dados não é algo recém inventado ou uma atitude inovadora que passou a acontecer a pouco tempo, em verdade, o Estado, a título de exemplo, possui dados e os coleta desde os primórdios, não obstante, é plausível atestar que o avanço tecnológico exponenciou a atividade citada, de tomo tal que o recolhimento, processamento e a análise ininterrupta realizada pela inteligência artificial por meio dos computadores permitem o mapeamento da personalidade das pessoas, ressaltando-se que, diferentemente dos seres humanos, a máquina não se cansa de realizar o processamento de dados coletados. (Queiroz, 2022, p. 34).

A autora ainda vai lecionar no seguinte sentido (p. 35):

> "Pesquisas afirmam que, com 250 curtidas, os algoritmos são capazes de saber mais sobre uma pessoa do que seu companheiro. A tecnologia tem, cada vez mais, ganhado relevância, inclusive no momento de combate à covid-19, com auxílio de inteligência artificial, *drones*, geolocalização. Cumpre ressaltar, contudo, que a proteção de dados

> não deve ser esquecida, devendo, portanto, a privacidade e a saúde interagir e dialogar, sem que uma exclua a outra".

A autora é assertiva quando faz análise sobre o período de luta contra a COVID-19, em que ainda mais dados foram coletados, em cumprimento ao dever legal do Estado de promover a saúde (Queiroz, 2022, p. 35), não obstante, a coleta de dados não pode ser pretexto para descumprir a legislação e afastar a necessária proteção de dados. Outro dado relevante trazido, é o fato de que, com a inteligência artificial, dentro de uma sociedade da informação, é possível que o comportamento manifestado na rede gera uma coleta de dados que, processada pela inteligência artificial, é capaz de analisar o comportamento a ponto de ter vasto conhecimento acerca do usuário pela mera utilização, até mesmo despretensiosa, da rede social.

Neste sentido, fala-se de uma revolução informacional a qual acarretou a sociedade da informação. Sabe-se que a revolução informacional trouxe consigo uma série de desdobramentos, aprimorando as tecnologias já existentes e criando outras, tal fato gera, por si só, efeitos socioeconômicos. Destarte, destaca-se o avanço científico na seara da comunicação, o que faz com que a sociedade industrial seja fortemente passível de influência pela sociedade da informação. (Lisboa, 2006, p. 2).

Quando se fala em sociedade da informação é importante entender que a colheita de dados ou transferência de informações pode ocorrer por meio da comunicação entre os atores que estão na rede informacional. Quanto a isto, importante mencionar que a tecnologia da comunicação pode acarretar uma autocomunicação de massa, ou seja, aquele que pode potencialmente alcançar um nível de audiência global, a título de exemplo, um vídeo no *Youtube*. (Castells, 2009, p. 87-88).

Neste sentido, tem-se que o avanço tecnológico, em especial nas comunicações, é capaz de acarretar mudanças consideráveis nas relações sociais e na forma como os dados e informações ultrapassam fronteiras com uma velocidade incontrolável, razão pela qual em certo momento surge a discussão sobre a colheita, domínio e titularidade dos dados, em especial, os dados pessoais.

Deste modo, é necessário entender que o momento hodierno em que a sociedade global se situa requer uma proteção de dados mais robusta e assertiva, em especial pela notória dependência das pessoas em relação à tecnologia, neste sentido, Selma Carloto (2021, p. 20) assevera que:

> "A tutela dos dados da pessoa natural é indispensável em um período atual, com a rápida evolução tecnológica e a globalização, além da crescente coleta e compartilhamento sem freios dos dados pessoais. Cada vez mais as pessoas estão dependentes da tecnologia e disponibilizam seus dados pessoais de forma pública e global. As relações passaram a ser marcadas pela inteligência artificial (inteligência similar à humana e exibida por mecanismos ou por *softwares*), *Big data* (megadados ou grandes dados) e internet das coisas (que se refere à interconexão digital de objetos cotidianos com a internet".

É possível afirmar, contextualmente, que a sociedade da informação torna-se uma sociedade na qual o uso da tecnologia, em especial, a utilização de instrumentos e operações na *internet*, ou seja, quando conectadas, faz com que as pessoas ou usuários passem a compartilhar seus dados desenfreadamente, em alguns momentos, de forma até mesmo irresponsável, posto que alguns aplicativos pugnam por dados que são irrelevantes ou até desconexos com a finalidade pretendida pelo usuário, ainda assim, para ter mais e mais acesso, o usuário cede seus dados.

Em verdade, pode-se afirmar que houve uma revolução tecnológica e acerca da citada revolução tecnológica e suas decorrências, tem-se que houve uma transformação inevitável na sociedade que altera consideravelmente a maneira como vive a sociedade, como esta trabalha e os relacionamentos, neste sentido Klaus Schawb (2016, p. 11):

> "Atualmente, enfrentamos uma grande diversidade de desafios fascinantes; entre eles, o mais intenso e importante é o entendimento e a modelagem da nova revolução tecnológica, a qual implica em nada menos que a transformação de toda a humanidade. Estamos no início de uma revolução que alterará profundamente a maneira como vivemos, trabalhamos e nos relacionamos".

Ainda, acerca do contexto no qual se encontra a sociedade da informação, os dados pessoais e sua proteção, conforme já citado, tem-se que existe uma afetação socioeconômica em razão do advento das tecnologias de comunicação que acarretam o trânsito fluído de dados e informações. Neste ponto, Shoshana Zuboff aborda o capitalismo de vigilância, o qual procura ter previsibilidade para modificar o comportamento humano como forma de produzir renda e controlar o mercado. (Zuboff, 2018, p. 18).

Neste sentido, ou seja, acerca do valor econômico que se outorga aos dados e à sociedade da informação, vale trazer os ensinamentos de Zigmunt Bauman (2008, P. 20), o qual, leciona que numa sociedade de consumo, aplicando-se no caso em estudo, uma sociedade que consome o que a internet proporciona, não é possível se tornar um sujeito sem antes ser, em verdade, mercadoria, de modo que "a subjetividade do sujeito, e a maior parte daquilo que

essa subjetividade possibilita ao sujeito atingir, concentra-se num esforço sem fim para ela própria se tornar, e permanecer, uma mercadoria vendável".

O problema, talvez filosófico, acerca do que se traz até este ponto, é o fato de que a captação de dados e a sua comercialização podem se revelar como problemas de maior magnitude, quando ultrapassam um mero desenlace de relações e da utilização da rede mundial de computadores para uma verdadeira coisificação do indivíduo, mostrando até mesmo um modelo falido, no sentido moral, em que o ser humano deixa de ser considerado, inclusive quanto à sua dignidade, para se tornar um mero produto de mercado, ou seja, uma coisa, perdendo, talvez, um de seus traços mais importantes ou aquele traço que o diferencia dos demais seres, qual seja, a sua humanidade (Teixeira e Passi, p. 121-122).

Dessarte, dentro do contexto em discussão, tem-se que as novas tecnologias e o ciberespaço ensejam mudanças sociais suficientes para que seja necessária a intervenção do direito, o qual traz os novos direitos consagrados em razão deste advento tecnológico, mas não se resume a mera consagração de novos direitos, também tem função de gerar a releitura de direitos já existentes. Por assim ser, urge a necessidade de que o Estado promova a positivação e a tutela quanto aos direitos surgidos em decorrência destas tecnologias, em especial, da *internet*. Fala-se que há necessidade de promover a tutela do indivíduo contra eventuais ingerências dos detentores de poder, os quais incluem até mesmo o Estado, já que os detentores fazem a coleta, em alguns momentos global, dos dados pessoais. (Rodotá, 2014, p. 61)

Deste modo, quanto à proteção dos dados pessoais importa ressaltar a edição da Emenda Constitucional nº 115/2022 elevou a proteção dos dados pessoais, inclusive nos meios digitais ao status de direito fundamental previsto na Constituição Federal, no rol de direitos fundamentais previstos no artigo 5º, inciso LXXIX, o qual estabeleceu que é garantida a proteção de dados, inclusive nos meios digitais, (Brasil, 1988)[1].

Insta mencionar que dentre os direitos fundamentais que possuem uma relevância e sensibilidade maior, encontra-se a privacidade, do qual a proteção de dados é uma decorrência, no que tange ao direito à privacidade, este não se resume à viver sem influência ou interferência do Poder Público ou de outros, seja sobre o aspecto da vida privada ou no íntimo do ambiente familiar, este direito fundamental reside no fato de ser ou dever ser garantida e protegida a

[1] *In casu:* Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

autonomia privada e respeitadas as informações (dados pessoais) que dizem respeito tão somente ao indivíduo ou que só deveriam ser compartilhados quando autorizado ou quando há necessidade comprovada, assim ensina Ingo Sarlet (2021, p. 199-200).

Ainda, acerca do contexto no qual surge a necessidade de proteger os dados pessoais, insta mencionar que a atualidade traz o fato de que há uma nova fase na sociedade, qual seja, a de um capitalismo de plataforma, em que dados são a principal matéria-prima na qual as plataformas são modelo de negócio, dentre as mudanças nas tecnologias digitais, os dados tornam-se cada vez mais centrais para todos os envolvidos na relação capitalista, de modo que a plataforma surge como um novo modelo de negócio, o qual é capaz de extrair, minerar e controlar uma infinitude de dados. (Srnicek, 2016, p. 12)

Ora, dentro da ideia de que há uma nova fase na sociedade, a qual se inspira num capitalismo de plataforma, de modo que os dados são a matéria-prima, inspirando um verdadeiro modelo de negócio, insta mencionar que a coleta de dados desenfreada e até predatória promovida por plataformas ou redes como *facebook*, *whatsapp* e *instagram*, são em verdade, remuneradas pelos usuários, já que não faz sentido algum afirmar que tais utilidades proporcionadas pelas citadas seriam gratuitas, já que há um contínuo fornecimento de dados pessoais pelos usuários, é neste sentido que Karina Fritz (2021, p. 114) ensina:

> "O que, de fato, ocorre é que o Facebook cede o uso da plataforma em troca dos valiosos dados pessoais dos usuários e isso configura um contrato oneroso *sui generis*, no qual a contraprestação não se dá em dinheiro, mas na cessão do uso dos dados pessoais, que a empresa converte em milhões de dólares com muita habilidade".

O que acaba de ser trazido à lustre corrobora com a ideia de que hodiernamente a utilização de plataformas faz com que aos poucos ou, às vezes, massivamente o usuário forneça todos os seus dados, de modo tal que não bastando os dados pessoais, as plataformas que oferecem determinadas facilidades acabam por captar os gostos, as vontades, as preferências, quais os desejos, quais ou o que os usuários não gostam e até mesmo preferências que o usuário prefere não externar nas relações diárias, mas que, por meio da inteligência artificial, utilizada nos computadores de captação das plataformas, é possível angariar.

Ademais, não se pode considerar concluída a análise do contexto que permeia a sociedade da informação sem antes tratar do papel preponderante da OCDE (Organização para a Cooperação e Desenvolvimento Econômico), bem como sobre a Convenção 108, a Diretiva

45/1996 e a RGPD (Regulamento Geral sobre a Proteção de Dados), o que se passa a fazer a partir de então.

No que tange à OCDE, tem-se que fora do Brasil, ou seja, no âmbito internacional, foram elaboradas as Diretrizes das Organização para Cooperação e Desenvolvimento Econômico, o que se deu em 1980, as diretrizes mencionadas servem como vetores que possuem um conjunto de regras basilares relativas à proteção aos dados pessoais, bem como, visam dar garantia de um ambiente sólido e seguro para a transferência de dados pessoais entre os países, ressaltando que este é o primeiro texto não vinculativo que analisa as consequências jurídicas decorrentes do processamento de dados pessoais, é neste sentido que Ortigosa (2018, p. 11) ensina, vide:

> "Las Directrices de la OCDE de 1980 suponen el primer texto no vinculante a escala internacional que analiza las consecuencias e implicaciones jurídicas que se derivan del tratamiento de datos personales. Los objetivos principales de este texto son por un lado, establecer una serie de reglas básicas en materia de protección de datos personales que traten de impedir la vulneración de derechos deriva- do del uso ilícito que se pudiera hacer de estos datos, y por otro lado, garantizar un entorno seguro de transferencia de datos personales entre países que logre reducir las restricciones y barreras de circulación de datos. Es decir, se pretendía implantar un sistema uniforme en las distintas legislaciones de los países integrantes de la OCDE en materia de tratamiento de datos personales.
> Es un texto que se caracteriza por su claridad y flexibilidad de aplicación, en él se incluyen gran parte de los principios relativos al tratamiento y derechos de los interesados que se reconocen por parte del actual RGPD. Cabe destacar ade- más que este texto internacional prestó especial importancia a la regulación de las transferencias internacionales de datos, fruto del marcado carácter económico de la Organización que impulsó tales directrices".

Acerca do que ensina o autor acima mencionado, tem-se que, conforme mencionado, as diretrizes possuíam o escopo de implementar sistema uniforme, ainda que nas diferentes legislações dos países membros da OCDE, ressaltando-se, novamente, não ser o texto vinculativo, mas orientativo. Os países que adotaram parcialmente as instruções foram os Estados Unidos, Canadá, Alemanha, Suiça, Austrália e Nova Zelândia, até mesmo a União Europeia adotou parcialmente o modelo trazido pela Diretrizes da OCDE (Queiroz, 2022, P. 38).

A autora citada anteriormente ainda vai fazer levantamento histórico relevante, no qual assim conclui:

> "Em 14 de dezembro de 1990, surge o primeiro documento, em âmbito universal, que estabelece uma lista mínima de princípios relacionados ao tratamento de dados pessoais. Aprovado pelas Nações Unidas e pela Assembleia Geral da Resolução

> 45/95, refere-se aos "Princípios Orientadores para regulamentação dos arquivos informatizados". No Conselho da Europa, entre o final da década de 1960 e o início da década de 1970, começou a ser observada uma preocupação sobre os perigos que as tecnologias de informação poderiam gerar aos direitos das pessoas. Dessa forma, em resposta a essa preocupação, foi emitida a Resolução n. 509, da Assembleia do Conselho da Europa. Esta serviu de prelúdio para a Resoluções (73) 22 e (74) 29, as quais trataram sobre os perigos específicos que poderiam surgir da utilização de dados pessoais pelos setores público e privado".

Deste modo, é possível atestar, pela análise dos dados trazidos, que houve um contexto de preocupação em razão do aceleramento da colheita dos dados pessoais, mencionando-se que a preocupação ultrapassou fronteiras geográficas, fazendo com que os países passassem a discutir sobre a colheita de dados não somente dentro de seus territórios, mas também de seus cidadãos por plataformas ou empresas que estivessem em outros países.

Ortigosa (2018, p. 13) ensina que a Convenção 108 do Conselho da Europa de 1981 foi, em verdade, o primeiro instrumento internacional com caráter vinculante que se ocupou da tarefa de regulamentar de forma expressa a proteção de dados pessoais. Menciona-se que na norma mencionada, de caráter internacional, preceito basilar era o de que a pessoa que se encontra no território de um dos Estados signatários deveria ter respeitados os tratamentos devidos aos seus dados pessoais, demonstrando quais era os direitos e deveres atinentes aos titulares de dados, bem como a responsabilidade daqueles que tratavam os dados pessoais, este é o ensinado do autor citado, vide:

> "El Convenio 108 del Consejo de Europa de 1981 se caracteriza por ser el primer instrumento internacional vinculante que regula de forma expresa la protección de datos personales. El Convenio tiene por objeto garantizar a cualquier persona que se encuentre en el territorio de un Estado Firmante el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto del tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona. (Art.1) Por lo que se refiere al contenido de esta normativa, en esta se especifican de forma clara los principios de calidad del tratamiento de datos, así como las facultades y deberes que ostentas los titulares de los datos y los responsables del tratamiento de datos respectivamente. Se regulan por vez primera los denominados datos sensibles o especialmente protegidos, estableciendo la prohibición de su tratamiento cuando no se den unas garantías jurídicas adecuadas, entre esos datos sensibles, el Convenio incluye los datos relativos a la salud, aquellos que revelen el origen racial, las opiniones políticas, etc. Se hace mención a la necesidad de que dichos datos se traten con las medidas de seguridad más apropiadas y además, se regulan brevemente los llamados flujos trasfronterizos de datos. En último lugar, se alude a la obligación que tiene los Estados de crear o designar una autoridad que se encargue de tomar medidas relacionadas con la protección de datos, autoridad que no deja de ser el germen de lo que hoy conocemos como las Autoridades de Control".

Notoriamente no contexto europeu, passa-se a ter uma preocupação latente com as pessoas que ostentam seus dados pessoais e a forma de tratamento que seria dada por aqueles

que coletam os dados, os tratam e, em determinadas situações, mercantilizam os dados da pessoa humana. Seguindo a linha temporal, necessário tratar, ainda que perfunctoriamente, sobre a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, a qual foi publicada em 1995, tendo sito o primeiro texto vinculativo em nível de União Europeia, o qual regula, de maneira mais direta, o tratamento de dados pessoais, promovendo o estabelecimento de dois objetivos claros, quais sejam, garantir o direito à vida privada no que atine ao tratamento de dados pessoais, sem prejuízo de evitar a livre circulação de dados pessoais entre os Estados que compõem a União Europeia. (Queiroz, 2022, p. 40).

Em verdade, até entrar em vigor o Regulamento Geral de Proteção de Dados Pessoais, o principal instrumento jurídico em matéria de proteção de dados na União Europeia foi a Directiva 95/46/CE, do Parlamento Europeu e do Conselho.

No mais, Renata Queiroz (2022, p. 40), acerca do Regulamento Geral de Proteção de Dados Pessoais (RGPD), ensina que:

> "Por fim, em 2016, o Parlamento Europeu e o Conselho publicaram, no dia 27 de abril, o *General Data Protection Regulation* (GDPR) – Regulamento Europeu de Proteção de Dados (doravante RGPD, na sigla em português) -, o qual tornou-se a regra da proteção de dados essencial a todos os países da União Europeia. Difere da Directiva 95/46/CE por ser diretamente aplicável, estabelecendo um novo modelo de apoio à proteção de dados na Europa. Entre os seus objetivos principais estão a proteção dos direitos e liberdades fundamentais das pessoas singulares, bem como a livre circulação de dados pessoais na União Europeia".

Assim, tem-se que os marcos primordiais para a proteção de dados numa sociedade que se tornou aquele nominada como sociedade da informação foram mencionados, cabendo ainda apontar que, em especial, o RGPD provocou uma verdadeira revolução na cultura organizacional, introduzindo novas obrigados no que tange ao tratamento de dados pessoais e à privacidade dos titulares destes dados, ressaltando que a revolução não se restringiu geograficamente aos Estados membros da União Europeia, posto que organizações internacionais e outros países terceiros também foram afetados (Caldeira, 2019).

Ademais, quanto à RGPD, ante a impossibilidade de tratar deste de maneira completa, iminente mencionar um dos princípios que servem como pilares de sustentação do seu cerne, qual seja, o princípio do *accountability*, deste modo, menciona-se que o RGPD determina que os agentes de tratamento adotem medidas capazes e assertivas para atender ao cumprimento das normas de proteção aos dados pessoais. Deste modo, o princípio em comento aborda as obrigações do controlador de adotar medidas eficazes e capazes de comprovar a observância,

bem como o cumprimento, de maneira ininterrupta das normas de proteção aos dados pessoais, mas não só, cabe ao controlador demonstrar a eficácia das medidas adotadas. Destarte, cabe ao controlador comprovar a eficácia da norma, demonstrando como o agente trata e conduz as atividades no que concerne à proteção dos dados pessoais. Deste modo, cabe a afirmação de que o princípio do *accountability* é responsável por demandar o cumprimento estrito do RGPD. (Queiroz, 2022, p. 42).

Menciona-se, ainda, ter sido a entrada em vigor do RGPD um marco para que todas as empresas passassem a ter responsabilidade civil pelo armazenamento e pela proteção da completude dos dados pessoais que coletam e armazenam, sendo isso decorrência da obrigação de reparar quaisquer danos causados aos titulares das informações que foram inicialmente coletadas e, posteriormente, armazenadas, por óbvio que a responsabilidade se dá quando há uma violação a um direito ou um vazamento, já no que diz respeito aos dispositivos das empresas, o RGPD impõe uma série de deveres e obrigações (Anjos *et al*., 2018).

Conclui-se, quanto ao contexto no qual se encontra a temática proposta, estar a proteção de dados presente no fator do advento de novas tecnologias, a qual advém de mudanças que ocorreram com o decorrer do tempo e, atualmente, possuem capacidade de afetar o contexto socioeconômico, havendo, inclusive, discussão acerca do capitalismo de vigilância, o qual busca angariar dados gerando uma previsibilidade da movimentação social, acarretando na possibilidade de gerar lucros e moldar o comportamento humano.

É neste sentido que foi apresentada a contextualização da sociedade da informação, de onde surge, como se dá o desenvolvimento da informação, dos dados e da legislação internacional que passou a se preocupar com a coleta e tratamento desenfreado dos dados pessoais, de modo tal que foi tratado, em especial, da União Europeia e seu papel de vanguarda no tema. Tendo sido ultrapassada a fase de contextualização, passar-se-á a abordar a sociedade da informação em si, não sobre um viés histórico, mas partindo de uma análise fática e jurídica da realidade de momento em que se trata do tema.

1.2 DESAFIOS DA SOCIEDADE DA INFORMAÇÃO EM RAZÃO NO FLUXO DE DADOS

Neste ponto compete a apresentação ao leitor acerca do que é de fato a sociedade da informação, quais as suas nuances essenciais para o desenvolvimento do presente trabalho, qual a importância da informação, conhecimento e dos dados nesta sociedade.

Importa salientar que o termo sociedade da informação não é recente, em verdade, trata-se de jargão utilizado nos meios de comunicação que acaba por trazer um conceito abstrato, o qual, em sua imprecisão, acaba por gerar lacunas que precisam ser sanadas para evitar eu se torne mera bravata ou jargão de bolso.

Jéssica Fachin *et al.* (2022, p. 3) ensina que alguns termos como Sociedade em Rede, Sociedade da Informação, Sociedade Tecnológica ou ainda Sociedade Digital são usados para abordar, ou seja, identificar o momento histórico que culmina na atualidade, a autora faz um levantamento histórico e ressalta que após 1960 até o momento hodierno as tecnologias desenvolvidas e aprimoradas na área da tecnologia da informação (TICs) fazem com que as nomenclaturas sejam devidamente cunhadas.

Acerca da expressão sociedade da informação, tem-se o ensinamento em artigo publicado nos idos de 2000, no seguinte sentido (Werthein, 2000):

> "A expressão 'sociedade da informação' passou a ser utilizada, nos últimos anos desse século, como substituto para o conceito complexo de 'sociedade pós-industrial' e como forma de transmitir o conteúdo específico do "novo paradigma técnico-econômico". A realidade que os conceitos das ciências sociais procuram expressar refere-se às transformações técnicas, organizacionais e administrativas que têm como "fator-chave" não mais os insumos baratos de energia como na sociedade industrial, mas os insumos baratos de informação propiciados pelos avanços tecnológicos na microeletrônica e telecomunicações. Esta sociedade pós-industrial ou "informacional", como prefere Castells, está ligada à expansão e reestruturação do capitalismo desde a década de 80 do século que termina. As novas tecnologias e a ênfase na flexibilidade, ideia central das transformações organizacionais, têm permitido realizar com rapidez e eficiência os processos de desregulamentação, privatização e ruptura do modelo de contrato social entre capital e trabalho característicos do capitalismo industrial".

Ora, é neste sentido que se pode afirmar que a informação predomina numa sociedade considerada informacional, predomina inclusive sobre os meios de produção e distribuição de bens, de modo que a massificação da informação vale como uma mola propulsora da economia, fazendo com que existam transformações sociais com grande profundidade (Lisboa, 2009, p. 9).

É dentro desta senda que se pode afirmar, novamente, que na sociedade da informação o dado é minério, ou seja, fonte de riqueza, já que as tecnologias recentes acarretaram o aumento da coleta, análise e tratamento dos dados, em especial dos dados pessoais. Ainda, é possível afirmar que na sociedade informacional a captação e geração de riquezas acontecem por intermédio da utilização, coleta, venda e tratamento dos dados pessoais. (Barreto Júnior e Naspolini, 2019, p. 146).

Imperioso mencionar que na sociedade da informação a *internet* causou uma notória revolução científico-tecnológica, criando um cenário capaz de gerar intensas mudanças não só na sociedade, mas no ordenamento jurídico, assim ensinam Caio Cazelatto e Michel Moreno (2016, p. 153):

> "Diante disso, as revoluções científico-tecnológicas, sobretudo após a utilização da internet, criaram um cenário inovador, isto é, o informático, causando intensas mudanças na sociedade e no ordenamento jurídico. É um ambiente repleto de interatividade, capaz de proporcionar aos seus usuários desde a comunicação, o entretenimento, a informação, até um local para se trabalhar. É também um ambiente que promove a personalidade humana a seus usuários, o que justifica a análise dessa temática, uma vez que garantir o acesso à internet é garantir o acesso a formação das pessoas. Esse espaço, ainda tão pouco explorado diante de sua dimensão, além de ter estabelecido mudanças no cenário social, também trouxe conflitos inéditos à ordem jurídica. De imediato, os juristas buscaram solucioná-los com os meios que detinham, os quais, como será abordado, foram insuficientes, emergindo a necessidade de se tutelar esse espaço, assim como sua utilização e acesso, fatos este que só ganharam relevância nos últimos anos".

Em verdade, a sociedade da informação está umbilicalmente ligada ao uso de novas tecnologias, em especial o uso da internet. É relevante trazer os ensinamentos de Marcos Dantas (1996, p. 12-13), o qual leciona no sentido de que a sociedade da informação é aquela que foi alcançada em razão do desenvolvimento do capitalismo contemporâneo, de modo que as atividades humanas determinantes para a economia ou para a vida econômica e social se organizam em volta da produção, processamento, coleta e disseminação da informação, primordialmente com a utilização de tecnologias eletrônicas.

É nesta senda que Castells vai defender que essa globalização virtual, guiada por movimentos culturais e econômicos em vários territórios que acabam por alterar até mesmo tradições, acabam por proporcionar uma nova configuração social que se alinha e se equilibra em volta da *internet,* fazendo com que essa grande rede seja, inclusive, fundamento da sociedade contemporânea, ou seja, da sociedade informacional, a ideia é a de que a sociedade informacional se pauta no conhecimento e na informação, a qual é interligada através de redes tecnológicas que são capazes de fornecer novas capacidades a uma forma já velha de organização social (Castells, 2005, p. 17-18).

Tem-se que a sociedade da informação se dá com uma reorganização da sociedade, a qual fica mais envolta das informações geradas aos milhares, em especial no ambiente virtual, de modo que se favorece uma reconfiguração nas relações estabelecidas entra os grupos e os

indivíduos, o que abrange a comunicação, formas de entretenimento, comércio, participação política, *etc*....

É válido o ensinamento de Yuri Lannes, Jéssica Fachin e Alexandre Veronese (2022, p. 13), quando ensinam que:

> "A atual era é marcada por rápidas transformações tecnológicas e o incremento de elementos ciberfísicos ao dia a dia. Recai, a partir de então, inúmeras preocupações aos estados soberanos e ao cidadão e à sociedade, voltadas para a regulação do ciberespaço e para o desenvolvimento de políticas públicas voltadas à universalização do acesso a internet e para a educação para o exercício da cidadania nos espaços digitais".

Ora, é neste contexto em que a sociedade da informação remonta à uma ideia de uma sociedade que tem grande foco no armazenamento, processamento e distribuição de informação por diversos meios, não obstante, equivoca-se aquele que entende que esse armazenamento, distribuição e processamento se dão tão somente pela via eletrônica ou pela utilização de computadores, em verdade, também pode ocorrer tais ações por meio da rádio, televisão, aparelhos de comunicação e tantas outras formas, ainda, é de se mencionar que pode ocorrer uma mistura, de modo que a colheita se inicie por um meio e a distribuição por outro, enfim. (Siqueira Junior, 2007, 748).

Nas palavras da professora Liliana Paesani (2007, p. 162):

> "A sociedade contemporânea é a sociedade da informação. Nas últimas décadas o mundo vem experimentando notáveis transformações em função da aceleração dos mecanismos de difusão das informações, proporcionada, especialmente, pelo desenvolvimento tecnológico das telecomunicações e da microeletrônica. A facilitação do acesso à informação pelos diversos meios de comunicação, como o rádio, a televisão, os telefones e os computadores – especialmente com o advento de novas tecnologias como a internet, o satélite, a telefonia celular e a rede de fibra óptica mundial -, modificou – e vem modificando – substancialmente as relações sociais econômicas e jurídicas, razão pela qual se pode dizer que a sociedade contemporânea é da informação".

É num mesmo sentido que ensinam Waldman e Matheus (2020, p. 109), vide:

> "No Brasil, foi possível perceber uma preocupação dominante com o uso da informática e a introdução dos computadores nas mais diversas de áreas que envolvessem tecnologia, mas não havia uma clara percepção do que seria a Sociedade da Informação, ou sequer a implantação da comunicação em rede e desenvolvimento dessa ferramenta. Enquanto isso, na Europa, já estudavam esse fenômeno. Todavia, por meio do Decreto n. 3.294, de 15 de dezembro de 1999, foi instituído o Programa Sociedade da Informação, com o objetivo declarado, em seu artigo 1º, de "viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira"

> (BRASIL, 1999, online). O Ministério da Ciência e Tecnologia, por sua vez, foi designado pela coordenação do disposto no referido decreto, quando então tratou do Programa Nacional da Sociedade da Informação, um trabalho iniciado em 1996 pelo Conselho Nacional de Ciência e Tecnologia, com o objetivo de disseminar o uso da tecnologia da informação no país e, nas linhas tênues do desenvolvimento, o intuito principal era garantir condições de competitividade econômica do Brasil nos mercados internacionais".

Conforme já abordado anteriormente, a Europa surgiu na vanguarda da proteção ao tratamento dos dados pessoais, em razão de uma preocupação cirúrgica quando vislumbrou os possíveis riscos advindos da sociedade da informação, ou seja, da forma como a sociedade da informação se comporta por meio de rotinas, não obstante, no Brasil, conforme abordado nas citações anteriores, passou a tratar do tema de maneira mais assertiva quase que de maneira tardia. Ainda assim, é importante ressaltar que a sociedade da informação não é estática, mas dinâmica, evoluindo-se constantemente, fato este que faz com que os operadores de tecnologia e do direito tenham a tarefa árdua de manter-se atualizados.

Não se pode confundir a necessária preocupação com o contexto das relações e o modo de agir na sociedade da informação com um suposto pretexto para evitar que a comunicação ocorra ou para que se inviabilize o avanço de novas tecnologias, inclusive, sabe-se que há uma relação de interdependência entre as comunicações e a democracia. Sabe-se que as novas tecnologias dão contorno robusto à informação, fazendo com que esta se torne uma riqueza fundamental para a sociedade, mas não só, a informação pode ser considerada como a matéria-prima das relações hodiernas, sendo plausível afirmar, inclusive, que a cada dia mais os sujeitos estão numa relação de dependência dos meios eletrônicos, cujo trânsito de informações pessoais, ora autorizadas, ora não, as expõe constantemente a toda a sorte de situações (Bonetti e Zainaghi, 2022, p. 91).

A sociedade da informação possui notórias vantagens, mas uma série de desafios em razão da facilidade de acesso em troca de dados e pelo fluxo de informações que tramitam nas redes e fora delas. A título de exemplo, os navegadores possuem configuração, em regra, para guardar dados que demonstrem a preferência dos usuários, os quais são colhidos com base na atividade daquele que se utiliza do navegador, deste modo, tem-se os *cookies* (vestígios que o usuário deixa pela utilização de sua navegação em rede), estes podem ser utilizados das mais variadas formas, inclusive, possuem valor econômico, já que são, em alguns casos, cedidos de forma onerosa. A questão primordial é que para que tais dados sejam fornecidos deveria se ter uma autorização do usuário, sob pena de se violar o direito da personalidade, qual seja, a

privacidade da pessoa. Ocorre que nos tempos hodiernos é impraticável navegar em rede sem que se utilize de ferramentas como os *cookies*. (Longui, 2020).

O que se pode verificar na atualidade, do que foi demonstrado pela bibliografia trazida, é o fato de que em aplicativos e programas, bem como no acesso a determinadas utilidades são apresentados os termos de uso, mas estes se preocupam, em verdade, com o caráter econômico que se quer alcançar com os dados do usuário, ao invés de ter o verdadeiro senso e preocupação com a autodeterminação informativa, ou seja, com o direito fundamental à proteção dos dados pessoais, inclusive nos meios digitais.

Os desafios notórios da sociedade informacional não se cessam à questão fáticas, mas também a situações jurídicas, já que há necessidade de se garantir a efetividade de direitos fundamentais, entre eles o da privacidade e seu corolário recente, a proteção aos dados pessoais, inclusive nos meios digitais, de modo que diante deste fenômeno informático, cabe aos juristas enfrentarem tal situação, levando em consideração que os avanços da tecnologia da informação passam a propiciar novas relações jurídicas e sociais, inovando a ponto de que deve ser propiciada, de forma assertiva, a tutela de uma denominada integridade virtual da pessoa humana, como um corolário, ou seja, um consectário lógico da cultura da dignidade humana. (Bittar, 2015).

Os desafios apresentados se dão pela maneira de formação da sociedade da informação, a qual se dá dentro de um contexto de desenvolvimento social e econômico em que tanto o armazenamento, como o processamento, transmissão, distribuição, valoração econômica tomam um papel central na atividade do capitalismo, de modo tal que as tecnologias da informação e de comunicações trazem impactos latentes na educação, ciência, saúde, transportes, no convívio social e, em especial, no lazer. As mudanças mencionadas, agindo de maneira sinérgica, acabam por projetar a informação e o conhecimento como elementos essenciais e até estratégicos, não só no ponto de vista econômico, mas também no ponto de vista político e sociocultural. (Fernandes e Neto, 2016, p. 255).

Verifica-se que o lazer, em especial, torna-se uma verdadeira vara de pescar para os coletadores de dados, no âmbito da sociedade da informação, explica-se. Os usuários, em regra, hipossuficientes e sem o conhecimento claro acerca da maneira como seus dados serão utilizados ou até mesmo sem saber que os dados estão sendo coletados, acabam por aceitar todo tipo de requerimento/requisição feita pelos fornecedores de entretenimento que, em verdade, fornecem um entretenimento oneroso, mas como uma maquiagem de gratuidade, como já mencionado anteriormente, posto que há a necessidade cada vez mais do fornecimento de

preferência, opções pessoais, dados pessoais contidos em documentos, estilo de vida, localização *full time*, acessos, lastros etc.

Ora, pode surgir o questionamento do leitor se a informação passou a existir na sociedade após o advento da *internet* ou dessa sociedade pós-industrial, por óbvio que a resposta é negativa, o que mudou foi o papel desempenhado pela informação e pelo conhecimento, Fernandes e Neto (2016, p. 259) têm lição valiosa acerca do tema, *in verbis:*

> "No atual estágio da sociedade, a informação e o conhecimento passaram a desempenhar o papel nuclear nas atividades social e econômica. É inegável que a informação sempre esteve presente na sociedade, todavia, na sociedade da informação ela modifica o seu tempo e o espaço por onde circula. A sua geração, o seu armazenamento e a sua transmissão são imediatos, alterando profundamente as suas formas de produção, posse, propriedade e transmissão, além de modificar o perfil dos seus usuários e os seus modos de convivência. Os riscos da realidade digital, com a sua imensa e crescente quantidade de informações produzidas e transmitidas no mundo, vem causando preocupações e colocado a sociedade, num sentido geral, em situação vigília. Entre os seus aspectos mais relevantes, que causam certa apreensão, pela variedade e profundidade das suas consequências, estão a interatividade generalizada e a separação entre a informação e seu substrato material. Convém ressaltar que, durante séculos, a sociedade humana lidou fundamentalmente com bens corpóreos ou tangíveis e com realidades materiais, preparando os universos econômico, social e jurídico, para lidarem com esse modelo de existência. Todavia, nos dias atuais, a informação dissocia-se do seu suporte físico e se apresenta como algo autônomo e, por isso mesmo, inalcançável para os tradicionais mecanismos de controle. Desse modo, se faz importante considerar como a informação e a comunicação, disponibilizadas atualmente através das diversas estruturas telemáticas, interferem não só nas relações sociais, políticas, econômicas e jurídicas, como também na organização do tempo e do espaço, de modo que diferentes pessoas em diferentes locais estabelecem contatos simultâneos umas com as outras em realidades muito diversas".

O que se tem discutido neste tópico é, além de demonstrar o conceito, apresentar do que se trata a sociedade da informação e quais os seus desafios, já que como em outros momentos, como na revolução industrial em que foi necessário discutir a substituição do homem pela máquina e o problema com o êxodo rural, a cada nova revolução, a cada nova mudança, em conjunto com as benesses da inovação e da tecnologia, sem qualquer passe de mágica, existem situações problemáticas que fazem com que o cenário econômico, cultural, social, político etc., mudem drasticamente, fazendo com que as mudanças nos cenários mencionadas gerem uma consequência no direito que, em seguida, precisa adaptar-se à nova realidade.

Defende-se que com a sociedade da informação a privacidade, num sentido técnico, é capaz de albergar uma sorte imensa de necessidades, a título de exemplo, a liberdade de escolha, busca pela igualdade, não discriminação etc., dentro de um complexo emaranhado de relações

que em alguns momentos ainda se apresentam como uma zona de penumbra para o direito (Doneda, 2006, p. 7).

Outro ponto que é um desafio a ser vencido ou a ser controlado na sociedade da informação é que com o advento das tecnologias recentes com o desenvolvimento de novos aparelhos, *softwares*, o aumento descomunal de redes sociais ao alcance dos usuários, há uma maior gama de possibilidades de compartilhamento desenfreado de dados com dificuldade de fiscalização por parte do Poder Público, por óbvio que as redes sociais possuem notória relevância na sociedade moderna, em especial pela "facilidade" de acesso, já que basta compartilhar seus dados pessoais, muitas vezes os dados pessoais sensíveis e, nestas redes, há milhares e milhares de usuários que ali compartilham da própria vida pessoal com uma possibilidade de interação com usuários de todo o mundo. (Ziegler e Piaia, 2015).

Pierre Levy e Lemos (2014, p. 101) lecionam que "o desenvolvimento de comunidades e redes sociais *on-line* é provavelmente um dos maiores acontecimentos dos últimos anos, sendo uma nova maneira de fazer sociedade". E prosseguem, trazendo o conceito de comunidade social, a definindo como um grupo de pessoas ligadas por intermédio do ciberespaço, de modo que a rede social é um serviço que permite o indivíduo construir perfil aberto ou restrito que articula uma lista de outros usuários e com estes passa a criar certo grau de relacionamento virtual.

A título de exemplo, pode-se mencionar modalidades de redes sociais que, dentro da discussão sobre os desafios da sociedade da informação, acabam por ter influência considerável no que atine ao fluxo de dados e informações repassadas ininterruptamente. Cita-se aqui as mais conhecidas como X (antigo *twitter*); *threads*; *Facebook*; *Whatsapp*; *Telegram etc*..., os quais dedicam seus sistemas para criar uma relação social, no qual o usuário alimenta o próprio perfil e apresente o que tem interesse e, em inúmeros casos, compartilha qual a sua religião, profissão, fotos de suas residências, de seus familiares, conquistas, foto de bens e tantas outras informações que podem ser usadas de maneiras variadas, seja para bom proveito, seja até para atos criminosos, alguns dos compartilhamentos são facultativos, já outros, para a ativação do perfil, a título de exemplo, são demandados como condição de acesso.

Dessa forma, o que se atesta é o fato de que a sociedade da informação faz com que se evolua o conceito da privacidade, o qual deixa de ser mera garantia de sigilo ou anonimato e passa a ser visto de maneira funcional, ou seja, dentro de contextos digitais, virtuais e de rede. (Warren e Brandeis, 2013, p. 2).

Rodotá (2008, p. 28), sobre este desafio iminente que é a manutenção da privacidade numa sociedade informacional, trata de maneira cirúrgica o tema com a seguinte afirmação sobre o que é o direito e continua sendo o direito à privacidade, veja, "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".

Ora, é dentro destes enfrentamentos teóricos que pode se afirmar que a análise bibliográfica trazida até então nos possibilita afirmar que a sociedade da informação pode ser considerada a sociedade da vigilância, em que a todo momento há uma vigilância incessante sobre dados pessoais e até mesmo atos de espionagem.

Vale ressaltar ao menos um exemplo concreto de como se dá a coleta de dados, a empresa *Nike* lançou uma pulseira inteligente chamada de *Nike Fuel Band,* a qual em sua política de privacidade estabelece que o *software* que controla a pulseira pode captar e armazenar hábitos do usuário, tais como localização, percursos traçados e executados, quantidade de gasto calórico diário, dentro outras tantas, ocorre que não fica explícito ou claro da maneira como se espera qual será a forma de utilização dos dados coletados, veja, enquanto para o usuário é mera comodidade, tais dados podem e, normalmente são, compartilhados e utilizados para os mais diversos fins (Nike, 2015). Importante pontuar que o projeto da pulseira foi abandonado pela empresa.

Gustavo Tepedino (2014), já ressaltava que com a diminuição do custo para acessar tecnologia da informação, os acessos e controles, bem como cruzamento e a circulação de dados fluem de maneira célere, cabendo ao estado estabelecer mecanismos de tutela dos direitos fundamentais, em especial quanto aos dados sensíveis, importante ressaltar que cerca de uma década antes da emenda constitucional que consagrou os dados pessoais como direito fundamental o professor citado já defendia se tratar de direito fundamental.

É interessante mencionar que a maioria das empresas de tecnologia ou detentoras das redes sociais e afins são alocadas nos Estados Unidos da América, sendo lá desenvolvidos os produtos com fundamento na legislação americana, não obstante, os usuários são globais, dos mais distintos países, continentes e culturas, assim leciona Eli Pariser (2012, p. 243):

> *"As billions come online in India and Brazil and Africa, the Internet is transforming into a truly global place. Increasingly, it will be the place where we live our lives. But in the end, a small group of American companies may unilaterally dictate how billions of people work, play, communicate and understand the world. Protecting the early vision of radical connectedness and user control should be an urgence for all of us".*

Dentro dos desafios até então trazidos, compete ao Estado, no âmbito interno, promover a tutela de forma assertiva, ou seja, com a eficácia necessária, sem, por óbvio, enrijecer a legislação ao ponto de tornar inviável os benefícios advindos da sociedade da informação, em especial com a *internet* das coisas, bem como com *big data*, os quais serão devidamente conceituados e tratados no momento oportuno, enfim, com a sociedade da informação e as mudanças favoráveis que foram geradas por esta. Notoriamente, não são apenas mazelas que o avanço tecnológico trouxe à sociedade, em verdade, há um rol imenso de benefícios, não obstante, ao trabalho compete apresentar, neste ponto, o que é a sociedade da informação, sua formação, seus desafios e outras nuances cabíveis.

Gomes e Rocha (2017, p. 64), ensinam um fator sobre a sobre o que é a privacidade e qual a consequência que a privacidade faz com a informação, vide:

> "A privacidade retira a informação do domínio público para estendê-la ao indivíduo, notadamente, no que tange a seus dados sensíveis. Controlar as informações acerca de si mesmo implica na construção de um perfil identitário, na medida em que passamos a ser aquilo que nossas informações nos definem. O controle sobre tais dados passa a estar ligado a uma possível área de confronto entre o público e o privado. Não é suficiente nos dias atuais entender a proteção da vida privada como a salvaguarda do indivíduo ensimesmado, acastelado sob a proteção dos muros de seu lar, ao qual se garante o isolamento reflexivo. A segurança do lar não mais protege satisfatoriamente o sujeito e é ineficaz diante de riscos potencializados pela "sociedade de vigilância", riscos tais que poderiam sujeita-lo a uma escolha de minerva: alijar-se do convívio proporcionado pela sociedade em rede, ou abrir mão da proteção aos dados relevantes para construção de sua identidade".

Vislumbra-se que, como tratado de forma pontual pelo autor citado anteriormente, há a necessidade de fazer uma escolha trágica, qual seja, fornecer os dados e viver em rede tendo ao seu dispor as informações e acesso à comunidade ou optar por não fazer isso e viver num quase isolamento social e em apartado não só dos riscos, mas também alheio aos benefícios e, como já dito, ao próprio convívio na sociedade virtual, a qual, inclusive, possui notória influência no mundo físico, de modo que nos momentos de convívio social muito se fala e discute sobre situações ocorridas em rede e, se a escolha for pela não participação das redes, primando pelo não compartilhamento de informações, o ônus certamente não é leve.

No Brasil a população optou pelo compartilhamento de dados, já que é um dos líderes em número de usuários em redes sociais. As redes sociais tornaram-se tão amplas que possuem as mais diversas finalidades. A princípio era apenas uma novidade para se relacionar em rede, contudo, com o decorrer do tempo, se tornou ambiente de compartilhamento de fotos, situações pessoais, vendas de produtos, *marketing,* local de embates ideológicos e políticos etc., o acesso

à internet é algo que também impressiona, já que em 2022 o Governo Federal já apontava cerca de 90% (noventa por cento) dos lares no têm acesso à internet no Brasil (Brasil, 2022).

Ora, quando se tem todo esse percentual de pessoas com acesso à internet e se leva em consideração a quase impossibilidade de viver, atualmente, em apartado às redes, vale mencionar o ensinamento de Arendt (2013, p. 71), quando ressalta que:

> "Viver uma vida inteiramente privada significa, acima de tudo, estar privado de coisas essenciais a uma vida verdadeiramente humana: estar privado da realidade advém do fato de ser visto e ouvido por outros, privado de uma relação objetiva com eles decorrente do fato de ligar-se e separa-se deles mediante um mundo comum de coisas, e privado da possibilidade de realizar algo mais permanente que a própria vida".

Pode-se afirmar que, dentre os desafios do capitalismo de vigilância, até então abordados e discutidos, é valiosa a lição de Costa e Oliveira (2019, p. 24), quando asseveram que a digitalização da vida vem ocorrendo "pelo aprimoramento tecnológico dos dias atuais, com o surgimento de tecnologias cada vez mais ágeis, eficientes e com grande potencial de armazenamento e difusão de informações", de modo que há uma nova forma de interação social, uma nova estrutura cultural, social, econômica e, consequentemente, jurídica.

Assim, vislumbra-se que dentro da sociedade da informação o que se discute primordialmente é qual informação deve ser pública e qual precisa ser mantida em sigilo ou como a informação deve ser tratada, de modo tal que as discussões sobre privacidade se ligam umbilicalmente e progressivamente com a proteção aos dados pessoais, já que estes possuem relevância jurídica, no mais, tem-se que considerável parcela das liberdades individuais dos tempos atuais podem ou são concretamente exercidas em plataformas ou até estruturas nas quais a comunicação e a informação possuem um papel de protagonismo (Doneda, 2019).

Ademais, é na sociedade da informação ou da vigilância em que surgem tecnologias para reconhecimento facial, das mais variadas formas, sejam para ingressar em determinados locais, seja para o acesso às contas bancárias, liberação de acesso ao *smartphone*, criar avatares em redes sociais ou por meio de inteligência artificial para criar imagens alternativas, enfim, ao mesmo tempo que existem tais facilidades seja para entretenimento ou não, é possível afirmar que os usuários passam a entregar dados faciais para terceiros sem sequer saber qual a destinação de tais traços. Utiliza-se o exemplo do risco de criar um avatar pela rede social fornecendo dados e traços faciais com a colheita e posterior uso para acesso a dados bancários, a título de exemplo, ou seja, há uma necessidade veemente de cuidado com as "facilidades gratuitas" geradas na sociedade em rede.

Importa ressaltar que dentro de uma sociedade que alimenta a rede com informações ininterruptamente, há uma possibilidade latente do vazamento de dados, assim como ocorreu recentemente, em que mais de 26 bilhões de registros (dados) foram vazados, entre eles estão e-mails, senhas, telefones, nomes de usuários, endereços, números de cartões, documentos pessoais, ou seja, de alguma forma um número ainda incerto, mas robusto de pessoas de todo o globo terrestre tiveram seus dados vazados, seja pela falta de segurança na tecnologia de informação, seja pela omissão, seja até pela ação, o que será devidamente apurado, o fato que é inalterável é o vazamento de tantos dados (Valor, 2024).

Deste modo, o presente tópico perpassou a conceituação da sociedade da informação ou sociedade do conhecimento, apresentando-a, ainda, ao final da discussão como sociedade da vigilância, ao mesmo tempo, apresentou-se benesses advindas do avanço tecnológico, mas o foco principal foi apresentar os desafios gerados com o avanço das novas tecnologias, como o vazamento de dados, o tratamento indevido, a coisificação das pessoas, o intento econômico e mercadológico incessante que paira sobre as informações, em especial os dados sensíveis das pessoais, a existência de vestígios deixados pelos usuários no uso da rede de computadores, a existência de serviços “gratuitos”, mas que em verdade são onerosos, posto que não pagos em dinheiros, mas com os próprios dados, enfim, discutiu-se e apresentou-se bibliografia sobre o tema, entendendo-se que a partir de então cabe o ingresso efetivo no tema sobre os dados pessoais e o avanço para o próximo capítulo.

Ressalta-se, apenas, não ser o intento do presente tópico o exaurimento do tema, seja na parte conceitual, seja na parte dos benefícios trazidos, ou ainda dos ônus ou desafios gerados dentro da sociedade da informação, defende-se que a apresentação foi feita dentro do que se entendeu relevante para o cerne do presente trabalho.

2 DA PROTEÇÃO DE DADOS PESSOAIS APONTAMENTOS INICIAIS

O segundo capítulo, desta dissertação, possui o escopo de apresentar apontamentos iniciais sobre a proteção de dados pessoais, com enfoque especial no Brasil, em especial, a evolução histórica que permeia o tema e, em seguida, o que os dados pessoais representam no presente século, sendo que a conclusão do capítulo se dará com a análise da aplicabilidade da proteção de dados, inclusive nos meios digitais. Ademais, far-se-ão os apontamentos necessários para introduzir o leitor ao tema.

2.1 EVOLUÇÃO HISTÓRICA PROTEÇÃO DE DADOS PESSOAIS

Nesta fase inicial de discussão, tem-se a necessidade de abordar a evolução histórica acerca da proteção dos dados pessoais, em especial no Brasil, tendo em vista que os dados passaram a ter grande relevância econômica e o seu reconhecimento enquanto direito fundamental recentemente, posto que o advento de novas tecnologias acabou por elevar o patamar de importância dos dados pessoais dentro do contexto social e econômico.

Tem-se que o processo de convergência do ordenamento se potencializou no século XX, com o fim da segunda guerra mundial. Com o desenvolvimento da ideia de um estado social, a norma jurídica assumiu o papel de sedimentar e promover hierarquia de valores, utilizando-se da Constituição, momento em que se verifica a elevação da proteção da pessoa humana. Há um desenvolvimento da proteção à personalidade nos séculos XIX e XX, mas é com a Constituição de Weimar que surge o marco mais característico de proteção à personalidade. (Queiroz, 2021, p. 15).

No âmbito internacional, verifica-se que o um dos marcos iniciais para o estudo sobre direito à privacidade foi uma publicação de 1890, qual seja, um artigo intitulado de *The Right of Privacy,* de autoria de Samuel Warren e Louis Brandeis, o qual foi publicado na revista *Law Review* de Harvard, sendo que este trouxe a ideia de que a privacidade seria o direito de ser deixado só (*right to be left alone*), noutras palavras, direito do indivíduo no qual o Estado deixa de agir para que o indivíduo tenha a liberdade de atuar ou agir como entender. (Neto, 2023, p. 45).

Verifica-se que desde as últimas décadas do século XX, em razão dos passos largos dados com os avanços tecnológicos, seja o surgimento da informática e dos computadores, bem como com a necessidade de registrar, manipular e armazenar dados, houve a necessidade de tutela estatal, posto que quanto maior o tratamento e colheita, também há uma crescente na possibilidade de infração a direitos fundamentais, como a vida privada, a privacidade e os corolários destes. Em razão da iminente lesão aos direitos fundamentais, competiu ao Estado desenvolver uma proteção moderna, específica e eficiente sobre o tema. (Pelcerman, 2022, p. 16).

É salutar mencionar que o Brasil acabou por ter uma criação tardia em relação a normas que tratem de forma adequada a proteção de dados, isso em relação a outros países. No Brasil as primeiras demonstrações de instrumentos que visavam a proteção dos dados pessoais surgem

por meio do *habeas data*, previsto no artigo 5º, inciso LXXII[2], da Constituição Federal, bem como no artigo 43, do Código de Defesa do Consumidor[3], enquanto noutros países, a título de exemplo Suiça e Alemanha, as regulamentações sobre o tema são anteriores ao do Brasil. (Flores e Silva, 2020, p. 2), os mesmos autores, seguem com a linha de pensamento e apontam que:

> "O direito à privacidade é personalíssimo e está estritamente ligado ao direito à intimidade e ao princípio da dignidade da pessoa humana. Por ser um direito fundamental, está previsto em importantes tratados e convenções internacionais, como a Declaração dos Direitos do Homem e do Cidadão (1789), a Declaração Universal dos Direitos do Homem (1948), a Convenção Europeia dos Direitos do Homem (1950) e a Conferência Nórdica sobre o Direito à Intimidade (1967), bem como no Código Civil Brasileiro (2002) e, principalmente, na Constituição Federal do Brasil (1988), que prevê, no art. 5º, inc. X, que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação".

Dalmo Dalari (2002, p. 240-242) faz apontamento relevante sobre a matéria quando faz uma análise sobre o instituto jurídico do *habeas data* no Brasil, mencionando que surge o remédio constitucional na Constituição de 1988 quando houve uma necessidade em razão dos fatos advindos do regime militar implementado anteriormente, de modo que bancos de dados podem ter sido alterados ao alvitre daqueles que regiam o país, com finalidades escusas, de modo tal que a proteção aos dados e o direito à informação verdadeira se coadunaram para que houvesse uma efetiva defesa de direitos, evitando-se o registro indevido de dados quanto aos titulares que foram ou poderiam ser lesados.

---

[2] *In casu:* LXXII - conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

[3] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Ainda que de maneira tímida e implícita, os dados pessoais já eram tutelados, não obstante, de forma explícita, as primeiras legislações que se voltaram à proteção de dados pessoais surgem na Europa, cita-se a Alemanha que publicou a Lei do *Land* alemão de Hesse, a qual tinha por escopo a regulamentação dos bancos de dados informatizados de dados governamentais. (Machado, 2018, p. 123).

A Lei supramencionada foi objetivo de controle de constitucionalidade pela Corte Constitucional alemã, posto que em decorrência da norma, o estado alemão criou censo com mais de uma centena de questionamentos para que o cidadão respondesse ao Estado e todos os dados ficaria sob a guarda deste, o que acarretaria um "Estado superinformado", a Corte qual entendeu pela inconstitucionalidade do texto, por alguns abusos previstos em favor do Estado, nas palavras de Ruaro e Rodriguez (2010, p. 191-192):

> "Este é o marco oficial em que surge da autodeterminação informativa, que seriam, segundo a sentença, o direito dos indivíduos decidirem por si próprios quando e dentro de quais limites seus dados pessoais poderão ser utilizados. A partir desta ideia, o sujeito passa a poder decidir quando e sob que circunstâncias poder-se-á conhecer de seus dados pessoais. Cabe ressaltar que o americano Alan Westin, já em 1967, falava nesta figura jurídica. No entanto, ainda que não desenvolvida originariamente pela Corte Constitucional, a Sentença da Lei do Censo é apontada pela maioria maciça da doutrina como uma referência na proteção de dados pessoais".

A Alemanha foi o berço da legislação acerca da proteção de dados e também do termo autodeterminação informativa, a qual se estabelece pela capacidade do sujeito decidir sobre a exibição e utilização dos seus dados pessoais, ressaltando que o termo autodeterminação informativa não é criada na legislação alemã, mas por meio de uma construção de entendimento judicial, a autodeterminação informativa não é mero poder de decisão do titular, mas também imposição de limites ao Estado tanto na dimensão positiva quanto negativa. (Assmann, 2014, p. 20-21).

Após a Alemanha, ainda há notícias de que a Suécia, em 1973, criou o Estatuto para banco de dados, numa ideia próxima à da Alemanha, visando promover um censo para angarir e deter dados pessoais da população, sendo que no ano seguinte, em 1974, os Estados Unidos da América optaram por introduzir um banco de controle de dados, não obstante, os Estados Unidos optou pela criação com a finalidade de obstar que as agências governamentais tornassem públicos os dados ou os repassassem a terceiros sem prévio conhecimento dos titulares, ideia esta que foi replicada na Lei Geral de Proteção de Dados brasileira. (Tavares e Alvarez, 2017, p. 166).

Verifica-se que a preocupação, inicialmente se dava com banco de dados, não necessariamente com o direito fundamental dos titulares destes dados, Danilo Doneda (2011, p. 96), ensinava que estas leis citadas eram da primeira geração, em suas palavras:

> "A primeira dessas quatro gerações de leis era composta por normas que refletiam estado da tecnologia e a visão do jurista à época, pretendendo regular um cenário no qual centros elaboradores de dados, de grande porte, concentrariam a coleta e gestão dos dados pessoais. O núcleo dessas leis girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle *a posteriori* por órgãos públicos. Essas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, que eram o destinatário principal (quando não o único) dessas normas. Esta primeira geração de leis vai, aproximadamente, até a *Bundesdatenschultzgesestz,* a lei federal da República Federativa da Alemanha sobre proteção de dados pessoais, de 1977".

Já as leis de segunda geração deixaram de focar apenas no *hardware* que armazena os dados para a qualidade dos dados que eram armazenados, o que surge em razão da insatisfação dos titulares de dados com o fato de seus dados, inclusive os sensíveis, serem utilizados de forma alheia à sua vontade, possível afirmar que a segunda geração de leis de proteção a dados pessoais se dá com a Constituição Portuguesa e a Constituição Espanhola, além da lei francesa de proteção de dados pessoais de 1978, a Lei Suíça de 1981, a Lei da Islândia de 1981 e a Lei de Luxemburgo de 1979. (Pezzi, 2007, p. 95).

A partir da década de 1980, A terceira geração de leis que visavam a tutela dos dados pessoais tinham como escopo não somente a liberdade dos cidadão em fornecerem seus dados pessoais, mas, em especial, a valorização da autodeterminação informativa e instrumentos que garantissem o direito previsto, como uma nova cultura e ruptura com costumes anteriores, os titulares de dados ainda não compreendiam a importância do tema e, alguns, sequer preocupavam-se com tal fato, não obstante, a semente foi lançada para que posteriormente houvesse o discernimento da tamanha relevância acerca da proteção de dados, fato que, no Brasil, tardou a acontecer. (Machado, 125-126).

Por fim, a quarta geração e última, até o momento, preocupam-se em suprir as lacunas deixadas pelas gerações anteriores. Em especial há uma procura por tutelar o tratamento individual, enquanto as primeiras gerações visavam o próprio indivíduo, formas de proteger dados pessoais, a nova geração possibilita a responsabilização da coletividade na proteção de dados pessoais. (Doneda, 2011, p. 98).

Do que se apresentou, fica claro que na Europa a proteção de dados pessoais passou a ocupar um lugar privilegiado desde muito cedo, nessa senda, Cristina Caldeira (2019, p. 634),

assevera “podemos observar que a matéria de proteção de dados pessoais ocupa um lugar central na legislação da União Europeia”.

Nesta senda, tem-se que a União Europeia tem publicado normativas com o escopo de tutelar a proteção de dados pessoais, sendo notório sua posição pioneira no assunto e que, por ser pioneira, impacta os demais países ao redor do mundo, cita-se, em especial, a GDPR – *General Data Protection Regulation,* qual seja, o Regulamento Europeu de Proteção de Dados. Menciona-se que tal regulamento serviu de inspiração para o Brasil na edição da Lei Geral de Proteção de Dados, posto que se deu no ano de 2016 – Regulamento 2016/679. Acerca da proteção do cidadão, o diploma europeu visava aspirar a conciliação entre a proteção do titular de dados, o interesse público, sem perder de vista o desenvolvimento tecnológico e econômico, os quais, em razão do advento das tecnologias já citadas, acabam por estar vinculados. (Corrêa, 2019).

Ainda, sobre o GDPR ou RGPD, esta última sigla tornada para o português, Regulameto Europeu de Proteção de Dados, tornou-se a regra de proteção de dados, sendo, ainda, diferente da directiva 95/46/CE, Renata Queiroz (2021, p. 27), assim leciona sobre o tema:

> “Por fim, em 2016, o Parlamento Europeu e o Conselho publicaram, no dia 27 de abril, o *General Data Protection Regulation* (GDPR) – Regulamento Europeu de Proteção de Dados (doravante RGPD, na sigla em português) -, o qual tornou-se a regra da proteção de dados essencial a todos os países da União Europeia. Difere da Directiva 95/46/CE por ser diretamente aplicável, estabelecendo um novo modelo de apoio à proteção de dados na Europa. Entre os seus objetivos principais estão a proteção dos direitos e liberdades fundamentais das pessoas singulares, bem como a livre circulação de dados pessoais na União Europeia. Vale dizer que o Regulamento Europeu de Proteção de Dados mantém os princípios definidos pela Convenção 108 ou pelas Diretrizes da OCDE, de 1980, porém aparecem mais sistematizados e esclarecidos no RGPD. Percebe-se, no sistema europeu, uma coesão, pois sua organização se deu a partir das diretivas editadas pelo Parlamento do Conselho Europeu, que manteve um núcleo de proteção”.

Desta forma, verifica-se que o Regulamento Geral trazido pela União Europeia foi de suma importância global, posto que se trata de norma coesa e moderna que visa a proteção de direitos fundamentais da pessoa humana, sem perder de vista a necessidade de evitar o impedimento de novas tecnologias e do avanço econômico. O tema inclusive já foi abordado no presente trabalho, não obstante, ante a sua relevância é importante rememorar e trazer novas pontuações neste capítulo, já de maneira mais afunilada com o interesse primário deste trabalho.

No Brasil, conforme foi pontuado anteriormente, a proteção de dados pessoais estava incutida, inicialmente, apenas na Constituição Federal de forma genérica, ou seja sem que

houvesse um literal tratamento específico acerca da proteção de dados, o exemplo que se pode citar é o direito à privacidade (artigo 5º, inciso X[4]), o direito à inviolabilidade do sigilo de comunicações, de dados e de comunicações telefônicas (artigo 5º, inciso XXII[5]), a garantia de acesso às informações pessoais e retificações de dados, previstas no remédio constitucional *habeas data* (artigo 5º, inciso LXXII), o qual foi regulamentado pela Lei 9.507 de 1977. (Tavares e Alvarez, 2017, p. 188).

Em linhas gerais, após a Constituição Federal de 1988, a legislação infraconstitucional se preocupou com o tema, iniciando-se ainda de forma tímida com o Código de Defesa do Consumidor de 1990, o qual trata da proteção ao titular de dados em face dos bancos de cadastro de dados, no artigo 43, do Código citado há uma preocupação com os dados pessoais dos consumidores e previsão de tutela, bem como de obrigações aos fornecedores. (Brasil, 1990)

Após um considerável lapso temporal, houve um marco para o Brasil com a promulgação do Marco Civil da Internet, Lei 12.965/2014, o qual surge em razão de um ambiente de insegurança gerado pelo episódio de espionagem revelado por Edward Snowden. Assim, o Marco Civil da Internet tinha como escopo conferir direitos e garantias aos usuários da internet, sem que isso acarretasse num embaraço para a inovação e novas revoluções tecnológicas, é possível afirmar que a lei em comento trata de forma principiológica a utilização da internet, buscando conferir, ao mesmo tempo, tutela especial ao titular dos dados. (Almeida e Lugati, 2020, p. 12).

O Brasil iniciou as tratativas para a edição de uma Lei Geral de Proteção de Dados no ano de 2010, mas foi em 2018 que houve a promulgação da Lei Geral de Proteção de Dados, a qual, em que pese a nomenclatura, não visa a proteção dos dados em si, mas do titular dos dados. Ainda, importa ressaltar que tal fator veio, à época, dar ainda mais força ao direito fundamental à privacidade, de modo que a legislação que abordou diretamente e de forma analítica a proteção de dados não tinha a intenção de inviabilizar ou dificultar negócios, mas visam que os negócios se concretizem com a devida proteção ao direito à personalidade, mencionando-se, ainda, ser a abordagem da Lei Geral de Proteção de Dados envolta de proteção aos titulares de dados pessoas físicas identificadas ou identificáveis, tendo por escopo os

[4] *In casu:* X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[5] XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

direitos fundamentais da liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Queiroz, 2021, p. 43).

As normas citadas já possuíam caráter constitucional, não formalmente, mas de forma material, o que tecnicamente se afirma estar incutida dentro do bloco de constitucionalidade, neste sentido, em sede de dissertação, Anderson Vargas (2007, p. 11-12) defende que:

> "A Constituição, dotada de extrema rigidez para produção de suas normas, por um procedimento cauteloso de adequação do ordenamento jurídico ao seu conteúdo, de um órgão guardião pela sua permanência e durabilidade e, principalmente, pela subordinação das demais normas infraconstitucionais, impõe uma dificuldade em caracterizar quais normas são qualificadas como constitucionais. Significa dizer que, como as normas constitucionais possuem determinadas características que lhes atribuem uma natureza jurídica distinta das demais, identificar como tal, qualquer norma jurídica, exige um cuidado para não reconhecer como norma constitucional àquele que não o seja, justamente pela peculiaridade e superioridade que ela carrega. Essa tarefa de definir quais as normas que compõem a Constituição e, portanto, aquelas aptas a tornearem o instituto do Bloco de Constitucionalidade, demonstrando balizas constitucionais de determinado país, acabam por se tornar mais árdua quando visualizada de maneira global, ou seja, sem definir previamente um ordenamento jurídico especifico".

Ou seja, por possuir um elevado valor axiológico, determinadas normas e princípios, ainda que não previstos no corpo do texto constitucional, podem ser consideradas constitucionais ou ao menos ter caráter de norma constitucional por compor o bloco de constitucionalidade, fugindo-se do minimalismo conceitual.

O Supremo Tribunal Federal, (Brasil, 2020, p. 51-52), decidiu em sede de julgamento de Ação Direta de Inconstitucionalidade número 6393, em face da Medida Provisória 954/2020, que a autodeterminação informativa e a proteção de dados pessoais são direitos fundamentais autônomos, em sede de fundamental, assim restou colacionado:

> "A proteção de dados pessoais e a autodeterminação informativa são direitos fundamentais autônomos, extraídos da garantia da inviolabilidade da intimidade e da vida privada (art. 5º, X), do princípio da dignidade da pessoa humana (art. 1º, III) e da garantia processual do habeas data (art. 5º, LXXII), previstos na Constituição Federal de 1988. [...] O presente voto é estruturado sobre a premissa de que o compartilhamento de dados, mesmo em cenários de crise, deve seguir os mandamentos constitucionais e legais, observando uma estrita relação entre adequação e necessidade. Nesse prisma, entendo que a Medida Provisória 954/2020 desborda dos limites fixados pelos direitos fundamentais à proteção de dados e à autodeterminação informativa, extraídos da garantia da inviolabilidade da intimidade e vida privada (art. 5º, X, CF/88), do princípio da dignidade da pessoa humana (art. 1º, III, CF/88) e da garantia processual do habeas data (art. 5º, LXXII, CF/88). A Medida Provisória afronta, ainda, o postulado da proporcionalidade, notadamente nas vertentes adequação e necessidade, mormente por não delimitar o objeto, a amplitude e a finalidade específica da estatística a ser produzida com os dados obtidos".

Deste modo, o Supremo Tribunal Federal reconheceu, antes de previsão expressa no texto constitucional a existência de direitos fundamentais autônomos à autodeterminação informativa e à proteção de dados fundamentais, sendo que, após isto, no ano de 2022, houve edição da Emenda Constitucional 115/2022, a qual, entre as alterações feitas na Carta Maior, acrescentou o inciso LXXIX ao artigo 5º, estabelecendo que é assegurada a proteção dos dados pessoais, inclusive no meios digitais. (Brasil, 2022).

Importante mencionar que a decisão do Supremo Tribunal Federal no ano de 2022 rompeu com a ideia retrograda de autodeterminação informativa, a qual, incialmente, era privilégio de uma minoria que decidia enfrentar os custos tanto econômicos como sociais do exercício dessa prerrogativa. Com o avanço do pensamento, foi possível um fortalecimento da posição da pessoa em relação aos detentores de dados, de modo tal que atualmente entende-se que a autodeterminação informativa é direito fundamental da pessoa humana. (Doneda, 2011, p. 98).

Houve, importa mencionar, decisão emblemática do Superior Tribunal de Justiça no ano de 1995, em voto de relatoria do Ministro Ruy Rosado de Aguiar (Brasil, Superior Tribunal de Justiça, 1995), o qual, àquela época já havia assim estabelecido:

> "A inserção de dados pessoais do cidadão em bancos de dados de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou pressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador".

A decisão que é muito antiga e bem anterior ao início da discussão acerca de proteção de dados pessoais já demonstrava que o advento das tecnologias fazia surgir uma certa preocupação com as consequências da entrega de dados que deixam de estar tão somente sob a guarida do titular de dados, citou-se à época os disquetes, via física, atualmente os dados estão alocados, em muitos momentos, junto à *internet*, ou seja, em rede, nas nuvens, *e-mails*,

plataformas, redes sociais e outros que são de mais fácil acesso e mais passíveis de ataques ou violações.

Nesta senda, é possível afirmar que a legislação brasileira atinente à proteção de dados pessoais é recente e passou por processo moroso para que viesse à existência, enquanto noutros países, em especial na Europa e Estados Unidos da América, a preocupação com os titulares de dados se deu anteriormente, fazendo com que nos locais mencionados houvesse uma cultura mais avançada quanto à sensibilidade dos dados pessoais, bem como da importância dada ao tema. Ainda assim, mesmo que morosa, a legislação brasileira pôde se utilizar das demais legislações enquanto paradigma, podendo-se, por fim, afirmar que o Brasil iniciou a sua tutela de proteção aos dados pessoais, diz-se, aos seus titulares, a partir da quarta geração de legislação protetiva.

Não obstante, vale mencionar que os tribunais, em especial o Superior Tribunal de Justiça e o Supremo Tribunal Federal enfrentaram a matéria em discussão antes dos legisladores, tendo demonstrado a sensibilidade do tema e a necessidade de amparo, ou seja, de tutela a ser prestada pelo Estado, posto que, na decisão recente do Supremo Tribunal Federal, anterior ainda à emenda constitucional 115/2022, já se reconhecia os dados pessoais enquanto direito fundamental, ainda que de forma decorrente do direito à privacidade, já na decisão do Superior Tribunal de Justiça, ainda de forma embrionária, demonstrou-se a fragilidade e o risco de ter dados pessoais fora da área de proteção apenas do titular, alarmando para a forma como isso seria tratada doravante.

2.2 DADOS PESSOAIS

Realizada a análise acerca do contexto em que se insere a proteção aos dados pessoais, passa-se a abordar, perfunctoriamente, os dados pessoais em si, fato este que auxiliará no decorrer de todo o texto para entender conceitualmente o que são os dados pessoais, bem como para compreender qual a relevância deste instituto na atualidade.

Quanto ao tema dados pessoais, é imperioso fazer a devida análise, evitando-se lacunas inapropriadas, em razão disto, antes de adentrar à conceituação própria de dados pessoais, é imperioso discernir o real sentido do que seria o termo dado, o qual compõe um trio, juntamente com outros dois termos, quais sejam, informação e conhecimento. No que atine ao conceito de dado, tem-se que este é um fato ou um átomo, um elemento ainda não lapidado, dependente de maior aprofundamento para que tenha um significado, ou seja, não se trata de fator pronto e

acabado, afirmar-se que o dado carece de um significado imediato, mas ainda assim, trata-se de algo perceptível e de baixo teor significativo, assevera-se que um dado, por si só, não seria capaz de ter relevância, não obstante, a premissa muda quando há um conjunto de dados, tem-se este como uma fração de informação, enquanto o conjunto de dados é capaz de ser classificado enquanto informação. (Semidão, 2014, p. 70).

Gabriel Guimarães (2021, p. 27) faz análise dos dados sob um viés meramente tecnológico, mas elucidativo, vide:

> "Do ponto de vista meramente da tecnologia em si, dados pressupõem elementos (símbolos, códigos) que representam informações (quando atingem um conjunto desses dados). Aleatoriamente, os dados não significam ou não expressam nada que o ser humano possa absorver ou dele conhecer algo. Já com o tratamento conferido aos dados coletados e disponíveis e, considerando a relevância e o objetivo a ser alcançado, chegaremos a diferentes e apuradas informações, com diferentes graus de interesse. Dessa forma, observamos que os dados são os elementos iniciais que antecedem as informações relevantes, para então, por exemplo, apontar os problemas, as soluções e as melhores providências a serem tomadas numa determinada situação. Numa comparação bem simples, os dados seriam os átomos de um organismo completo".

Considera-se, desta forma, que o dado possui pouco valor agregado e carece de processo de tratamento para que seja viável retirar dele algum significado e seja útil em algum processo, assim ensinam Marcos Botelho e Elimei Camargo (Botelho e Camargo, 2021, p. 4).

É viável discutir qual o motivo para conferir tanta importância aos dados pessoais. Conforme tratado no subcapítulo anterior, num capitalismo de vigilância, a coleta de dados, em especial, dados pessoais, torna-se atividade corriqueira e almejada. Nesse sentido, destaca-se que o mundo, ainda que de modo díspar, se situa na chamada Quarta Revolução Industrial (Schwab, 2018), em que se verificou, desde 2012, a intensificação do uso de tecnologias variadas, em especial as tecnologias da informação e a inteligência artificial, permitindo intensa cooperação entre o físico e o digital.

Ademais, os avanços referidos capacitaram o advento de contornos mais incisivos à sociedade da informação. Castells aponta nesta sociedade um novo paradigma tecnológico em torno da tecnologia da informação (Castells, 2019, p. 87), indicando, dentre suas bases materiais, a informação como matéria-prima e a tecnologia sendo utilizada para agir sobre a informação (Castells, 2019, p. 124-125). Desse modo, salienta que para a sociedade a qual se vive, as informações, logo, os dados, têm muita relevância.

Castells (2019, p. 80-82) ainda vai afirmar que além de a sociedade da informação conferir um novo paradigma tecnológico, gerou uma ruptura cultural, trazendo um novo modelo

de cultura, o qual é aquele que se preocupa com os dados pessoais, seu tratamento, sua operação, seu resultado e todas as nuances que formam um satélite em volta do tema.

Em sentido semelhante, destaca-se a autora Shoshana Zuboff, já citada outrora, a qual aponta para o *capitalismo de vigilância*, em que a atual roupagem do capitalismo, por meio dos dados, manipula o comportamento dos usuários das plataformas digitais, em especial quando se fala em consumo, isto só se torna possível em razão da grande coleta de dados geradas e possíveis pelos meios tecnológicos utilizados na atualidade, inclusive, tem-se que nas *smart cities* (cidades inteligentes) há uma tendência de fazer coleta de dados e verificar quais os comportamentos das pessoas que tiveram seus dados coletados (Zuboff, 2019, p. 90).

A Lei Geral de Proteção de Dados traz o conceito de dados pessoais enquanto informações da pessoa natural identificada ou identificável, vide artigo 5º, incisos I, II e V[6]. No mais, faz-se uma subdivisão que aborda os dados pessoais, na condição de dados sensíveis, sendo aqueles que versam acerca da origem, opiniões, dados biológicos e outros capazes de receber tal classificação (Brasil, Lei nº 13.709 de 2018).

Impera trazer à lustre o fato de que o avanço tecnológico acarreta a necessidade de tutela pelo Estado, mas não é possível conceber a ideia de que a utilização, coletas e tratamento de dados seja tão somente problemática, em verdade, a tecnologia exerce um papel disruptivo, sendo capaz de auxiliar na coleta de dados para apresentar informações relevantes, a título de exemplo, dados médicos de um paciente que está numa emergência. Assim, a coleta de dados pessoais serve para o desenvolvimento de inúmeros benefícios, sendo impulsionada a coleta e tratamento por meio de *open data* (dados abertos), *living labs* (laboratórios vivos) e *tech hubs* (centros tecnológicos) (Cunha, 2016, p. 33).

Insta mencionar que os dados pessoais são considerados o novo petróleo do século XXI, essa foi a abordagem trazida pela revista *The Economist* (2017), a qual elencou os dados pessoais enquanto o como o recurso mais valioso do mundo, apresentando, destarte, os dados pessoais enquanto um novo insumo, o qual, inclusive, tornou-se essencial ao desenvolvimento

---

[6] *In casu:* Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

de atividades econômicas, tendo sido passível de mercantilização, por isso é viável afirmar que há uma existência de uma economia guinada por dados pessoais.

Fala-se de dados pessoais enquanto novo petróleo, tem-se que tal frase tornou-se praticamente um mantra pelos *CEOS* de grandes empresas de tecnologia, palestrantes, vendedores etc., tem-se que tal afirmação não é vã, posto que hodiernamente o mercado de dados pessoais possui grande parcela na economia informacional, assim, verifica-se que os dados pessoais são como uma moeda paga para a utilização "gratuita" de plataformas, *sites* e serviços online. (Avelino *et al*., 2016, p. 220).

Quando se trata sobre dados pessoais e seus efeitos econômicos no mundo capitalista, tem-se os ensinamentos de Rodrigo Magalhães e Erika Oliveira (2021, p. 55-56), os quais assim discorrem sobre o tema:

> "Não há dúvidas de que as tecnologias possibilitam mudanças significativas para os indivíduos inseridos na sociedade da "Era Informacional". Atualmente o indivíduo precisa ser observado, fornecer suas informações, expor sua rotina e se comunicar rapidamente, para participar da sociedade como um ser existente – afinal, não estar conectado ou não ter informações retidas em uma base de dados torna-se quase um sinônimo de inexistir. (...) Empresas e entidades públicas usam dados pessoais a todo momento, seja para o oferecimento de produtos e serviços de acordo com o perfil do cliente ou para elaboração de controles internos, com o interesse de manter o funcionamento das tecnologias que facilitam esses serviços e melhoram o atendimento aos clientes".

Desta forma, resta claro que os dados são de suma importância no presente século, posto que com o tempo passaram a ter valor econômico, razão pela qual o mercado se alvoroça com o intento de angariar dados e prever qual o tipo comportamental das pessoas, visando obter lucro, em verdade, não é em prever o comportamento, mas, nalguns momentos, conforme já citado, é possível afirmar que moldam o comportamento da sociedade para que determinada conduta social, ainda que induzida, acarrete o aumento da lucratividade. Cita-se como exemplo os dados pessoais coletados como preferências das pessoas, o que clarifica para as empresas quais produtos devem ser apresentados para determinada pessoa ou grupo de pessoas induzindo-as a adquirir bem ou serviço.

Necessário apresentar o que é *big data*, posto que quando se fala em coleta de dados não é possível relevar o que é *big data*, o qual pode ser entendido enquanto um conjunto massivo de dados que são coletados por meio do acesso de usuários à *internet*, seja de forma direta ou, ainda, indireta, neste caso pela *internet* das coisas (IoT – *internet of things*), sendo a IOT compreendida como os equipamentos da vida cotidiana com a capacidade de se conectar à

internet, em outras palavras, a IoT pode ser vista como uma infraestrutura capaz de permitir a interconexão de "coisas" físicas e digitais. Ainda, os conjuntos massivos de dados coletados (*Big Data*) podem ser processados e analisados por um processo extremamente rápido, via *Big Data Analytics*. (Barbosa *et al*., 2019, p. 89).

Quanto à *internet* das coisas (IoT), tem-se que a internet, em suas primeiras quatro décadas, tem sido utilizada com enfoque na conexão de pessoas, seja por e-mails, *sites* e outros, mas, nos últimos tempos, em especial pelas redes sociais, as quais coletam e distribuem dados pessoais, na atualidade, além de tudo que foi acima citado, a *internet* tem sido utilizada para conectar dispositivos, máquinas e objetos de posicionamento tecnológico, o que constitui o que atualmente se chama de internet das coisas. (Dutton, 2014, p. 1-21).

Nairobi Oliveira *et al.* (2019, p. 4-5), acerca da *internet* das coisas, assim lecionam:

> "Um número cada vez maior de objetos físicos está sendo conectado à internet a uma velocidade sem precedentes, atribuindo a estes a ideia da IoT. Muitos dispositivos os quais normalmente não se conectavam a rede, estarão presentes, podendo coletar dados, gerar informações para análises e monitoramentos, bem como automatizar tarefas ou prover alguma facilidade ao usuário, tais dispositivos denominam-se restritos. (...) a IoT pode prover diversas classes de serviços, dentre elas, destacam-se os serviços de identificação, responsáveis por mapear entidades físicas (de interesse do usuário), entidades virtuais (EV) como, por exemplo, a temperatura do local físico, coordenadas geográficas e serviços de agregação de dados que coletam e sumarizam dados obtidos por objetos inteligentes, entre tantos outros segmentos".

Ocorre que com a premissa estudada, verifica-se a existência de um intento muito grande em conectar objetos que originariamente não foram criados para ter tal função, não obstante, no processo de uso, passou a ser útil a conexão de tais objetos com a rede, de modo tal que os objetos que se conectam à rede em muitos momentos compartilham dados pessoais dos usuários, por este motivo é inviável tratar sobre a proteção de dados sem melhor elucidar a *internet of things – internet* das coisas (IoT).

Nesta senda, o que se tem é que o tráfego de dados pessoais nos aparelhos e objetos conectados à *internet* das coisas, inclusive dados sensíveis, fazem surgir a necessidade da adoção de medidas e instrumentos para gerar segurança em rede, isso até mesmo na fase de projeto dos dispositivos, no *hardware, software* e afins. A segurança citada é conhecida como segurança da informação, a qual pode ser entendida como a forma tomada para a proteção dos dados contra a enorme gama de riscos gerados, tendo por finalidade o menor risco nas atividades relacionadas que envolvam dados pessoais e sua disposição na *internet* das coisas. (Hintzbergen, 2018).

Num mesmo sentindo, tem-se os ensinamentos abaixo (Lima e Bioni, 2015):

> "Nesse caso em específico, considera-se que o próprio produto ou serviço deve ser arquitetado de forma condizente a proteger as informações pessoais de seus usuários. Vale dizer que a privacy by default é, apenas, um dos diversos tipos de abordagem propiciadas pelo privacy by design, a qual consiste como, a própria terminologia induz, em considerar a privacidade como um elemento condutor na fase de projeção e desenvolvimento de produtos e serviços".

Assim, quanto à IoT, verifica-se que se trata de realidade existente em razão de uma necessidade que surgiu de conectar coisas que não foram criadas necessariamente com a finalidade de estar em rede, mas que por alguma utilidade passaram a estar conectadas, a título de exemplo cita-se os relógios inteligentes, os quais marcam dados sensíveis, quais sejam, dados da saúde da pessoa, como batimentos cardíacos, quantos passos foram dados em determinado dia, qual a distância percorrida diariamente, entre outros. Deste modo, entende-se pela necessidade de cuidados com os objetos que terão integração com a rede, isso desde o momento de seu projeto, visando a criação de mecanismo de defesa contra os eventuais ataques e riscos gerados pela conexão e disposição de tais dados em rede.

Obviamente a sociedade atual vive num momento que há uma superoferta de dados, não obstante, estes dados carecem de conversão em ativos estratégicos, posto que o dado por si só ou colhido de forma esparsa pode não possuir valor, não obstante, a partir do momento em que se lapida o dado há uma geração de valor. Noutras palavras, tem-se um dilúvio de dados gerados sem planejamento, mas que, quando lapidados, servem para alimentar ferramentas analíticas de *big data*. (Rogers, 2019, p. 22).

No mesmo sentido, cabe a afirmação de que com a facilidade de acesso à *internet* o titulador de dados passou a ter exposto fragmentos de sua vida, com isso, *big datas* passaram a ter existência com o armazenamento de tais informações, Parentoni (2015, p. 540), acerca da temática, afirma que:

> "Se, por um lado a preocupação com o tema não é nova; por outro, o desenvolvimento tecnológico das últimas décadas, principalmente com a invenção dos computadores pessoais e da internet, trouxe uma miríade de problemas e questionamentos referentes à privacidade, anteriormente inimagináveis. A internet relativizou distâncias, permitindo a comunicação praticamente instantânea entre partes opostas do mundo, com som e imagens de alta definição. E juntamente, com os benefícios, o progresso tecnológico trouxe também novos riscos".

É conveniente entender que existem muitos benefícios com o advento das tecnologias, não só para o mercado capitalista, mas também para os indivíduos que conseguem o acesso à informação quase de forma instantânea, não obstante a virtualização da vida traz riscos quando os dados são utilizados de forma indiscriminada, neste sentido Luiz Taborda (2022, 78):

> "No entanto, apesar dos inegáveis benefícios trazidos para a vida em sociedade após o advento das novas ferramentas tecnológicas pautadas na troca de informações instantâneas, a virtualização da vida trouxe também alguns riscos aos indivíduos considerando que em uma sociedade que tem a informação como a base de sua economia, os dados pessoais passaram a ser utilizados de forma indiscriminada, ocasionando assim, uma infinidade de problemas e transtornos em razão do uso indevido desses dados. Nesse contexto, tem-se que a dinâmica na maioria dos casos de violência financeira praticados contra a pessoa idosa no mercado de consumo, ocorrem por meio do vazamento e uso indevido de dados pessoais existentes nas diversas plataformas de dados de empresas públicas ou privadas que, uma vez acessados ou disponibilizados a terceiros de forma indevida, acabam servindo de munição para a aplicação das mais variadas espécies de golpes e abusos".

Do que se afere até o momento, é possível afirmar que o dado por si só não possui tanto valor agregado, mas quando devidamente tratado e manipulado, é possível tirar proveito, inclusivamente econômico. Neste sentido, os dados das pessoas ou ainda de um conjunto de pessoas somente terão validade se organizados para determinado fim, ocorre que essa manipulação é onde pode ocorrer os abusos ou ilegalidades, de modo tal que surge a necessidade de que a tutela estatal exista para evitar a lesão sobre as pessoas físicas identificadas ou identificáveis (Guimarães, 2021, p. 37).

Surge, então, um binômio entre segurança e liberdade, posto que enquanto as pessoas optam pela liberdade e facilidades oferecidas pelas plataformas que colhem os dados, em contramão, cedem dados pessoais que acabam por fragilizar a segurança de dados.

Baumann (2014) trata isto como a morte do anonimato por cortesia da internet, no qual se troca as maravilhas oferecidas em troca dos direitos de privacidade, entendendo ser este um preço razoável, não obstante, pela falta de cultura acerca da proteção de dados, em nosso país, a população não entende a profundidade dos danos que podem ser causados pela troca da privacidade por facilidades oferecidas.

Num mesmo sentido, Amadeu Neto (2023, p. 43) discorre em sua dissertação que:

> "Como é cômodo acordar, ser despertado geralmente pelo relógio do aparelho celular, o qual foi configurado a se adaptar conforme rotinas, gostos, lugares e *sites* visitados. Como é facilitado encontrar produtos e serviços nos *sites* e aplicativos acessados regularmente, sendo interessante que eles "magicamente" mostrem aquilo que se deseja no momento. O que se tem observado é que o preço dessa comodidade seria a

> invasão de privacidade, muitas vezes desconhecida, pelo compartilhamento de dados pessoais com agentes operadores os quais moldariam o comportamento de usuários ofertando serviços e produtos tecnológicos a cada necessidade. Essa customização é apenas uma das modalidades de utilização de dados pessoais em benefício do marcado capitalista. Grandes dúvidas e riscos pairam acerca do acesso, compartilhamento e fim de utilização desses dados".

Neste ponto, quanto à coleta de dados (*data mining*), verifica-se que não se trata de procedimento simples, mas de um processo analítico que, dentro de oceanos de dados, tem a finalidade de cruzar dados suficientes para que estes se transformem em uma informação relevante dentro de um processo decisório, ou seja, o *data mining* é um processo de mineração de dados que atua como uma peneira ou funil para que possibilite alcançar informações (conjunto de dados) que sejam relevantes para o negócio. (Burkart, 2021, p. 22).

Quanto à mineração dos dados, tem-se que o contexto no qual se aplica é o de que a sociedade da informação tem um alto desenvolvimento da tecnologia, de modo tal que o grau de penetrabilidade na vida dos titulares de dados apresentam consequências positivas, como a maximização da utilização do tempo, novos mercados e outros, mas também consequências negativas, como o acesso facilitado a dados pessoais que não necessariamente o titular quer que estejam na posse de terceiros ou que sejam publicizados. Por óbvio que com a tecnologia a sociedade de consumo acaba por ter novos patamares no consumo e uma mudança comportamental. É neste contexto que surge a mineração de dados, a qual atua como forma de prospecção de dados, visando explorar e guardar informações de sujeitos para uma utilização *a posteriori*, com a finalidade de estabelecer os padrões de comportamento e formas de relacionamento do titular de dados. Neste cenário que surge a importância da reflexão acerca de qual a tutela que o Estado deve prestar para mitigar eventuais danos ou até prevenir que aconteçam. (Gropp e Mota, 2020, p. 65)

Do que foi demonstrado, é possível afirmar que houve a conceituação de dados, informação e conhecimento, apresentando os dados pessoais enquanto bem com valor econômico agregado na atualidade, sendo reconhecido até como o petróleo do século XXI, ainda, foi mencionado que dentro do capitalismo de vigilância os dados são coletados reiteradamente para fins comerciais, sendo estes muitas vezes utilizados como moeda de troca pelas facilidades oferecidas pelas plataformas que trocam serviços gratuitos por dados, de modo tal que, por fim, foi apresentado o que é *big data* e *data mining*.

3 APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS AO PODER PÚBLICO

O terceiro capítulo tem o escopo de, passada a análise sobre a sociedade da informação e depois de perpassada a fase inicial da discussão sobre o que são os dados pessoais e a preocupação da sociedade hodierna, bem como do Estado, com o fluxo de dados, necessário se aproximar do cerne da presente dissertação, já que, após apresentar a aplicabilidade da lei geral de proteção de dados e da legislação protetiva também ao Estado, passar-se-á a discutir os reflexos da norma no poder público, sendo esta a tarefa que se passa a cumprir.

3.1 A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO À ADMINISTRAÇÃO PÚBLICA

Inicialmente, tem-se que é primordial apresentar ao leitor a razão de existir da Lei Geral de Proteção de Dados e por qual motivo é imperioso demonstrar que a norma se aplica ao Estado. Desde já, menciona-se que há norma expressa no sentido de que compete ao Estado o cumprimento da norma, ainda assim, é necessário apresentar a problemática, ou seja, a dor existente na atualidade para que, posteriormente, seja possível apresentar possíveis soluções e até mesmo *cases* de sucesso no Poder Público que podem servir como paradigma na pesquisa e para a regulamentação do Estado internamente para solução dos problemas basilares que, conforme será demonstrado, ainda carecem dos passos iniciais por parte da administração pública.

Verifica-se que com o fenômeno, já explicitado, da massificação da coleta, trânsito e até vazamento dos dados, os usuários das tecnologias virtuais demandavam norma para a proteção das situações jurídicas que demandavam soluções, foi nesta toada que o Brasil, desde o ano de 2010, iniciou a tramitação, via Poder Legislativo, visando a criação de uma Lei Geral de Proteção de Dados, a qual dentro do moroso processo legislativo no Brasil, acabou por demorar cerca de oito anos para que fosse sancionada, passando a ter aplicabilidade jurídica tão comente no ano de 2021, (Almeida, 2020, p. 3).

O professor Danilo Doneda (2020, p. 243), de saudosa memória, ensinava que a Lei Geral de Proteção de dados foi a norma de vanguarda que trouxe ao ordenamento jurídico os elementos necessários e capazes de reordenar a forma de abordagem que até então existia sobre os dados pessoais, sendo que a norma citada foi capaz de estabelecer novos regramentos de conduta para o tratamento de dados, disto é possível afirmar que a Lei Geral de Proteção de Dados estabeleceu uma nova sistemática protetiva.

A Lei Geral de Proteção de Dados (Brasil, 2018) trata, em seu primeiro artigo, de forma expressa que se aplica e dispõe sobre o tratamento de dados pessoais, sendo incluído o meio digital, restringindo a proteção dos direitos fundamentais de liberdade, privacidade e livre desenvolvimento da pessoa natural, ou seja, não é esta norma que trata sobre a proteção de dados de pessoas jurídicas e, continua, no parágrafo primeiro estabelece que compete aos entes da federação, quais sejam, União, Estados, Distrito Federal e Municípios o respeito às normas contidas na lei, posto que são de interesse nacional e devem ser observadas[7]. Ressalta-se que as disposições do parágrafo único foram incluídas pela Lei nº 13.853, de 2019, ou seja, não estava desta forma inicialmente.

Deste modo, tem-se que que a norma é de aplicabilidade ao Estado, não obstante, vale mencionar que o poder público é o coletor de dados por excelência, explica-se. Desde os primórdios, o Estado é responsável por saber quem vive em seu território, quem o adentra, quem transita nele, enfim. Em razão disto, a necessidade de coletar os dados para ter as informações necessárias, mas não só, o Estado por ser coletor de impostos, detém os dados dos contribuintes, no mais, visando ter controle dos nascimentos e óbitos, emite certidões para estes, quando é necessário efetuar o casamento civil, faz-se num cartório, quando se faz uma transação imobiliária, em regra, faz-se por registro público, deste modo, notoriamente o Estado é um coletor por excelência.

Verificando ser o Estado um coletor de dados por excelência, a este cabe ou caberia promover o devido tratamento aos dados, posto que, conforme o inciso LXXIX, do artigo 5º, da Constituição Federal eleva a proteção aos dados pessoais ao patamar de direito fundamental positivado. Não obstante, reiteradamente se tem notícia de vazamento de dados ou espionagem interna no poder público por agentes públicos com notório vício/desvio na motivação, sem que sequer se saiba o lastro do que foi realmente vazado, cita-se, a título de exemplo, apuração da Polícia Federal que aponta ter a Agência Brasileira de Inteligência (ABIN) ter sido instrumentalizado para monitorar ilegalmente determinadas pessoas, utilizaram-se do *software* FIRST MILE, o qual serve para indicar a geolocalização e movimentações de pessoas por meio dos celulares destas. (Portal G1, 2024).

---

[7] *In casu:* Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Neste ponto, é de se indicar que o Poder Público é o responsável por qualquer dano que algum de seus agentes públicos causem a terceiros pelo vazamento de seus dados, o que será devidamente discutido no momento devido, inclusive, é isso que aponta a Constituição Federal no artigo 37, § 6º[8], o qual estabelece que tanto as pessoas jurídicas de direito público como as pessoas jurídicas de direito privado, desde que prestadoras de serviço público, respondem pelos danos causados por aqueles que são perpetrados por seus agentes que estejam investidos desta qualidade, o texto faz alusão aos danos causados a terceiros, assegurando ao poder público ou às prestadoras de serviço público o direito de regresso contra o responsável, tanto nos casos de dolo como nos casos de culpa (Brasil, 1988).

Outro ponto a ser mencionado que ressalta a responsabilidade e necessidade de cuidado estatal nesta sociedade em que se vive, qual seja, a sociedade da informação, é o fato da existência de *smart cities*, as quais, em alguns casos, implementam projetos por meio de parcerias público-privadas, esta é a lição trazida por Tharsila Fariniuk (Fariniuk *et al*., 2020, p. 160-161):

> "No Brasil, o uso do termo *smart city* tem sido geralmente adotado por projetos patrocinados por empresas estrangeiras ou desenvolvidos a partir de parcerias público privadas. A disseminação ocorre, ainda, por meio de feiras e exposições, onde o conceito é também associado a protótipos da indústria automobilística e da construção civil, e produtos originados em startups. A utilização dos termos nos projetos não possui uma lógica definida, pois o conceito pode denominar ações nas mais diversas áreas. Na ocasião da Copa do Mundo FIFA 2014, por exemplo, ocorreu a implantação de projetos voltados especialmente para vigilância, monitoramento e segurança, e alguns destes foram considerados como iniciativas *smart city*. Outras cidades denominaram dessa maneira projetos relacionados às energias renováveis e à adaptação da malha elétrica urbana, como é o caso da cidade de Armação dos Búzios, balneário turístico do Rio de Janeiro".

Deste modo, verifica-se que as *smart cities* naturalmente podem existir com a finalidade de monitoramento. Quando se mencionou no presente trabalho o capitalismo de vigilância de Zuboff, tratou-se do fator de que a vigilância que existe tem a finalidade econômica, em boa parte do tempo, tendo por escopo direcionar o comportamento da sociedade monitorada, promover pesquisas de comportamento de consumo e afins, também existem

---

[8] *In casu*: Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
§ 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

projetos no setor de segurança, os quais envolvem o Estado, é nesse contexto que surge a problemática, qual seja, há fiscalização efetiva por parte do poder público sobre a destinação dos dados? Infelizmente o vazamento pode ser descoberto somente após um lapso considerável de tempo, de modo que, notoriamente, o exercício do poder de polícia pelo Estado deve ser efetivo e contínuo.

Ainda, acerca das *smart cities*, não se olvida que há benefícios com a sua implementação, em especial com maior participação da população, não obstante, não se pode tirar de cena o fato ou fator de que a coleta de dados é o que alimenta a sistemática proposta, sobre o tema, Rizzon *et al*. (2017, p. 128) leciona que:

> "Cidadãos são os principais atores ou agentes no desenvolvimento das *Smart Cities* e, portanto, em grande parte moldam padrões da cidade, incluindo padrões sociais, econômico, ambientais e de governança. Desenvolver redes de cidadãos é uma função crítica para uma cidade frente aos seus esforços de planejamento. Desenvolver capacidades para soluções em rede irá criar fortes comunidades de cidadãos que têm a capacidade de intervir e resolver problemas locais, em coordenação com instituições locais e estruturas de governança. O empoderamento dos cidadãos devido à utilização das TICs representa um recurso amplamente enfatizado nas Smart Cities. (...) Assim, o empoderamento dos cidadãos é uma maneira de apoiar o processo de tomada de decisão com base em uma ampla base de opiniões dos cidadãos e, portanto, assegurar o desenvolvimento de processos mais participativos, colaborativos e capazes de responder eficazmente a necessidade das comunidades locais".

Deste modo, vislumbra-se que o poder público entre tantas vertentes acaba por ter acesso ininterrupto a dados que são coletados, armazenados, mas precisam ser devidamente tratados, já que ter acesso à informações em tempo real não importa em abdicar direito dos cidadãos, em especial a liberdade, a privacidade, o direito à não publicizar o que não é necessário. Ressalta-se que a coleta excessiva de dados pela administração pública, se não tratada da maneira devida, prestar-se-á ao vilipendio de direitos fundamentais. (Hiroki, 2019, p. 83).

Tem-se que compete ao Estado promover a segurança da sociedade e isto nos tempos de tecnologia, envolve também a segurança tecnológica, visando dar manutenção a direitos fundamentais, entre eles, da proteção aos dados pessoais, inclusive nos meios digitais, por ser assim, o ponto inicial é a promoção de segurança dentro do próprio estado, diz-se, do ambiente interno da administração pública, posto que esta possui, nalguns pontos, o monopólio de informações e dados sensíveis da sociedade, a qual é vigiada pelo poder público em inúmeras atividades, deste modo, por assim ser que se afirma que o risco iminente de causar danos a indivíduos é latente.

O Estado, nesta condição de vigilante e coletor de dados, busca em muitos momentos a solução para problemas, como situações urbanas, malha viária, segurança pública *etc*..., dentro desta ideia que Mosco (2021, p. 110) escreve que:

> "A vigilância em massa detalhada não apenas produz dados comercializáveis, mas também cria o "eu qualificado". Os governos, sejam eles explicitamente autoritários ou não, veem as tecnologias das cidades inteligentes como soluções para o problema de monitoramento e gerenciamento das populações em crescimento, incluindo migrantes recém-chegados. Os algoritmos dinâmicos, que mudam a cada nova onda de dados, facilitam o trabalho, transferindo a tomada de decisão para um conjunto de regras geradas por computados e eliminando a responsabilidade política. Embora pesquisas evidenciem que eles incorporam discriminações de raça, gênero e classe, o que equivale a inscrever a desigualdade no código desses sistemas, a aparência de objetividade, reificada no algoritmo, é um meio conveniente para aprofundar e ampliar o controle político".

Deste modo, dentro da vigilância estatal, tem-se a responsabilidade da administração em implantar devidamente a Lei Geral de Proteção de Dados, em especial, demonstrando o fluxograma dos dados, após sua coleta, de modo que seja possível, num eventual vazamento de dados ou alguma intercorrência indevida, encontrar a origem do problema e saber como sanar, em especial para determinar se a falha é subjetiva, ou seja, humana, ou se da própria máquina, ou, ainda, por algum eventual ataque ao sistema.

Verifica-se que existem entes da federação e órgãos públicos que têm se preocupado com a adequação à norma, qual seja, com a Lei Geral de Proteção de Dados, a título de exemplo, há uma série de guias e orientações emanadas para que ocorra a devida tomada de ações necessárias à implementação da Lei Geral de Proteção de Dados, cita-se a Recomendação nº 73/2020 do Conselho Nacional de Justiça[9], este estabelece a diretriz de que seja promovida a

[9] *In casu*: Art. 1º Recomendar a todos os órgãos do Poder Judiciário brasileiro, à exceção do Supremo Tribunal Federal, a adoção das seguintes medidas destinadas a instituir um padrão nacional de proteção de dados pessoais existentes nas suas bases:
I – elaborar plano de ação que contemple, no mínimo, os seguintes tópicos:
a) organização e comunicação;
b) direitos do titular;
c) gestão de consentimento;
d) retenção de dados e cópia de segurança;
e) contratos;
f) plano de respostas a incidentes de segurança com dados pessoais;
II – disponibilizar, nos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários:
a) informações básicas sobre a aplicação da Lei Geral de Proteção de Dados aos tribunais, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores e os direitos dos titulares;
b) formulário para exercício de direitos dos titulares de dados pessoais;
III –elaborar ou adequar, bem com publicar nos respectivos sítios eletrônicos, de forma ostensiva e de fácil acesso aos usuários:

criação de grupos de trabalho para estudo e identificação das medidas necessárias à implementação da Lei Geral de Proteção de Dados, trazendo por resultado uma política nacional para os tribunais e conselhos de justiça (Brasil, 2020).

A norma trazida e comentada tem o interesse de promover a devida regulamentação e adaptação à norma, evitando-se sejam cometidas falhas na coleta e tratamento de dados que possam acarretar posterior danos à pessoa natural que acabem por desrespeitar direito fundamental.

Cita-se ainda o Estado do Paraná que, numa espécie de vanguarda, por sua Controladoria Geral do Estado editou manual de implementação da Lei Geral de Proteção de Dados, apresentou uma análise de diagnósticos[10], demonstrando ainda uma estratégia para que o Estado implemente a lei, sendo capaz de, inicialmente, mapear a forma e o tratamento dos dados pessoais, fazendo o levantamento dos riscos no tratamento, seja capaz, ainda, de elaborar um relatório de impacto à proteção de dados, criando também políticas de privacidade de dados e tratamento de incidentes, determinando ainda a adaptação de documentos internos e externos, sendo tarefa da administração estabelecer os canais de comunicação com a consequente nomeação do encarregado de dados e, de maneira louvável, incentiva a capacitação contínua

---

a) a política de privacidade para navegação no website da instituição em relação à Lei Geral de Proteção de Dados Pessoais e ao art. 7º, VIII, da Lei nº 12.965/2014 (Marco Civil da Internet);
b) os registros de tratamentos de dados pessoais contendo, entre outras, informações sobre:
1) finalidade do tratamento;
2) base legal;
3) descrição dos titulares;
4) categorias de dados;
5) categorias de destinatários;
6) transferência internacional;
7) prazo de conservação;
8) medidas de segurança adotadas;
9) a política de segurança da informação;
IV – constituir Grupo de Trabalho para estudo e identificação das medidas necessárias à implementação da Lei Geral de Proteção de Dados no âmbito do respectivo tribunal, cujo relatório final subsidiará o Conselho Nacional de Justiça na elaboração de uma política nacional.
Art. 2º O Conselho Nacional de Justiça, por meio do Grupo de Trabalho instituído pela Portaria CNJ nº 63/2019, coordenará os estudos a serem realizados pelos tribunais para implementação da Lei Geral de Proteção de Dados.
Art. 3º Os Grupos de Trabalho instituídos pelos tribunais deverão elaborar e apresentar relatório final, no prazo máximo de 180 dias, contados a partir da publicação desta Recomendação, encaminhando-o ao Grupo de Trabalho do Conselho Nacional de Justiça.

[10] Baseado nos resultados dos diagnósticos mencionados nos itens 2.1 e 2.2 é possível iniciar uma estratégia de implementação à LGPD, dividida nos seguintes tópicos: 2.2. DA GOVERNANÇA DE DADOS 2.3. ANÁLISE DOS DIAGNÓSTICOS a. Mapear o tratamento dos dados pessoais; b. Levantar os riscos do tratamento; c. Elaborar o Relatório de Impacto à Proteção de Dados (RIPD); d. Criar políticas de privacidade de dados e tratamento de incidentes, e adaptar os documentos internos e externos; e. Canais de Comunicação; f. Designar o Encarregado de Dados; g. Treinar as equipes que tratam dados pessoais; h. Associar o compliance à LGPD.

das equipes que tratam os dados pessoais, por fim, associa o *compliance* à Lei Geral de Proteção de Dados. (Paraná, 2021, p. 7).

No que atine ao serviço público e à Lei Geral de Proteção de Dados, pode-se afirmar que a Administração Pública deve buscar, incessantemente, a primazia do interesse público, de modo tal que na coleta, no tratamento, na disposição e até no compartilhamento de eventuais dados pessoais, compete à administração pública esquadrinhar o atendimento à finalidade pública.

O foco da administração pública, ou seja, do Estado, deve ser executar as determinações legais, por meio de suas competências, bem como cumprir as normativas da Lei Geral de Proteção de Dados, entre as quais se encontra a informação ao titular dos dados sobre as hipóteses em que seus dados serão tratados, fornecendo ao titular informações claras, objetivas e assertivas quanto à finalidade do tratamento, mencionando os procedimentos e as práticas na execução do tratamento de dados pessoais. Assim, a transparência deve servir de diretriz e princípio, inclusive, esta é a diretriz estabelecida na Cartilha sobre a Lei Geral de Proteção de Dados, editada pela Controladoria Geral do Estado do Paraná (Paraná, 2020, p. 19), vide *in verbis:*

> "O tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público. Consideram-se pessoas jurídicas de direito público para fins da LGPD: os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares. Porém, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público. O titular dos dados deverá ser informado quanto às hipóteses em que, no exercício de suas competências, as pessoas jurídicas de direito público realizarem o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos. As formas de publicidade das operações de tratamento poderão ser estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD)".

Nesta senda, sabe-se que não há novidade no fator de o poder público coletar e tratar dos dados pessoais, já que, como foi dito anteriormente, essa coleta, tratamento e detenção dos dados pessoais fazem parte de atividade essencial do Estado, seja pela necessidade na seara fazendária, na assistência social, na segurança pública etc., o que é necessário apontar é a maneira pela qual deve ocorrer a operação de colheita, tratamento, compartilhamento e demais atividades com os dados pessoais, após a edição da Lei Geral de Proteção de Dados.

Vale advertir que, ao contrário do que o senso comum acredita, o tratamento de dados, coleta e atividades correlatas não passaram a ser proibidas ao Estado, em verdade, passa-se a existir um regramento que orienta o *modus operandi* nas ações que permeiam os dados pessoais, inclusive, a Lei Geral de Proteção de Dados aborda, no seu artigo 7º[11], quais as bases legais para que seja autorizado o tratamento de dados pessoais.

A presente dissertação não tem o escopo de exaurir ou trata base por base, posto que o afunilamento teórico se dá na aplicabilidade e adequação do Poder Público à Lei Geral de Proteção de Dados, deste modo, opta-se pelo tratamento de dados voltado à Administração Pública, nas suas funções típicas e atípicas.

A professora Laura Schertel e Bruno Bioni (2019, p. 171) fazem análise no sentido de que a Lei Geral de Proteção de Dados e o RGPD são muito próximos em seus conceitos e diretrizes, em especial por este ser modelo para aquele, de modo que, neste sentido, quanto à base legal do serviço público, fazem diferenciação entre a norma e o RGPD, pontuando da seguinte maneira:

---

[11] *In casu:* Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

> "No que diz respeito à base legal do serviço público, percebe-se uma diferença entre a LGPD e o RGPD, visto que a base da lei brasileira tem uma finalidade mais restrita ao tratar apenas de execução de políticas públicas. Tal base não abrange toda a gama de serviços executados pelo Estado em que se faz necessário o tratamento de dados, o que poderia gerar, à primeira vista, problemas para fundamentar legalmente diversas outras atividades estatais que exigem o processamento de informações pessoais. Um olhar atento 'à lei, todavia, permite corrigir tal déficit, na medida em que o art. 23 da LGPD acaba por enunciar uma base legal mais ampla para o tratamento de dados pelo setor público, podendo, portanto, também ser considerada uma base legal para o tratamento de dados pelos controladores públicos. Do exposto, percebe-se que, também no que se refere à racionalidade *ex ante* de proteção de dados, há grande convergência entre os sistemas europeu e brasileiro".

Assim, dentre as bases legais do artigo 7º, da Lei Geral de Proteção de Dados, segundo ensina a autora susodita, há uma suposta restrição da base de tratamento do Poder Público para que seja possível promover o tratamento tão somente quando se tratar de execução de políticas públicas previstas em lei, regulamentos ou respaldadas, ainda, em contratos, convênios ou instrumentos congêneres. Não obstante, o artigo 23[12], da Lei Geral de Proteção de Dados estabelece que o tratamento, pelo Estado, deve ser realizando atendendo sua finalidade precípua, qual seja, o interesse público, cabendo ainda cumprir as atribuições do serviço público. O artigo citado, ainda estabelece que compete ao Estado indicar um encarregado de dados pessoais.

---

[12] *In casu:* Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:
I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
II - (VETADO); e
III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência
IV - (VETADO). (Incluído pela Lei nº 13.853, de 2019)
§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

A Lei Geral de Proteção de Dados ocupou-se de trazer uma definição legal para a figura do encarregado de dados, a qual está prevista no artigo 5º, inciso VIII[13], sendo que a este compete, segundo a norma, ser indicado pelo controlador e operador, bem como atuar enquanto canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

Vainzof (2020) ensina que o encarregado de dados é peça fundamental na busca pela adequação à Lei Geral de Proteção de Dados, de modo que assevera ser a nomeação do encarregado de dados uma das mais importantes medidas de governança das organizações, incluindo-se aqui o Estado. Ressalta, ainda, que deve ser conferida autonomia e recursos para que o encarregado possa agir de maneira eficaz, posto que se trata de peça-chave no cumprimento normativo e na mitigação dos riscos.

Quanto ao encarregado, há conceituação trazida por Maria Leitão e Filipa Magalhães (2020, p. 10) que se mostra adequado, em razão da importância da função, vide

> "Pessoa designada pela organização que estará envolvida em todas as questões relacionadas com a proteção de dados pessoais e cujas principais funções envolvem informar e aconselhar a empresa sobre a conformidade da proteção de dados, aconselhar sobre a avaliação de impacto da proteção de dados, monitorizar a conformidade da proteção de dados, que inclui por exemplo formar equipe e realizar auditorias relacionadas com esta área e cooperar e atuar como ponto de contato com as autoridades de proteção de dados".

Dessarte, nota-se que o encarregado de dados é mais do que mero canal de comunicação, prestando-se a estar presente em todas as pautas que envolvam a proteção de dados pessoais dentro do contexto em que está inserido, prestando-se, ainda, ao aconselhamento do Poder Público para que o impacto do tratamento seja o menor possível, evitando-se eventuais danos e promovendo ações para que haja integral respeito à legislação e, por consequência, ao direito fundamental da privacidade e da proteção aos dados pessoais, inclusive nos meios digitais.

A nomeação do encarregado é dever do Poder Público, em que pese isso não esteja ainda acontecendo como deveria no âmbito da Administração Pública, em especial, nos municípios, que passam de cinco mil no Brasil, é plenamente possível contestar que

---

[13] *In casu:* Art. 5º Para os fins desta Lei, considera-se:
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

determinado ente da federação esteja cumprindo a Lei Geral de Proteção de Dados quando sequer houve a nomeação do encarregado de dados.

Ora, vale ressaltar que a figura do encarregado é essencial, de modo tal que é indicado pela Administração Pública para atuar não só como um canal de comunicação, mas realmente lidando com as situações de tratamento de dados pessoais, em razão disto, o encarregado de dados deve possuir capacidade e conhecimento multidisciplinar, sendo viável que faça análise jurídica, bem como de gestão de risco e governança de dados. O Estado do Paraná, em sua cartilha sobre o encarregado pelo tratamento de dados pessoais (2021, p. 6) a título de exemplo, vetou que o encarregado seja lotado nas unidades de Tecnologia de Informação (TI), bem como gestor responsável dos sistemas de informação do órgão ou entidade, justificando tal vedação por um possível conflito de interesses, já que cabe ao profissional citado a promoção da segurança da informação, ou seja, evita-se a concentração da proteção tão somente a um setor ou a uma pessoa, vide:

> "Para exercer as atribuições de Encarregado, o indicado deve possuir conhecimentos multidisciplinares, essenciais à sua atribuição, preferencialmente, os relativos aos temas de: privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público. Com a alteração promovida pela Medida Provisória 869/2018, o Encarregado pode ser pessoa física ou jurídica. Porém, apesar de não haver vedação legal para a designação do Encarregado como pessoa jurídica, um terceirizado pode ter dificuldades em exercer as suas funções de forma satisfatória, considerando que não conhece a fundo os procedimentos de governança do órgão e entidade. Importante observar que o inciso II, do § 2º, do art. 1º da Resolução CGE nº 13/2020 é taxativo quanto ao impedimento do Encarregado se encontrar lotado nas unidades de Tecnologia da Informação, ou ser gestor responsável de sistemas de informação do órgão ou da entidade. Essa vedação ocorre para que se evite o conflito de interesses, considerando que o profissional da área de TI é responsável pela segurança da informação".

Assim, tem-se que o encarregado de dados, conforme dito, deve ser pessoa capacitada e não possuir qualquer tipo de impedimento ou suspeição, vale mencionar que o encarregado deverá ter a identidade e as informações de contato divulgadas publicamente, de forma clara e objetiva, ainda, o encarregado possui um rol não taxativo de atividades previsto na Lei Geral de Proteção de Dados. O artigo 41, §§1º a 3º[14], estabelecem as diretrizes acerca desta figura

[14] *In casu:* Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
§ 2º As atividades do encarregado consistem em:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - receber comunicações da autoridade nacional e adotar providências;

emblemática da norma, cabe ainda ao Estado, vale mencionar, fornecer o aparato necessário para que seja possível o cumprimento dos seus deveres normativos.

Destarte, de todo o exposto, tem-se que a norma é cogente à Administração Pública, cabendo ao Estado a promoção das ações necessárias para que o tratamento de dados seja realizado dentro das bases normativas previstas no artigo 7º combinado com o artigo 23, da Lei Geral de Proteção de Dados. Ademais, ainda compete ao Poder Público a nomeação do encarregado de dados que deverá atuar não só como um canal de comunicação, mas atuando efetivamente nas pautas que abarcarem o tratamento de dados dentro do órgão ou entidade. Ainda, o Estado em sua função ininterrupta de coletor de dados não pode se furtar de sua responsabilidade e responsabilização no caso de vazamento de dados pela falta de denodo no tratamento, coleta e, por óbvio, da proteção dos dados pessoais das pessoas, inclusive nos meios digitais. Em razão disto, destina-se subtópico específico para abordar a responsabilidade do Estado advindo da Lei Geral de Proteção de Dados.

3.2 DA RESPONSABILIDADE DO ESTADO PELO VAZAMENTO DE DADOS PESSOAIS

Cumpre apresentar uma análise acerca da responsabilidade e da responsabilização do Estado em razão de alguma falha no cumprimento da Lei Geral de Proteção de Dados, em especial por se tratar os dados pessoais, inclusive nos meios digitais, de direito fundamental positivado na Constituição Federal e que para ter a sua plena eficácia demanda a tomada de ação pelo Estado, ou seja, há necessidade de garantias para que o direito seja resguardado, de modo tal que a responsabilização daquele que desrespeita o direito fundamental, ainda que seja o Estado, deve ocorrer.

Inicialmente, importa mencionar que a figura do encarregado de dados não pode ser responsabilizada diretamente, inicia-se com a pontuação acerca do encarregado pela congruência temática com que se encerrou o último subtópico. Deste modo, quanto ao encarregado, tem-se que sua função é consultiva, não obstante, a não responsabilidade do

---

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
§ 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

encarregado não é absoluta, ou seja, não o isenta de responder em casos excepcionais de vazamento de dados, quando houver comprovação de imprudência, imperícia, negligência, ou até dolo em induzir o agente de tratamento de dados a agir em desrespeito ao que preceitua a Lei Geral de Proteção de Dados (Paraná, 2021, p. 13).

No campo da responsabilidade civil impera rememorar que esta se dá em razão de toda a manifestação do ser humano trazer em si o problema da responsabilidade, ou seja, as ações advindas da atividade humana geram consequências passíveis de responsabilização. (Dias, 2006, p. 3).

Acerca do tema, Renata Queiroz (2022, p. 79) ensina que:

> "Em um primeiro momento, é importante falar da responsabilidade civil realizando um contraste entre as responsabilidades subjetivas e objetivas, para que, então, possa ser traçado da forma correta um caminho para compreender a responsabilidade civil proposta pela LGPD, para, após, refletir sobre o regime no qual se enquadra a responsabilidade civil do encarregado de proteção de dados pessoais. No âmbito jurídico, a responsabilidade civil decorre da violação de um dever, ocasionando um dano. O responsável pelo ato deverá ressarcir o dano decorrente da violação de um precedente dever jurídico. Daí ser possível dizer que toda conduta humana, violando dever jurídico originário, causa prejuízo a outrem, é fonte geradora de responsabilidade civil".

Nesta mesma linha, pode-se afirmar que a ideia de responsabilização remete a uma reparação, a uma punição ou ainda a uma prevenção, a responsabilidade é matéria que os civilistas se debruçam sobre, mas advém não só do direito civil, mas da própria constituição federal (Rosenvald, 2017, p. 21).

Das lições trazidas acima, verifica-se que a responsabilidade civil possui ao menos três funções precípuas, quais sejam, a de punir, a de reparar ou satisfazer, bem como a de prevenir. Noutras palavras, quando uma atividade humana causa dano a outrem haverá a possibilidade de responsabilização, a qual, se perpetrada, gerará um efeito sancionatório no causador do dano, visando ainda uma reparação ou uma satisfação do direito do lesado, bem como acarretará um efeito preventivo, ou seja, em razão da punição, tanto o causador do dano como outros que tomem ciência da pena, evitarão o cometimento de danos.

O afunilamento teórico da presente dissertação se destina à Administração Pública, razão pela qual será abordada a responsabilidade dentro do Poder Público, e acerca deste contexto de responsabilização, tem-se que o Estado exerce poder de império, de modo que possui um acervo imensurável de dados pessoais, não havendo meios para se equiparar o poderia do Estado face ao titular dos dados pessoais, pode-se afirmar, assim, a existência de

uma relação de hipossuficiência do titular de dados face ao poder público. De modo a buscar arrefecer a voracidade da coleta de dados surge a Lei Geral de Proteção de Dados, a qual visa o reequilíbrio da relação titular de dados e o coletor, criando, portanto, responsabilidade do Estado e necessidade de adequação, esta já tratada anteriormente. Deste modo, notória a possibilidade de responsabilização do Estado em respeitar a Lei Geral de Proteção de Dados e em garantir o direito fundamental ao titular, qual seja, da proteção aos dados pessoais, inclusive nos meios digitais (Drumond, 2022, p. 9).

Deste modo, verifica-se que para aferir a responsabilização do Estado é importante que este já esteja adaptado à Lei Geral de Proteção de Dados, este que é o passo inicial, bem como defina a figura do controlador e do encarregado de dados, em seguida, institua um grupo permanente, seja uma comissão ou comitê, com a finalidade de executar e deliberar a política de proteção de dados pessoais, a qual será adotada pela Administração Pública. É necessário que se implemente mecanismos de governança corporativa gerando, por consequência, um fluxograma das informações bem como o devido tratamento dos dados (Cunda *et al*., 2021, p. 206).

Deste modo, atesta-se que a responsabilidade civil pode ser dar quando há uma violação de algum direito de outrem, a origem da responsabilidade, ou seja, sua fonte pode ser uma relação jurídica obrigacional, um contrato, ou ainda, preceito geral de direito ou até a própria lei (Cavalieri Filho, 2020, p. 25). Inclusive, a responsabilidade do Estado advém diretamente da Carta Maior e da própria Lei Geral de Proteção de Dados.

Quanto à modalidade de responsabilização do Estado, tem-se que ao analisar a Lei Geral de Proteção de Dados não se tem a indicação se a responsabilidade é objetiva ou subjetiva, em especial pela ausência dos termos independentemente de culpa ou da menção sobre a modalidade culposa, não obstante, o tema ainda será abordado neste tópico (Queiroz, 2022, p. 82).

Não obstante, tem-se que a Constituição Federal estabelece qual a modalidade de responsabilidade do Estado, qual seja, a objetiva, conforme estabelece o artigo 37, § 6º, desta forma, sanada a discussão acerca de qual modalidade de responsabilidade civil se enquadra ao Poder Público.

A Lei Geral de Proteção de Dados possui seção própria acerca da responsabilidade e do ressarcimento de danos, de modo que, no artigo 42[15], aborda a responsabilidade do controlador ou do operador que causar danos patrimoniais, morais, sejam individuais ou coletivos, quando em violação à norma geral, deve reparar. Estabelece, ainda, meios para assegurar a efetiva indenização ao titular dos dados, bem como regra de inversão do ônus da prova e, por fim, delineia a possibilidade do exercício do direito de regresso contra o real causador do dano (Brasil, 2018).

Nalguns momentos trata-se da figura do controlador, do titular e do operador. Importante mencionar que o primeiro é entendido como a pessoa natural ou jurídica a quem compete tomar a decisão referente ao tratamento de dados pessoais, enquanto o titular é a pessoa natural que tem os dados tratados, enquanto o operador é a pessoa natural ou jurídica que realiza o tratamento dos dados pessoais, o que faz em nome do controlador, importante mencionar que tanto o controlador como o operador podem ser pessoas jurídicas de direito público ou privado, estes são os conceitos retirados da Lei Geral de Proteção de Dados, conforme artigo 5º, incisos V ao VII[16] (Brasil, 2018).

O artigo 43, da Lei Geral de Proteção de Dados[17] estabelece as hipóteses em que os agentes de tratamento não serão responsabilizados, ou seja, a Lei traz hipóteses excludentes da

---

[15] *In casu:* Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

[16] Art. 5º Para os fins desta Lei, considera-se:
V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

[17] *In casu:* Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

responsabilidade, ou seja, ainda que ao Estado se aplique a responsabilidade objetiva, não se aplica a teoria do risco integral, como no direito ambiental, de modo tal que é possível que existam hipóteses nas quais a Administração Pública possa se eximir da responsabilização, em especial quando não realizaram tratamento dos dados que lhes são atribuídos, quando mesmo tendo realizado o tratamento não houve violação à norma ou, ainda, quando houver culpa exclusiva do titular dos dados ou de terceiro (Brasil, 2018).

A Lei Geral de Proteção de Dados, ainda em sua seção específica para tratar sobre a responsabilidade e ressarcimento dos danos decorrentes do tratamento indevido dos dados pessoais, conforme o artigo 44, *caput* e incisos[18], indica que o tratamento é irregular quando deixa de observar a legislação ou quando não disponibiliza da segurança que o titular dele espera, devendo o tratamento ser realizado dentro da técnica necessária para evitar danos.

Tornando à discussão acerca do regime de responsabilidade adotado pela Lei Geral de Proteção de Dados, tem-se que há divergência doutrinária. Guedes, Tepedino e Terra (2020, p. 242), ensinam ser a responsabilidade civil subjetiva, vide:

> "Para além disso, há mais um indicativo na LGPD que aponta para o regime de responsabilidade subjetiva: o inciso II do Art. 43. De acordo com esse dispositivo, os agentes de tratamento só não serão responsabilizados quando provarem, entre outros fatores, "que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados" (...) No inciso I do Art. 43, o legislador isenta de responsabilidade os agentes que provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído. Essa excludente de responsabilidade está, evidentemente, afastando o nexo de causalidade entre a conduta do agente e o dano. Como se refere à relação causal, é excludente que poderia existir ainda que a responsabilidade consagrada pela LGPD fosse a objetiva".

Dessarte, citou-se uma doutrina que defende ser a responsabilidade subjetiva, não obstante a existência de outras num mesmo sentido. Ademais, vale trazer a visão doutrinária no sentido de que a responsabilização trazida, em regra, pela Lei Geral de Proteção de Dados seria objetiva.

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

[18] *In casu:* 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

Há doutrina no sentido de que quando inexiste uma segurança do titular de dados, conforme prevê o artigo 44, da Lei Geral de Proteção de Dados, já tratado anteriormente, então a responsabilidade será objetiva (Schreiber, 2021, p. 336).

Queiroz (2022, p. 89), acerca da responsabilidade civil na Lei Geral de Proteção de Dados, tendo promovido o comparativo da doutrina que defende a responsabilização subjetiva e objetiva, conclui que:

> "Apesar da ausência de previsão expressa e do uso de expressões diversas em sua redação, apresentadas ambas correntes doutrinárias acerca do regime da responsabilidade civil adotada pela LGPD, considerando que a atividade do agente de tratamento impõe riscos aos direitos dos titulares, parece mais acertada a adoção da responsabilidade objetiva. Isso porque, além dos argumentos defendidos pela doutrina abordados neste capítulo, os riscos aos quais estão expostos os titulares de dados resultam em danos a direito fundamental, por isso cabe aos agentes a obrigação de indenizar os prejuízos causados aos titulares de dados, afastando destes o dever de comprovar a existência de conduta culposa por parte do controlador ou operador".

Nota-se que a interpretação se dá em razão da notória hipossuficiência, ao menos em regra, do titular dos dados pessoais, imperando, assim, a responsabilidade objetiva daquele que coletou, tratou e, eventualmente, disseminou e/ou causou algum tipo de dano àquele que é o titular de dados.

Ressalta-se que só se discute a responsabilidade civil quando houver uma inobservância dos deveres expressamente trazidos pela Lei Geral de Proteção de Dados, de modo que deve preponderar, enquanto não houver uma alteração legislativa que ponha fim à presente discussão, a responsabilidade objetiva, já que o bem jurídico tutelado pela Lei Geral de Proteção de Dados contempla o risco como o núcleo essencial para delimitar os critérios de imputação advindos de sua violação, de modo que, aquele titular de dados pessoais que sofrer pela ruptura com o dever legal, tem-se o dever de reparar (Martins e Faleiros Júnior, 2020, p. 293).

Quanto à responsabilidade civil do Estado a Lei Geral de Proteção de Dados ocupou-se de tratar em seção específica da norma, prevendo que em havendo infração à norma em decorrência do tratamento de dados pessoais promovidos por órgão pública, cabe à Autoridade Nacional de Proteção de Dados o envio de informe com as medidas cabíveis para fazer cessar

a violação, esta é a previsão contida no artigo 31[19], da Lei Geral de Proteção de Dados (Brasil, 2018).

O texto normativo ainda confere à Autoridade Nacional de Proteção de Dados poder de polícia, ou seja, o artigo 32[20], da Lei Geral de Proteção de Dados, estabelece que pode a Autoridade Nacional de Proteção de Dados requisitar ao Poder Público publicação de relatórios de impacto, concernentes à proteção de dados pessoais, bem como sugerir a adoção de padrões e de boas práticas para o tratamento de dados pessoais a ser realizado pela Administração Pública (Brasil, 2018).

A própria Lei Geral de Proteção de Dados prevê em seu artigo 55-J, inciso XI[21], que compete à Autoridade Nacional de Proteção de Dados o poder para solicitar a qualquer momento de quaisquer das entidades do Poder Público que realizem operações de tratamento de dados pessoais, de modo que, notoriamente, o Estado também deve ser fiscalizado pela Autoridade Nacional e pode ser sancionado, inclusive na via administrativa quando houver desrespeito à norma citada (Brasil, 2018).

A responsabilização administrativa, já citada acima, pode ser imputada e apurada pela Autoridade Nacional de Dados, a qual já foi outrora citada neste trabalho, mas ainda não conceituada e discutida. Elucidando a temática, tem-se que este é o órgão da Administração Pública que carrega a responsabilidade por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional, conforme o artigo 5º, inciso XIX[22], da norma susodita (Brasil, 2018).

No ano de 2022 a Lei Geral de Proteção de Dados foi alterada para melhor abordar a Autoridade Nacional de Proteção de Dados, de modo que a partir de então a autoridade nacional passou a ter *status* de autarquia especial, dotada de autonomia técnica e decisória, possuindo

---

[19] *In casu:* Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.
[20] *In casu:* Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.
[21] Art. 55-J. Compete à ANPD:
XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei
[22] Art. 5º Para os fins desta Lei, considera-se:
XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

patrimônio próprio e tendo sua sede e foro no Distrito Federal, ou seja, passou a ser verdadeira agência reguladora, conforme estabelece o artigo 55-A[23], da norma em discussão.

Do que foi demonstrado no presente capítulo, formatou-se uma subdivisão em dois subtópicos que tiveram por finalidade, inicialmente, apresentar a aplicação da Lei Geral de Proteção de Dados ao Estado, bem como as nuances atinentes à sua aplicação e, em seguida, apresentou-se a discussão, sem por óbvio, a exaurir, acerca da responsabilidade do Estado pelo descumprimento à Lei Geral de Proteção de Dados, apresentou-se a responsabilidade civil e administrativa, permeando qual a modalidade de responsabilidade prevista na norma, a quem compete a fiscalização da aplicação da norma, concluindo-se que compete à Autoridade Nacional de Proteção de Dados, a qual atua como verdadeira agência regulatória. Concluiu-se que a Autoridade Nacional tem atribuição para fiscalizar e atuar sobre o Poder Público. Deste modo, ultrapassada a discussão deste capítulo, impera dar prosseguimento teórico ao escopo da presente dissertação.

4 ANÁLISE DE CASOS PRÁTICOS E APONTAMENTO DE SOLUÇÕES

O capítulo que antecede a conclusão da presente dissertação tem o escopo de apresentar ao leitor casos práticos, voltados ao Poder Público, em que houve a análise da aplicação da Lei Geral de Proteção de Dados ao Estado, de modo tal que serão demonstradas ações judiciais e administrativas que ensejaram uma condenação ou mudança de práticas por parte dos entes da federação, seja em razão da Lei Geral de Proteção de Dados ou, ainda anteriormente, quando se via como direito fundamental a autodeterminação informativa.

4.1 CASOS JUDICIAIS ACERCA DA PROTEÇÃO DE DADOS

O objetivo neste subtópico será apresentar ao leitor casos concretos em que se discutiu, na via judicial, acerca da proteção de dados pessoais, apresentando julgamentos emblemáticos, em especial aquelas derivadas do Supremo Tribunal Federal e cortes superiores para que seja possível entender qual a aplicação que tem sido dada quando da análise jurisdicional.

Inicialmente discutir-se-á a Arguição de Descumprimento de Preceito Fundamental 695 do Distrito Federal, a qual teve por relator o eminente Ministro Gilmar Mendes. O caso em

[23] Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.

estudo é de ação de controle concentrado de constitucionalidade proposta pelo Partido Socialista Brasileira em face de ato do Poder Público, o qual, com base em decreto, a saber, o de número 10.046/2019, autorizou que fossem compartilhados com a Agência Brasileira de Inteligência (ABIN) dados pessoais de aproximadamente 76 (setenta e seis) milhões de brasileiros, cerca de 36% (trinta e seis porcento) da população do Brasil, à época.

A tese sustentada na arguição de descumprimento de preceito fundamental citada anteriormente foi a de que o Poder Público Federal estava violando preceitos fundamentais da proteção da privacidade, a garantia de proteção aos dados pessoais e da autodeterminação informativa, bem como havia um risco basilar ao princípio democrático, posto que havia risco de vigilância massiva sem controle dos cidadãos, sem que houvesse qualquer envolvimento destes com ações ou prática ilegais.

O ministro relator valeu-se de uma análise histórica sobre a autodeterminação informativa, inicialmente abordada pela Corte Constitucional alemã, a qual acabou por criar um direito que não estava previsto, claramente, no texto constitucional, mas decorreria da proteção à dignidade da pessoa humana, bem como outros valores constitucionais, como a intimidade e a privacidade. (Supremo Tribunal Federal, 2022, p. 21).

O voto proferido e vencedor esclareceu uma série de nuances quanto ao tratamento e proteção dos dados pessoais pelo Poder Público, esclareceu que já na Ação Direta de Inconstitucionalidade 6.387, de relatoria da Ministra Rosa Weber, o Supremo Tribunal Federal reconheceu a existência de um direito fundamental autônomo, qual seja, a proteção de dados pessoais e à autodeterminação informativa, tendo usado como exemplo o julgamento do suprema corte alemã, não obstante, a Emenda Constitucional 115/2022 positivou esse direito fundamental, de modo que é indiscutível a natureza do direito à proteção aos dados pessoais, inclusive nos meios digitais. A conclusão do julgado merece ser colacionada para que se tenha claro na visão dos ministros qual o cerne e diretriz a ser tomada na temática proposta (Supremo Tribunal Federal, 2022):

> "O tratamento de dados pessoais pelo Estado é essencial para a prestação de serviços públicos. Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais. Interpretação conforme à Constituição para subtrair do campo semântico eventuais aplicações ou interpretações que conflitem com o direito fundamental à proteção de dados pessoais. O compartilhamento de dados pessoais entre órgãos e entidades da Administração Pública, pressupõe: a) eleição de propósitos legítimos, específicos e explícitos para o tratamento de dados (art. 6º,

> inciso I, da Lei 13.709/2018); b) compatibilidade do tratamento com as finalidades informadas (art. 6º, inciso II); c) limitação do compartilhamento ao mínimo necessário para o atendimento da finalidade informada (art. 6º, inciso III); bem como o cumprimento integral dos requisitos, garantias e procedimentos estabelecidos na Lei Geral de Proteção de Dados, no que for compatível com o setor público. O compartilhamento de dados pessoais entre órgãos públicos pressupõe rigorosa observância do art. 23, inciso I, da Lei 13.709/2018, que determina seja dada a devida publicidade às hipóteses em que cada entidade governamental compartilha ou tem acesso a banco de dados pessoais, "fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos". O compartilhamento de informações pessoais em atividades de inteligência deve observar a adoção de medidas proporcionais e estritamente necessárias ao atendimento do interesse público; a instauração de procedimento administrativo formal, acompanhado de prévia e exaustiva motivação, para permitir o controle de legalidade pelo Poder Judiciário; a utilização de sistemas eletrônicos de segurança e de registro de acesso, inclusive para efeito de responsabilização em caso de abusos; e a observância dos princípios gerais de proteção e dos direitos do titular previstos na LGPD, no que for compatível com o exercício dessa função estatal. O acesso ao cadastro base do cidadão deve observar mecanismos rigorosos de controle, condicionado o compartilhamento e tratamento dos dados pessoais à comprovação de propósitos legítimos, específicos e explícitos por parte dos órgãos e entidades do Poder Público. A inclusão de novos dados na base integradora e a escolha de bases temáticas que comporão o Cadastro Base do Cidadão devem ser precedidas de justificativas formais, prévias e minudentes, cabendo ainda a observância de medidas de segurança compatíveis com os princípios de proteção da Lei Geral de Proteção de Dados Pessoais, inclusive a criação de sistema eletrônico de registro de acesso, para fins de responsabilização em caso de abuso. O tratamento de dados pessoais promovido por órgãos públicos que viole parâmetros legais e constitucionais, inclusive o dever de publicidade fora das hipóteses constitucionais de sigilo, importará a responsabilidade civil do Estado pelos danos suportados pelos particulares, associada ao exercício do direito de regresso contra os servidores e agentes políticos responsáveis pelo ato ilícito, em caso de dolo ou culpa".

O que ficou consignado pelo Supremo Tribunal Federal é emblemático para o Estado e para a devida interpretação acerca da Lei Geral de Proteção de Dados. Antes o que parecia ser comum, ou seja, o livre trânsito de dados pessoais entre entes públicos já não é mais aceito, em especial pelo *status* de direito fundamental. Inicialmente, reconhece-se que o tratamento de dados em verdade está no cerne da atividade estatal, mas que isso não serve de pretexto para o tratamento indevido, devendo-se aplicar a Lei Geral de Proteção de Dados no que couber à Administração Pública.

Outro fator preponderante é o de que deve existis uma sistemática própria no tratamento dos dados pessoais pelo Estado, de modo que o compartilhamento seja limitado e que aqueles que tiverem acessos aos dados tenha um lastro de acesso, ou seja, fique possível à Administração Pública saber quem acessou o dado pessoal, de modo que, em eventual condenação, possa exercer seu direito de regresso sobre os servidores responsáveis.

É nesta linha que merece ser feito apontamento, ou seja, o servidor responsável pelo tratamento ou aquele que acessou e desvirtuou a finalidade no tratamento ou no acesso, ou seja, aquele que foi o causador do dano, em nome do Estado, poderá sofrer as sanções cabíveis e indenizar o Poder Público em ação de regresso caso tenha agido, seja com dolo ou culpa, na configuração do dano.

O Estado, quando atuando com os dados pessoais, seja no tratamento, compartilhamento, ainda que interno, ou afins, deve deixar clara qual a finalidade do ato tomado, a motivação deve ser expressa, a razoabilidade e proporcionalidade devem servir como vetores, reitera-se que o uso de sistemas eletrônicos e de controle de acesso são essenciais para que seja possível verificar o lastro de acesso e por quais locais os dados podem ser tramitados.

É importante ressaltar a clareza do Supremo Tribunal Federal em estabelecer que o tratamento desleal, ou seja, o tratamento que importe em violação dos parâmetros constitucionais e legais poderá importar em responsabilização civil do Estado, em decorrência dos danos sofridos pelo titular dos dados pessoais, deixando claro que é possível e até devido o exercício do direito de regresso em face não só contra os servidores responsáveis pelo ato ilícito, mas também pelos agentes políticos responsáveis, o que parece ser algo recente. Explica-se. Notoriamente nos períodos eleitorais aqueles que compõem a máquina pública, enquanto agentes políticos, possuem acesso a dados pessoais dos cidadãos de modo a facilitar o caminho até o eleitor e, de alguma forma, praticar um abuso de poder político, ainda que velado, mas a partir da coleta indevida de dados pessoais.

Acerca da responsabilização, vale mencionar que a decisão colacionada do Supremo Tribunal Federal, em suas razões, ainda estabelece que "a transgressão dolosa ao dever de publicidade estabelecido no art. 23, inciso I, da LGPD, fora das hipóteses constitucionais de sigilo, importará a responsabilização do agente estatal por improbidade administrativa, nos termos do art. 11, inciso IV, da Lei 8.429/1992" (Supremo Tribunal Federal, 2022, p. 93). Assim, o Supremo Tribunal Federal dá a devida importância e de maneira didática, incentivando o efeito preventivo, afirma quais as possíveis sanções, tanto para o Estado, como para os seus agentes.

Outro caso emblemático julgado pelo Supremo Tribunal Federal se deu na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.561 de Tocantins, relatoria do eminente ministro Edson Fachin, o caso abordava Lei do Estado do Tocantins que estabelecia um cadastro estadual de usuários e dependentes de drogas, o qual estaria sob a tutela da secretária estadual de segurança pública, o cadastro deveria possuir informações concernentes ao registro

de ocorrências policiais, reincidência e previa o acesso a dados pessoais daqueles envolvidos no cadastro. (Supremo Tribunal Federal, 2020).

Na decisão exarada o douto ministro ressalta que no Estado de Direito democrático os direitos fundamentais devem ser respeitados e que o cadastro proposto desrespeitava diretamente entre outros direitos o direito fundamental à intimidade e à vida privada, ressalta-se que à época ainda não estava positivado o direito fundamental à proteção de dados, inclusive nos meios digitais. No mais, há trecho do voto que merece ser colacionado, quando o ministro adentra à análise do cadastro proposto com a Lei Geral de Proteção de Dados, veja:

> "É assim que a evolução dos sistemas de tratamento de dados e a centralidade que eles adquirem hoje no funcionamento da política, da economia, do direito, e dos demais setores da sociedade, fizeram com que o constitucionalismo brasileiro se reconfigurasse para atualizar os princípios que já se inscreviam no texto da Constituição da República. Nessa toada, a Lei Geral de Proteção de Dados, Lei n.º 13.709/2018, traz em seu bojo o princípio da autodeterminação informativa (art. 2º, II) e a inviolabilidade da intimidade, da honra e da imagem (art. 2º, IV), a partir da concretização de princípios constitucionais que já se encontram plenamente em vigor na ordem jurídico brasileira. Ali, dados referentes à saúde são classificados como "dados pessoais sensíveis" (art. 5º, II) e, por isso, seu tratamento submete-se a um regime jurídico especial (art. 11). Esse sistema constitucional especial de proteção é violado pela lei impugnada, a qual, ademais, não prevê formas de controle prévio à inclusão no cadastro, não prevê a comunicação e o consentimento do interessado e, para a sua exclusão, exige laudo médico e informação oficial sobre a não reincidência. Tampouco existe protocolo claro de proteção e tratamento desses dados".

A decisão menciona o direito à autodeterminação informativa e estabelece que a Lei Geral de Proteção de Dados deve ser respeitada pelo Estado, não somente com mero formalismo, mas na prática. Menciona-se que a decisão estabelece a necessidade de uma sistemática, ou seja, uma forma de controle quanto à inclusão, a colheita, o tratamento dos dados pessoais que seriam colhidos, em especial, dados de saúde, que são considerados como dados pessoais sensíveis. Funções como a comunicação ao titular dos dados pessoais, o seu consentimento em algumas hipóteses, aqueles que não se enquadrarem no base legal de cumprimento da norma, bem como a possibilidade de exclusão ou cessação do tratamento são direitos inerentes ao titular que sequer foram respeitados pela norma, razão pela qual tida por inconstitucional.

Vale ressaltar que uma análise conjunta dos dois processos supracitados leva ao entendimento de que o controle quanto aos dados pessoais e quem os acessa devem ser rigorosos a ponto de evitar danos que podem ser considerados irreparáveis. O tratamento de

dados pessoais deve ser levado com seriedade, em especial pelo Poder Público que é aquele que coleta e trata dados por primazia para cumprir as funções estatais.

Outro julgado relevante do Supremo Tribunal, este de relatoria do Ministro Luiz Fux que envolve o direito à saúde e outra lei estadual, esta no sentido de que haveria uma obrigação na adoção de medidas de segurança que evitem, impeçam ou dificultem a troca de recém-nascidos nas dependências de hospitais, públicos ou privados e que possibilitem a posterior conferência via exame de DNA acerca da filiação, devendo ser colhido o material da genitora e do filho, ainda na sala de parto (Supremo Tribunal Federal, 2023).

O julgado se deu também em controle concentrado de constitucionalidade, via ação direta de inconstitucionalidade número 5.545 do Rio de Janeiro, nos autos foram sopesados direitos fundamentais como o da personalidade e da intimidade, bem como da privacidade. O direito de personalidade numa análise quanto à perda do vínculo genético, posto que este violaria diretamente o direito à identidade genética, o direito à privacidade no sentido de que é prerrogativa exigir do estado uma abstenção de intervenção em sua intimidade e vida privada, ou seja, possui caráter negativo em alguns momentos, enquanto em outros exige uma prestação positiva do Estado, posto que se impõe o debate sobre medidas de segurança a respeito dos dados que incidam diretamente sobre a esfera privada do indivíduo, o que importa numa "salvaguarda das informações pessoais armazenadas tanto pelo setor público como pelo setor privado" (Supremo Tribunal Federal, 2023, p. 2)

Há trecho do voto (2023, p. 19) que merece ser colacionado, posto que enfrenta a análise sobre os riscos que a detenção pelo próprio Estado do material genético poderia causar, vide:

> "O material genético, além das informações relativas ao parentesco, registra muitos outros dados reveladores de características genotípicas dos indivíduos, inclusive no que se refere à predisposição ao desenvolvimento de certas doenças genéticas, etnia, sexo etc., mediante o sequenciamento de DNA. Partindo dessa perspectiva, não tenho dúvidas de que a utilização inadequada é de enorme potencial lesivo para a dignidade e a personalidade do indivíduo. (...) A par disso tudo, a lei impugnada também viola o direito fundamental à proteção de dados pessoais. Quanto ao tema, esta Suprema Corte, ao julgar as ADIs 6.387, 6.388, 6.389, 6.390 e 6.393, teve a oportunidade de declarar seu assento constitucional, antes mesmo do advento da Emenda de n. 115/2022, que acrescentou o inciso LXXIX ao art. 5º da Constituição de 1988. A norma impugnada afronta também o direito fundamental à autodeterminação informativa ao obrigar a colheita do material genético de todos os bebês e mães. Quanto às crianças, elas nem mesmo têm capacidade biopsíquica ou jurídica para consentir; em relação às mães, tampouco seriam indagadas, segundo propõe a lei impugnada, quanto a quererem ou não arquivar o seu material genético. E, mesmo que o fossem, estariam em contexto puerperal, que tem o potencial, não raro, de toldar o

> entendimento da pessoa. Isso para não referir a quase impossibilidade de falar em consentimento informado numa situação como a cogitada".

No voto do ministro Luiz Fux fica muito clara a ideia de que o Estado precisa se adequar para que a colheita de dados sensíveis não possa importar em futuro dano à direitos fundamentais como a dignidade e a personalidade do indivíduo e, em especial, ao direito fundamental à proteção aos dados pessoais. O caso em discussão demonstra hipótese em que os dados pessoais não são coletas pelos meios digitais, necessariamente. Ademais, menciona-se de forma explícita a necessidade de respeito à autodeterminação informativa, ou seja, o titular dos dados precisa poder ser capaz de concordar com a coleta de seus dados, em especial, no caso concreto em que se trata de dados pessoais sensíveis, vide artigo 5º, inciso II, da Lei Geral de Proteção de Dados[24].

Salienta-se que a concordância demanda ciência notável acerca do que se está coletando, quais os riscos futuros e a possibilidade de pedido de eventual descarte, posterior, deste modo, a determinação cogente de que o Estado poderia promover tal coleta e tratar sem sequer mencionar qual a operacionalização do tratamento destes dados sensíveis faz com que seja declarada inconstitucional a lei em comento.

Na mesma ação direta de inconstitucionalidade (2023, p. 38), o ministro Alexandre de Moraes faz relevante apontamento quando assevera que "o crescente volume de dados pessoais recolhidos torna cada vez mais difícil garantir a sua verdadeira dissociação irreversível da pessoa a que dizem respeito". Em razão disto a importante de consentimento prévio e livre, cabendo aos Estados desenvolver esforços no sentido de proteger os dados pessoais dos indivíduos e, nesse caso, os dados genéticos associados ao titular dos dados pessoais sensíveis. Dessarte, é necessário que o Estado disponha de condições de segurança e tratamento adequadas para o tratamento dos dados, inclusive com a atuação da Autoridade Nacional de Proteção de Dados.

Encerrar-se-á o presente tópico com análise de julgado promovido pelo Tribunal Superior Eleitoral, de relatoria do Ministro Edson Fachin, no Processo Administrativo nº 0600231-37.2021.6.00.0000 – São Paulo. Os autos mencionados são relativos a caso concreto em que candidato alcançou a condição de suplente do cargo de vereador e pediu a retirada de

---

[24] *In casu:* Art. 5º Para os fins desta Lei, considera-se:
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural

informações pessoais constantes do sistema e divulgação de candidaturas e contas eleitorais, nos termos da Lei Geral de Proteção de Dados, o pedido se fundamentou em razão de ameaças sofridas e outros dissabores decorrentes do acesso facilitado aos seus dados pessoais (Tribunal Superior Eleitoral, 2021).

No caso apresentado se discutiu o princípio da transparência no Direito Eleitoral e o direito à privacidade e à proteção de dados pessoais, no âmbito eleitoral, conforme consigna o ministro, há interesse público na publicização de dados pessoais relativos a candidatos, não obstante, quando o caso concreto demonstra que a publicização, no caso, a manutenção da publicidade dos dados pessoais do candidato podem ensejar riscos de várias ordens, verifica-se a necessidade de flexibilizar o amplo acesso aos dados pessoais do titular dos dados.

Em seu voto o ministro Edson Fachin (2021, p. 13) faz pontuações relevantes e atinentes à temática da presente dissertação, conforme se colaciona abaixo:

> "Portanto, é diante de todas essas circunstâncias, que aparentemente se contrapõem, que deve ser construída a nova dinâmica de tratamento de dados pessoais dentro da Administração Pública, buscando se compatibilizar a publicidade própria do atuar desta última com as garantias asseguradas em prol do titular de dados pessoais pela LGPD. Partindo de tal premissa, impõe-se crítico reflexionar acerca dos moldes em que hoje se opera o requerimento de registro de candidatura, especificamente no que diz com a coleta e exposição de dados pessoais do candidato, uma vez que as máximas da finalidade, da necessidade e da adequação perpassam justamente a noção limitatória das atividades de tratamento de dados pessoais. Aquele que opta por concorrer a um mandato eletivo há de suportar, por via de consequência,
> rotina mais exposta ao escrutínio da sociedade. Portanto, indubitável que os limites da privacidade de quem elege a vida pública são realmente mais elastecidos. Entretanto, há de se ter cautela na condução de tal raciocínio, pois tal noção de elastecimento não pode ser alargada a ponto de implicar verdadeira nulificação daqueles lindes. No curso do período crítico do processo eleitoral, a publicização de determinados dados e informações relativas aos candidatos é crucial para viabilizar o manejo de relevantes instrumentos processuais a legitimados (como a própria ação de impugnação de registro de candidatura), assegurar a transparência das campanhas e a livre atuação da imprensa, nortear a própria escolha dos eleitores".

O julgado revoluciona quando demonstra que até mesmo na seara eleitoral em que notoriamente se entende pela flexibilização do "homem público", ou seja, daquele que busca ou que já atua no meio político, deve ser promovido uma flexibilização da publicidade quando houver a necessidade de assegurar direitos fundamentais primordiais. No julgado restou determinado que um grupo específico de estudo e implementação da Lei Geral de Proteção de Dados atuasse apresentando soluções viáveis para as necessidades da era informacional em que se vive na atualidade.

Deste modo, verifica-se que o presente subtópico teve a finalidade de apresentar decisões judiciais que versassem sobre a Lei Geral de Proteção de Dados e o Poder Público, demonstrando ao leitor que o Poder Judiciário tem sido acionado, em especial nas suas esferas superiores para dar cabo à situações de lesão aos titulares de dados pessoais. Quanto às decisões do Supremo Tribunal Federal, todas em controle concentrado de constitucionalidade, discutindo normas de efeito abstrato que podiam causar dano em larga escala, enquanto a decisão colacionada do Tribunal Superior Eleitoral foi capaz de demonstrar que, mesmo a seara eleitoral que é notória pela flexibilização da privacidade, é necessária uma releitura de institutos para salvaguardar o direito fundamental à proteção de dados pessoais, inclusive nos meios digitais. O próximo subtópico se ocupará de demonstrar processos administrativos que versem sobre a Lei Geral de Proteção de Dados.

4.2 CASOS ADMINISTRATIVOS ACERCA DA PROTEÇÃO DE DADOS PELA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

O subtópico proposto tem o escopo de apresentar ao leitor processos em que se discutiu a aplicação da Lei Geral de Proteção de Dados ao Poder Público, em especial processos em que se demonstra que o Estado deixou de respeitar a norma supracitada de alguma forma que foi suficiente a ensejar punição ou investigação. Ressalta-se que, conforme já foi debatido nesta dissertação, é inarredável o fator de que a Lei Geral de Proteção de Dados se aplica ao Estado, ao mesmo tempo que é notório que o Poder Público ainda tem deixado de cumprir norma que se lhe aplica e vem, inclusive, sofrendo sanções em razão disto.

No ano de 2023 a Autoridade Nacional de Proteção de Dados divulgou lista de processos sancionatórios em curso que envolvia órgãos públicos, entre eles alguns devem ser aqui citados, menciona-se o Ministério da Saúde que passa por investigação pela não nomeação de um encarregado de dados pessoais, bem como pela ausência de comunicação de incidente de segurança (Brasil, 2023).

A Secretaria de Estado de Saúde de Santa Catarina, num mesmo sentido, possuía investigação em curso em razão da possível ausência de comunicação a titulares de incidente de segurança, bem como pela ausência de medidas de segurança e não atendimento à determinações da Autoridade Nacional de Proteção de Dados (Brasil, 2023).

Em síntese, os casos citados demonstram a inexistência do devido cuidado que acarreta no vazamento de dados e posterior abstenção no cumprimento do dever legal de informar os

titulares dos dados defraudados acerca do vazamento ou intercorrência com os dados que estavam sob a tutela do órgão público, outro fator que demanda a atenção é a de que a nomeação do encarregado de dados é primordial para que se exista o mínimo possível na aplicação da Lei Geral de Proteção de Dados.

Quanto à Secretaria de Estado de Saúde de Santa Catarina, tem-se que houve a aplicação de penalidade por parte da Autoridade Nacional de Proteção de Dados, posto que a conduta grave da sancionada no sentido desta não ter relatado o incidente de segurança aos titulares dos dados pessoais, cerca de 300 mil pessoas, demonstrou a falta de clareza e inadequação no modo de agir do órgão público, ainda o órgão não apresentou o Relatório de Impacto de Proteção de Dados Pessoais (RIPD), ao final, a Autoridade Nacional de Proteção de Dados implementou quatro sanções de advertência, sendo uma para cada infração, bem como determinou que fossem mantidos por 90 dias avisos acerca do incidente de segurança, ainda ficou consignado que a secretaria deveria informar o incidente diretamente aos titulares de dados pessoais envolvidos, os quais, podem buscar eventual reparação (Brasil, 2023).

No ano de 2024 a Autoridade Nacional de Proteção de Dados já penalizou órgãos públicos em razão da violação às disposições legais sobre o tratamento de dados pessoais, ou seja, desrespeito à Lei Geral de Proteção de Dados. Puniu-se o Instituto Nacional do Seguro Social pela não comunicação de incidente de segurança aos titulares de dados, sendo a conduta agravada pelo não atendimento às determinações da Autoridade Nacional de Proteção de Dados, o incidente de segurança ocorreu pela exposição de informações como CPF, dados bancários e data de nascimento, ou seja, dados passíveis para serem usados em fraudes e até mesmo para utilização da identidade dos segurados (Brasil, 2024).

Ora, quanto ao incidente supracitado, verifica-se que há um crescente número de fraudes envolvidos idosos aposentados, a título de exemplo, os quais tiveram fragilizados seus dados pessoais a ponto de criminosos terem acesso à dados pessoais que estavam sob a tutela do Estado, a lesão é coletiva e acarreta danos de grande lastro.

Na mesma senda, foi condenada a Secretaria de Educação do Distrito Federal por violar uma série de dispositivos da Lei Geral de Proteção de Dados e do Regulamento de Fiscalização da Autoridade Nacional de Proteção de Dados, concluiu-se que a Secretaria não manteve registro de operações dos dados pessoais, deixou de elabora o Relatório de Impacto à Proteção de Dados Pessoais, mesmo após solicitado pela autoridade, não se utilizou de sistemas que atendam os requisitos mínimos de segurança e deixou de comunicar titulares de dados

pessoais acerca de incidente de segurança que representasse risco ou dano relevante (Brasil, 2024).

Os processos apresentados demonstram que há ainda um longo caminho ao Estado para que em todas as esferas dos entes da federação, quais sejam, municípios, estados, distrito federal e união, possam de fato ter implementado a Lei Geral de Proteção de Dados, bem como seja de fato implementada uma cultura de proteção aos dados pessoais, devendo existir uma verdadeira linha de comunicação entre o titular dos dados pessoais e o Estado, o que demanda, notoriamente, a nomeação de um encarregado de dados. Enfim, o subtópico apresentou processos sancionatórios em face da Administração Pública por desrespeito a princípios basilares da norma protetiva, razão pela qual, entende-se que as "dores" atinentes à Lei Geral de Proteção de Dados no âmbito do Poder Público foram apresentadas, cabendo, a partir de então, apontar possíveis soluções e até mesmo casos de sucesso em que o Poder Público promoveu a implementação real da norma supracitada.

4.3 APONTAMENTO DE SOLUÇÕES

O escopo do trabalho não é somente criar um alerta e apresentar um cenário caótico e insolucionável, em verdade, apresentou-se uma série de dificuldades, diga-se de passagem, não todas, mas com o fim de chegar ao presente subtópico e demonstrar que há viabilidade em solucionar o problema ou, ao menos, mitigar os danos que vêm sendo causados pelo desrespeito à Lei Geral de Proteção de Dados e, consequentemente, pela afronta ao direito fundamental à proteção dos dados pessoais, inclusive nos meios eletrônicos.

O subtópico tem a função de permear manuais e cartilhas editadas pelos tribunais e outros órgãos públicos com a finalidade, inclusive didática, de orientar, ou seja, guiar o Poder Público na regulamentação e implementação da Lei Geral de Proteção de Dados, em especial, citar-se-á caso específico em que a Câmara Municipal de Apucarana contratou programa de *compliance* para se adequar da maneira devida.

A primeira análise quanto à possíveis soluções para a implementação perpassa pelo regime de informação da Universidade Federal do Rio Grande do Sul (UFRGS), a universidade mencionada promoveu, por meio do seu Comitê de Segurança da Informação (CSI), a edição de uma resolução, a qual tem por número 1 de 09 de novembro de 2021 que criou uma política de proteção de dados pessoais na Universidade Federal do Rio Grande do Sul, nominada como PPDPU, a resolução é dividida em quatorze capítulos, sendo o primeiro de disposições gerais,

com a repetição do que já prevê a Lei Geral de Proteção de Dados, no capítulo segundo é apresentado um rol de princípios, também idênticos ao que a legislação geral prevê, enquanto no capítulo terceiro, apresentam-se os objetivos, entre os quais o de garantir o nível de privacidade e proteção aos dados pessoais determinados por legislação, de modo que são definidas medidas técnicas e administrativas à proteção de dados e privacidade, observadas desde a concepção do processo de trabalho ou serviço até a sua execução, os objetivos são cogentes aos agentes públicos vinculados à Universidade Federal do Rio Grande do Sul, é isto que preceitua o artigo 4º[25], da Resolução citada (Universidade Federal do Rio Grande do Sul, 2021, p. 3).

O capítulo quarto e quinto tratam sobre as finalidades de tratamento dos dados pessoais e sobre o tratamento em si, enquanto o capítulo sexto aborda o exercício de direitos do titular dos dados, nos capítulos seguintes são abordadas as formas de coletas de dados para pesquisas, transferência de dados para o exterior, retenção de dados pessoais e sua duração, os relatórios de impacto à proteção de dados pessoais, a privacidade desde a concepção, ou seja, durante todo o ciclo de vida de softwares, serviços, processos ou produtos, primando pela proatividade e o caráter preventivo, ainda, é abordada a forma de fiscalização e a função do encarregado pelo tratamento dos dados pessoais, há capítulo específico para o tratamento de incidentes, bem como se encerra com a menção de possível responsabilização (Universidade Federal do Rio Grande do Sul, 2021, p. 4-11).

Ora, mas qual a motivação de apresentar uma análise completa da resolução citada num subtópico destinado à apresentação de soluções? Explica-se.

No subtópico anterior e no decorrer da dissertação foram apresentadas dores, ou seja, dificuldades enfrentadas na implementação da Lei Geral de Proteção de Dados, bem como hipóteses de investigação e até de condenação de órgãos públicos em razão do desrespeito com a normativa geral. Ora, entre as dificuldades estavam a ausência de nomeação do Encarregado

[25] *In casu:* Art. 4º O objetivo da PPDPU é definir as principais normas, princípios, objetivos e diretrizes em relação à proteção de dados que são aplicáveis à Universidade, para garantir o nível de privacidade e proteção aos dados pessoais determinados por legislação.
§ 1º A PPDPU atende ao determinado na Política de Segurança da Informação da UFRGS e o determinado pela legislação e define as medidas técnicas e administrativas à proteção de dados e privacidade, que deverão ser observadas desde a fase de concepção do processo de trabalho ou serviço até a sua execução e seguidas pelos agentes públicos vinculados à UFRGS e operadores.
§ 2º As medidas técnicas e administrativas devem ser aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e considerar a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos em legislação

de Dados Pessoais, a resolução trazida à lustre aborda inclusive a função do encarregado, atuando, literalmente como canal de comunicação com os titulares e a Autoridade Nacional de Proteção de Dados e o controlador.

Em página própria, a Universidade Federal do Rio Grande do Sul disponibiliza informações sobre o tratamento de dados pessoais, nos quais informa quais são os dados pessoais e os dados pessoais sensíveis tratados internamente, informa, ainda, quais os tratamentos realizados pelo controlador, qual a base legal em que se enquadra as hipóteses de tratamento e indica o encarregado pelo tratamento de dados pessoais, no mais, ainda cria espaço próprio para que sejam realizados pedidos de acesso a informações e endereçamento de manifestações sobre o tratamento de dados pessoais (Universidade Federal do Rio Grande do Sul, 2023).

É realmente salutar verificar que entre tantas situações, há indicação expressa acerca do encarregado, endereço de e-mail para comunicação, apresentação didática acerca dos modos de tratamento, em que importa o tratamento, quais as finalidades, bases legais nas quais estão enquadradas as hipóteses de tratamento, tudo isto demonstra que é possível a implementação da norma.

Retomando o pensamento anterior, acerca das dificuldades apresentadas no decorrer do trabalho, além da ausência da nomeação da figura do Encarregado de Dados Pessoais, verificou-se a ausência de notificação acerca de incidentes de segurança que envolvam os dados pessoais dos titulares. A Universidade Federal do Rio Grande do Sul demonstrando verdadeira noção técnica do assunto, prevê em capítulo próprio de seu regulamento a necessidade de notificação ao titular dos dados pessoais nas hipóteses em que há risco ou dano relevante aos titulares dos dados pessoais, é o que prevê a Resolução citada anteriormente, conforme o artigo, 22 e parágrafos[26], os quais estabelecem até mesmo o prazo para notificação do titular dos dados (Universidade Federal do Rio Grande do Sul, 2021, p. 10).

---

[26] *In casu:* Art. 22. A perda, roubo, furto ou extravio de dispositivo eletrônico ou material impresso da UFRGS contendo dados pessoais, deve ser notificada ao Time de Resposta a Incidentes de Segurança da UFRGS (TRI) pelo e-mail tri@ufrgs.br, bem como a notificação de evento de violação de acesso aos dados pessoais.
§ 1º O TRI analisará as informações do evento, caso as informações sejam relativas ao caput, um incidente será criado e encaminhado ao Gestor de Segurança da Informação da UFRGS e ao ETDP.
§ 2º Caso o incidente tenha ocasionado risco ou dano relevante aos titulares, o respectivo incidente deverá ser notificado aos titulares dos dados pessoais e à ANPD, no prazo de 2 (dois) dias úteis a partir da ciência do fato.
§ 3º A comunicação dos incidentes do caput à ANPD deve ser realizada pela UFRGS, por intermédio do ETDP, após decisão do Reitor, e deve ser realizada conforme regulamentado na legislação aplicável.
§ 4º As decisões relativas aos incidentes avaliados, serão registradas e armazenadas pelo ETDP, conjuntamente as seguintes informações:
I - a descrição dos incidentes ou eventos;

Deste modo, verifica-se que, do primeiro caso de sucesso apontado como solução para as dificuldades anteriormente apresentadas, a regulamentação local versando sobre o tratamento de dados, com a nomeação da figura do Encarregado de Dados Pessoais, a previsão do modo de agir quando da ocorrência de eventual incidente sobre a segurança dos dados pessoais, a previsão de relatório de impacto à proteção de dados pessoais, é um dos caminhos viáveis e aceitáveis para a adequação da Administração Pública ao regramento da Lei Geral de Proteção de Dados. Ressalta-se a importância da regulamentação local, posto que é neste momento em que são analisadas as hipóteses, nuances e dificuldades locais, bem como quais os pontos a serem mais bem abordados ou tratados, de modo que com os dados locais é possível promover uma regulamentação adequada à necessidade local, sem prejuízo algum de seguir a norma geral.

Outro apontamento de solução passa pelo Conselho Nacional de Justiça, órgão do Poder Judiciário, o qual editou a Recomendação número 73, de 20 de agosto de 2020, na qual traz recomendações aos órgãos do Poder Judiciário brasileiro para a adequação às disposições contidas na Lei Geral de Proteção de Dados. A norma acima já foi citada neste trabalho no subtópico 2.1, de modo que desnecessário colacionar o texto normativo novamente, não obstante, a recomendação é de suma importância por apresentar qual o modo de agir que o Poder Público deve tomar, em especial com a regulamentação e edição de normas de fácil entendimento para que o titular dos dados pessoais possa ter acesso, real e não ficto, acerca dos seus direitos e possa, concomitantemente, saber os canais de comunicação e formas de buscar garantir que seus direitos sejam respeitados (Conselho Nacional de Justiça, 2020).

Após a recomendação acima mencionada, o Conselho Nacional de Justiça editou a Resolução de número 363 de 12 de janeiro de 2021, na qual estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados, visando facilitar o processo de implementação no âmbito do sistema judicial, a norma é apontada como uma solução para as problemáticas indicadas por apresentar a necessidade do Poder Público, no caso, do Poder Judiciário, criar comitê gestor de proteção de dados pessoais em cada tribunal, visando entender as nuances locais, como já dito anteriormente, e, após a análise das demandas locais, promover o estabelecimento de sítio eletrônico com as informações necessárias e acessíveis para que os titulares de dados possam entender o meio pelo quela seus dados serão coletados e tratados,

---

II - as informações, processos e sistemas envolvidos;
III - as medidas técnicas e de segurança utilizadas para a proteção das informações;
IV - os riscos relacionados ao incidente;
V - os motivos da demora, em caso de comunicação fora do prazo; e
VI - as medidas que foram ou que serão adotadas para reverter, para mitigar os danos e para evitar reincidências.

bem como tenha ciência de quem é o encarregado de dados, informe qual a base legal para o tratamento dos dados que estão em sua detenção, bem como implemente medidas de segurança, técnicas e administrativas, aptas a salvaguardar os dados pessoais de acessos indesejados e não autorizados, bem como evitar situações acidentais, ilícitas e qualquer tratamento inadequado (Conselho Nacional de Justiça, 2021).

Interessa mencionar que o artigo 2º[27], da Resolução 363/2021, do Conselho Nacional de Justiça, recomenda que o processo de implementação da Lei Geral de Proteção de Dados contemple, minimamente, uma série de ações, quais sejam, mapeamento de todas as atividades de tratamento de dados pessoais, realização de avaliação acerca das vulnerabilidades da instituição em relação ao que é necessário para se adequar à Lei Geral de Proteção de Dados e, ainda, a elaboração de um plano de ação com a previsão das atividades para a implementação completa de Lei Geral de Proteção de Dados (Conselho Nacional de Justiça, 2021).

As resoluções citadas acima demonstram que a solução viável para a solução da problemática acerca da implementação da Lei Geral de Proteção de Dados é a da regulamentação, cuidado com o cumprimento normativo com a nomeação do encarregado de dados, disponibilização no sítio eletrônico do órgão dos contatos do encarregado de dados, da finalidade da coleta, da base legal para que os dados pessoais sejam coletados e tratados, menciona-se da necessidade ou possibilidade de anonimização dos dados – vide artigo 5º, incisos III e XI[28], da Lei Geral de Proteção de Dados - quando necessário à segurança e à salvaguarda dos direitos do titular dos dados pessoais.

Dentre as soluções apresentadas, verifica-se que a capacitação, não só dos agentes públicos, mas também dos titulares dos dados pessoais é o caminho para que seja possível que os primeiros saibam qual o modo de agir perante os dados pessoais e os titulares saibam como fiscalizar e entenda quais são os direitos atinentes à proteção dos seus dados pessoais, inclusive no meio digital. Neste sentido, tem-se cartilha sobre a aplicação da Lei Geral de Proteção de

---

[27] *In casu:* Art. 2º Para o cumprimento do disposto nesta Resolução, recomenda-se que o processo de implementação da LGPD contemple, ao menos, as seguintes ações:
I – realização do mapeamento de todas as atividades de tratamento de dados pessoais por meio de questionário, conforme modelo a ser elaborado pelo CNJ;
II – realização da avaliação das vulnerabilidades (gap assessment) para a análise das lacunas da instituição em relação à proteção de dados pessoais; e
III – elaboração de plano de ação (Roadmap), com a previsão de todas as atividades constantes nesta Resolução.

[28] Art. 5º Para os fins desta Lei, considera-se
III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento
XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Dados Pessoais no Superior Tribunal de Justiça, a qual de maneira didática aborda o que é a Lei Geral de Proteção de Dados, mencionando que os objetivos são variados, mas entre eles o de proteger direitos fundamentais como a liberdade e privacidade, bem como que servidores e colaboradores conheçam do tema e possa se engajar e colaborar nas rotinas de trabalho do Tribunal à Lei Geral de Proteção de Dados, deixando de maneira clara os direitos e deveres dentro do novo contexto apresentado (Superior Tribunal de Justiça, 2023, p. 2).

Como mencionado, de forma didática, apresenta-se os principais conceitos da Lei Geral de Proteção de Dados, os princípios contidos na norma, a atribuição de responsabilidades ao controlador, do encarregado, pelo operador, ainda, é apresentada as sanções previstas na Lei Geral de Proteção de Dados (Superior Tribunal de Justiça, 2023, p. 3-11).

O Superior Tribunal de Justiça faz relevante interface entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados, ou seja, faz uma ligação entre leis que parecem ser opostas, mas, em verdade, interagem. Ora, inicialmente, tem-se que a Lei de Acesso à Informação se pauta em princípios como a transparência e acesso dos dados públicos, de modo que não só os titulares, mas também outros que tenham interesse possam acessar os dados atinentes à atividade pública, e Lei de Acesso tem o escopo de promover a transparência a coisa pública, facilitando a responsabilização, a fiscalização e a prestação de contas. Já a Lei Geral de Proteção de Dados prevê que o Estado precisa promover com zelo a proteção aos dados pessoais que detém ou publica, nesta em cumprimento ao dever de transparência, em especial, o cuidado deve existir quando se relacionar a dados pessoais e dados pessoais sensíveis. Nas publicações deve ser avaliada e justificada à luz da principiologia prevista na Lei Geral de Proteção de Dados as publicações que contenham dados pessoais sensíveis ou não dos titulares. A cartilha (Superior Tribunal de Justiça, 2023, p. 12) traz uma pacificação para tema que inquieta as alas que defendem a superioridade de uma legislação sobre a outra, quando prevê que:

> "Portanto, tecnicamente, não existe superioridade de uma lei sobre a outra. A LAI garante o acesso à informação, enquanto a LGPD normatiza e resguarda a privacidade dos dados pessoais. Ambas as leis protegem a informação pessoal do acesso de terceiros não autorizados. No entanto, apenas a LGPD realiza a análise de impacto da privacidade documentada, estabelece políticas de privacidade, proteção e respostas a incidentes".

A cartilha do Tribunal se encerra com a indicação de boas práticas de trabalho alinhadas à Lei Geral de Proteção de Dados, em que instrui os servidores e colaboradores qual

o modo de agir a ser tomado no dia a dia, em atividades corriqueiras, como evitar coletar dados pessoais desnecessários ou em excesso na atuação diária quando no interesse do Estado, ainda, indica-se que não se deixe documentos que contenham dados pessoais expostos em impressora, mesas ou até deixar o monitor do computador aberto, se não estiver em uso, orientando a utilização de meios seguros ao tratar de dados pessoais, ressaltando que a finalidade deve ser legítima e relacionada ao interesse público (Superior Tribunal de Justiça, 2023, p. 13).

Foi apresentado pelo Superior Tribunal de Justiça um verdadeiro manual de boas práticas, demonstrando direitos, deveres, conceitos, ponderações, análise entre a Lei Geral de Proteção de Dados e a Lei de Acesso à Informação, de modo a demonstrar aos servidores, colaboradores e pesquisadores que há necessidade da criação de uma nova cultura, ou seja, uma cultura de coexistência entre a legislação existente com a proteção dos dados pessoais, de modo que ocorra uma integração na função da Administração Pública que deve, ao mesmo tempo, proteger os dados pessoais e cumprir com seu dever de transparência, bem como o Estado continuará exercendo sua finalidade precípua, seja na tributação, seja na assistência social ou em qualquer outra de suas áreas de atuação estatal, não obstante, suas funções passam a considerar e ter o dever de cumprir a Lei Geral de Proteção de Dados. Assim, acredita-se que a capacitação, o zelo com a apresentação aos servidores e colaboradores dos deveres criados pela lei, a criação de meios preventivos e proativos, são capazes de fazer com que o Poder Público rompa o estado de inércia e passe cumprir a norma protetiva e resguardar direitos fundamentais dos titulares de dados, sem prejuízo do cumprimento às suas funções precípuas.

Foi demonstrado no decorrer do trabalho que o Brasil iniciou de maneira tardia, em relação à Europa, a regulamentação acerca da proteção de dados, de modo que na atualidade, como já dito, compete a capacitação e o *spread* da nova cultura, uma que dê acesso fácil, rápido e didático aos titulares dos dados pessoais para que estes entendam a relevância de seus dados e a importância de que alguns de seus dados não sejam tratados de forma indevida ou até coletados. Na seara da informação, é basilar a indicação do encarregado que tem a função de ser o elo entre o titular, a Autoridade Nacional de Proteção de Dados e o controlador. Cita-se, aqui, novamente, o Superior Tribunal de Justiça que, em seu sítio eletrônico, disponibiliza as informações básicas ao titular como a figura do encarregado de Dados, as resoluções editas pelo tribunal, a política de privacidade, a cartilha outrora citada, dentro outras informações (Superior Tribunal de Justiça, 2024).

Por fim, quanto às soluções, apresenta-se o que a Câmara Municipal de Apucarana promoveu para se adequar à Lei Geral de Proteção de Dados. O Poder Legislativo municipal

citado promoveu a contratação de empresa, via inexigibilidade, em conformidade com a antiga Lei de Licitações, a saber, Lei 8.666/93, a finalidade da contatação consistiu na "adequação jurídica da Câmara Municipal de Apucarana em todos os seus setores e a capacitação dos servidores a Lei Geral de Proteção de Dados". O contrato celebrado entre as partes demonstra que foi criado um sistema de governança, por meio de *compliance*, visando instituir e fazer com que a Casa Legislativa citada saísse da inércia para o cumprimento da Lei Geral de Proteção de Dados. Verifica-se que foi realizada capacitação setorial dentro do Poder Público, ensinando a promoção de gestão de riscos, bem como estabelecendo quais as bases legais para o tratamento de dados (Câmara Municipal de Apucarana, 2024).

Cita-se que a Casa Legislativa acima citada promoveu a publicação em seu sítio eletrônico da Política de Segurança da Informação (Câmara Municipal de Apucarana, 2023), bem como a Política de Privacidade (Câmara Municipal de Apucarana, 2023). Nos documentos apresentados verificou-se a indicação do encarregado, quais as finalidades de tratamento do ente público, quais as bases legais de tratamento, rol de direitos do titular de dados pessoais, a responsabilidade em informar incidentes, enfim, dentro das nuances locais o ente, por meio de capacitação contratada, estabeleceu os meios para o cumprimento da Lei Geral de Proteção de Dados.

Ademais, a Casa Legislativa municipal em estudo promoveu a edição de duas resoluções, a saber, a Resolução número 9 e 10, do ano de 2023, as quais dispuseram sobre a regulamentação da Lei Geral de Proteção de Dados, sendo a primeira com relação à publicização dos documentos de origem externa (Câmara Municipal de Apucarana, 2023) e a segunda com relação ao Portal da Transparência (Câmara Municipal de Apucarana, 2023). Notoriamente, o ente, após a capacitação, foi capaz de editar regramento local para atender as necessidades que existem em sua própria atuação, o que vai além do regramento geral trazido pela Lei Geral de Proteção de Dados.

Entende-se que foi apresentado ao leitor, sem exaurir as possibilidades, várias soluções para que ocorra a efetiva implementação da Lei Geral de Proteção de Dados pelo Poder Público. O Estado deve sair da inércia para uma atuação proativa, buscando garantir o cumprimento à norma, bem como atuando de modo a resguardar os direitos dos titulares.

CONCLUSÕES

O texto dessa dissertação se iniciou com a proposta de apresentar ao leitor uma abordagem acerca das novas tecnologias, sob uma ótica jurídica, o afunilamento teórico ocorreu para a aplicação da Lei Geral de Proteção de Dados ao Poder Público.

Demonstrou-se no decorrer do estudo que o Estado é um coletor de dados por excelência, fazendo a coleta de dados desde os primórdios. Além de coletar, o Poder Público promove o tratamento dos dados. A coleta e tratamento massificados fazem com que a Administração Pública não esteja alheia ao dever de ter diligência em suas atividades estatais, em especial por se tratar de dados de outrem que estão em sua posse.

A abordagem acerca da sociedade da informação demonstrou que desde os idos dos anos de 1960 o rumo da sociedade passou a demonstrar mais valor nos dados pessoais, de modo que as novas tecnologias promoveram real revolução no modo de pensar e agir em sociedade. Os fatos históricos e mudanças sociais foram capazes de impactar o direito, em razão disto os estudiosos passaram a tratar sobre temas relevantes, como capitalismo de vigilância, a Europa passou a se preocupar e estudar o tema saindo na vanguarda sobre o tema.

A edição do Regulamento Geral de Proteção de Dados da Europa serviu como um marco e um paradigma para que as demais nações passassem a se preocupar e regulamentar a proteção aos dados pessoais em seus territórios. Demonstrou-se que os dados pessoais passaram ao *status* de novo petróleo do século XXI, ante sua vasta valorização no meio econômico, podendo-se afirmar que a sociedade da informação ensejou uma economia que gira em torno da informação.

Foi demonstrado que os dados se diferenciam do conhecimento e da informação, tendo sido realizada diferenciação entre os três institutos e apresentando que os dados pessoais passaram a ter relevância não só econômica, mas também jurídica, de modo que se discutiu o contexto no qual se insere a proteção aos dados pessoais, demonstrando-se a evolução histórica acerca dos dados pessoais, os quais não passaram a existir na sociedade da informação, mas que nesta passaram a um nível tão relevante que ensejaram uma proteção por parte do Estado e uma proteção em face do próprio Poder Público que de forma massificada coleta e trata dados.

Após ter apresentado a evolução histórica dos dados pessoais e sua aplicação na atualidade, valendo-se da Lei Geral de Proteção de Dados para a conceituação de dados pessoais, dados pessoais sensíveis e outros conceitos necessários, apresentou-se ao leitor a existência da Emenda Constitucional 115 de 2022 que elevou a proteção aos dados pessoais, inclusive nos meios digitais, ao patamar de direito fundamental, previsto no artigo 5º, inciso LXXIX, da Constituição Federal.

Demonstrou-se que ainda antes da emenda citada o Supremo Tribunal Federal já havia reconhecido a proteção aos dados pessoais enquanto direito fundamental componente do bloco de constitucionalidade, utilizando-se da autodeterminação informacional, ou seja, antes da previsão constitucional entendia-se como materialmente constitucional a proteção aos dados pessoais, após a emenda passou-se a ser além de material, também formalmente constitucional.

Encerrada a análise acerca da evolução histórica e das nuances gerais acerca dos dados pessoais, a dissertação se ocupou de demonstrar que a Lei Geral de Proteção de Dados é aplicável ao Estado. Ressalta-se que não há sequer divergência quanto à aplicação da norma ao Poder Público, não obstante, há um regramento próprio previsto na Lei Geral de Proteção de Dados que se aplica ao Poder Público.

O Estado coleta e trata dados por excelência, é provavelmente aquele que detém a maior gama de dados pessoais, em razão da sua função estatal e administrativa que enseja a necessidade de ter acesso aos dados pessoais, inclusive sensíveis, dos cidadãos. O fator apresentado fez com que fosse necessária uma abordagem específica acerca da aplicação da Lei Geral de Proteção de Dados ao Estado.

Envidou-se esforços para abordar a responsabilidade do Estado, iniciou-se abordando a responsabilidade civil do Estado quando da geração de danos em razão da violação à Lei Geral de Proteção de Dados, entende-se que a responsabilidade do Estado é objetiva, seja pela revisão bibliográfica promovida, ou ainda pelo que prevê o artigo 37, parágrafo sexto, da Constituição Federal. Menciona-se que ficou clara a possibilidade de exercício do direito de regresso pelo Estado face os seus servidores ou aqueles que atuem em nome da Administração Pública que derem causa, ainda que culposamente, pelo dano ao titular dos dados pessoais.

Verificou-se que há possibilidade, inclusive, de incidência da Lei de Improbidade Administrativa quando o agente público ou político dolosamente desrespeita diretrizes estabelecidas na Lei Geral de Proteção de Dados, tendo o tema sido enfrentado pelo Supremo Tribunal Federal.

Enfrentou-se a responsabilidade administrativa do Estado pela violação à Lei Geral de Proteção de Dados, de modo que cabe à Autoridade Nacional de Proteção de Dados a tarefa de, enquanto autarquia especial que atua como verdadeira agência reguladora, promover a fiscalização das pessoas jurídicas de direito público ou privado, além do poder de polícia para sancionar aqueles que descumprirem as diretrizes da Lei Geral de Proteção de Dados.

Em seguida, a dissertação se ocupou em apresentar as dores, ou seja, as dificuldades apresentadas pela inadequação do Poder Público com a Lei Geral de Proteção de Dados. Entre

as maiores dificuldades apresentadas por meio de processos administrativos e judiciais, verificou-se que o Estado toma seu tempo nalguns momentos para a criação de normas que afrontam o direito fundamental à proteção de dados, criando, a título de exemplo, banco de dados de DNA sem o consentimento dos envolvidos, noutros momentos o Poder Público deixa de comunicar os titulares de dados acerca de incidentes de segurança que são potencialmente causadores de danos, de modo o Poder Público desrespeita frontalmente e reiteradamente as diretrizes estabelecidas na Lei Geral de Proteção de dados e, consequentemente, afronta e viola o direito fundamental à proteção de dados, inclusive nos meios digitais.

Do estudo promovido é possível afirmar que nalguns momentos há uma suposta antinomia entre princípios como a transparência e a proteção aos dados pessoais, mas, em verdade, deve ocorrer uma coexistência pacífica entre os princípios, por meio da integração interpretativa.

Após apresentar uma série de dificuldades que se encontram no dia a dia do Poder Público, buscou-se demonstrar que há uma luz capaz de guiar o Estado na implementação da Lei Geral de Proteção de Dados. Expuseram-se hipóteses em que a Administração Pública, por meio de seus entes e órgãos, promoveu a regulamentação, por meio de diferentes metodologias.

Entende-se que a capacitação é condição de existência para que seja possível implementar a Lei Geral de Proteção de Dados, posto que os servidores, colaboradores e prestadores que atuam no Poder Público ou fazendo as vezes do Estado devem entender a nova cultura implementada com o advento da norma protetiva.

A nomeação do Encarregado de Dados para que possa cumprir sua função normativa de atuar enquanto canal de comunicação entre a Autoridade Nacional de Proteção de Dados, o controlador e o titular dos dados pessoais é um dos passos iniciais para que seja possível estabelecer um ponto de encontro, de modo que seja possível iniciar a implementação da Lei Geral de Proteção de Dados.

Além disto, promover um sistema de governança, com gestão de riscos, estabelecendo políticas de privacidade e de tratamento que sejam claras e didáticas aos titulares de dados e aos operadores é necessário para que se saia da inação para a ação. A contratação de cursos de capacitação é relevante para que continuamente os servidores possam entender a cultura de proteção aos dados pessoais e sejam capazes de atuar dentro de suas funções. A edição de manuais de boas práticas quanto à legislação fazendo correlação com as atividades diárias é salutar para que se torne palpável aos envolvidos a aplicação da lei.

Por fim, verificou-se que as novas tecnologias não são um problema, em verdade, otimiza-se e se fornece muitas utilidades no dia a dia, não obstante, a atuação dos coletores de dados, inclusive o Estado, atuando como verdadeiros predadores de dados pessoais demanda a regulamentação e proteção aos dados pessoais, de modo que as utilidades e benefícios não se tornem posteriores mazelas aos titulares de dados que, em muitos momentos, não entendem a real importância no compartilhamento de dados e como os dados podem ser utilizados posteriormente, bem como nas hipóteses de incidentes de segurança com os dados pessoais.

O direito se preocupa com as relações sociais e, numa sociedade da informação, é cabível que o direito se preocupe com os dados pessoais e a sua proteção, criando direitos e deveres para o bom convívio social, ainda que nos ambientes virtuais. A Lei Geral de Proteção de Dados, dentro deste contexto, é norma relevante e aplicável no dia a dia, inclusive no mundo virtual, de modo que, quanto ao Estado, compete a necessária regulamentação e implementação dentro do contexto de suas rotinas de coleta e tratamento.

Ao Estado compete a atuação enquanto verdadeira locomotiva, demonstrando que a implementação e regulamentação da Lei Geral de Proteção de Dados é possível, servindo de exemplo para que isso se irradie na seara privada. Existem soluções para os problemas apresentados, não obstante, as soluções não são possíveis se o Poder Público permanecer em estado de inércia. Deste modo, a proatividade e a ação da Administração Pública são necessárias para que os problemas sejam solucionados e haja paz e tranquilidade social, em especial dos titulares dos dados pessoais, nos ambientes físicos e virtuais, pois assim, é possível a contínua evolução social e tecnológica.

REFERÊNCIAS BIBLIOGRÁFICAS:

ALMEIDA, Juliana Evangelista de; LUGATI, Lys Nunes. Da Evolução das Legislações sobre Proteção de Dados: A Necessidade de Reavaliação do Papel do Consentimento como Garantidos da Autodeterminação Informativa. REVISTA DE DIREITO | VIÇOSA | ISSN 2527-0389 | V.12 N.02 2020 DOI: doi.org/10.32361/2020120210597.

ALMEIDA, Rodrigo Magalhães.; OLIVEIRA, Erika Cristina Rodrigues Nardoni. O Direito à Privacidade na Era Digital. Revista Jurídica da FA7, v. 18, n. 1, p. 55-70, 28 jun. 2021. Disponível em: https://periodicos.uni7.edu.br/index.php/revistajuridica/article/view/1173/857. Acesso em: 07 out. 2023.

APUCARANA. Câmara Municipal de Apucarana. Política de Privacidade. 2023. Disponível em: https://www.apucarana.pr.leg.br/politica-de-privacidade. Acesso em: 10 fev. 2024.

APUCARANA. Câmara Municipal de Apucarana. Política de Segurança da Informação. 2023. Disponível em: https://www.apucarana.pr.leg.br/politica-de-seguranca-da-informacao. Acesso em: 10 fev. 2024.

APUCARANA. Câmara Municipal de Apucarana. Resolução n. 09/2023. Disponível em: https://sapl.apucarana.pr.leg.br/media/sapl/public/normajuridica/2023/9380/resolucao_no_09_23.pdf. Acesso em: 10 fev. 2024.

APUCARANA. Câmara Municipal de Apucarana. Resolução n. 10/2023. Disponível em: https://sapl.apucarana.pr.leg.br/media/sapl/public/normajuridica/2023/9381/resolucao_no_10_23.pdf. Acesso em: 10 fev. 2024.

APUCARANA. Câmara Municipal de Apucarana. Portal da Transparência. 2023. Contratação empresa para Capacitação na Lei Geral de Proteção de Dados. Disponível em: https://camaraapucarana.atende.net/transparencia/item/licitacoes-gerais. Acesso em: 10 fev. 2024.

ARENDT, Hannah. A Condição Humana. Trad. Roberto Raposo. 11ª ed. Rio de Janeiro: Forense Universitária, 2013.

ASSMANN, Jhonata. O Direito à Autodeterminação Informativa no Direito Germânico e Brasileiro. Orientador: Airton Lisle Cerqueira L. Seelaender. 2014. 65 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2014. Disponível em: https://repositorio.ufsc.br/handle/123456789/117169. Acesso em: 11 out. 2023.

BARBOSA, Eduardo Henrique de Oliveira; OLIVEIRA, Izadora Gabriele dos Santos; SILVA, Fabrício José dos Santos. Big Data: O Petróleo da Indústria 4.0 – Uma Análise Conjunta com a Lei 13.709/18. P. 89. Políticas, Internet e sociedade (recurso eletrônico) / orgs. Fabrício Bertini Pasquot Polido, Lucas Costa dos Anjos e Luiza Couto Chaves Brandão. Belo Horizonte: IRIS, 2019. Disponível em: https://d1wqtxts1xzle7.cloudfront.net/60040262/Livro_politicas_internet_e_sociedade20190717-91903-2b8sm6-libre.pdf?1563389102=&response-content-disposition=inline%3B+filename%3DO_LIVRE_DESENVOLVIMENTO_DA_IDENTIDADE_PE.pdf&Expires=1696693482&Signature=TwJ5jNff0oKxJeZFrSRJJxoOewIEiEcS6S00G7MIs4Fvt0CTRgRxxBJdroybWLgjIkZVh7SNlkypLplyt0jyEHAHlj~VWMjWjmJ6mR7Xc63640BYrKvMFQxhwBYbw~H1CHDO80xAbX0WUpVj2fAWb-sDJ7XduMoXYbo79PiOfEdYQOrzjN2O6Fa8CmTL2UJb1XnAY9XLRDg9tikRWDuiThGXfu31qWicvGtYZQI-ZcnX-64yy5pFrLVKI5yM7h7OMq8hkxhXGsNt2aaXcVEJkjwDZpFfEL7fE4RUBP1lFxPDFSaxQu8dEigq0-rfE0pJfKXmaqhXXPH0yf69w80Y~w__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=88. Acesso em: 07 out. 2023.

BAUMAN, Zygmunt. Cegueira Moral. Google Books, 2014. Disponível em: https://www.google.com.br/books/edition/Cegueira_moral/IXPTDwAAQBAJ?hl=ptBR&gbpv=1&printsec=frontcover. Acesso em 10 out. 2023.

BAUMAN, Zygmunt. Vida para Consumo: transformação das pessoas em mercadorias. Rio de Janeiro: Jorge Zahar Editor, 2008.

BOTELHO, Marcos César; CAMARGO, Elimei Paleari do Amaral. A Aplicação da Lei Geral de Proteção de Dados na Saúde. Revista de Direito Sanitário, da Universidade de São Paulo – USP, 21, e0021. Pág. 4. Disponível em: https://doi.org/10.11606/issn.2316-9044.rdisan.2021.168023. Acesso em: 06 out. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. Brasília. DF. ANPD Divulga Lista de Processos Sancionatórios. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-lista-de-processos-sancionatorios. Acesso em: 7 fev. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. Brasília. DF. Autoridade Nacional de Proteção de Dados sanciona mais um órgão público. Disponível em: https://agenciagov.ebc.com.br/noticias/202310/anpd-sanciona-mais-um-orgao-publico. Acesso em: 7 fev. 2024.

BRASIL. Autoridade Nacional de Proteção de Dados. Brasília. DF. ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-inss-e-secretaria-de-educacao-do-df-por-violacoes-a-lgpd#:~:text=ANPD%20sancionou%20mais%20dois%20%C3%B3rg%C3%A3os,Distrito%20Federal%20(SEEDF). Acesso em: 7 fev. 2024.

BRASIL. Casa Civil. Brasília. DF. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa. Acesso em: 25 jan. 2024.

BRASIL. Recomendação nº 73, de 20 de agosto de 2020. Conselho Nacional de Justiça. Disponível em: https://atos.cnj.jus.br/files/compilado135819202102266038fe7b3b752.pdf. Acesso em: 18 set. 2023.

BRASIL. Recomendação nº 363, de 12 de janeiro de 2021. Conselho Nacional de Justiça. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3668. Acesso em: 9 fev. 2024

BRASIL. Constituição Federal. Brasília. DF. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 jan. 2024.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.html. Acesso em: 12 out. 2023.

BRASIL. Lei nº 8.078/1990. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 out. 2023.

BRASIL. Lei nº 13.709/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 out. 2023.

BRASIL. Superior Tribunal de Justiça. Aplicação da Lei Geral de Proteção de Dados Pessoais no STJ. Jun. 2023. 16 p. Disponível em: https://www.stj.jus.br/sites/portalp/WebPub/NovoPortal/midias/cartilha-lgpd-novo.pdf. Acesso em: 10 fev. 2024.

BRASIL. Superior Tribunal de Justiça. LGPD: Um marco na Regulamentação sobre dados pessoais no Brasil. 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Leis-e-normas/lei-geral-de-protecao-de-dados-pessoais-lgpd. Acesso em: 10 fev. 2024.

BRASIL. Superior Tribunal de Justiça. Recurso Especial n. 22.337/RS. Relator: Ministro Ruy Rosado de Aguiar. Diário da Justiça, Brasília, DF, 20 mar. 1995. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=199200114466&dt_pu. Acesso em: 15 out. 2023.

BRASIL. Supremo Tribunal Federal. ADI 5.545 Rio de Janeiro. Relatoria Min. Luiz Fux. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=768636835. Acesso em: 7 de fev. 2024.

BRASIL. Supremo Tribunal Federal. ADI 6393 MC-REF/DF. Relatoria Min. Rosa Weber. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950595&ext=.pdf. Pág. 51-52. Acesso em: 12 out. 2023.

BRASIL. Supremo Tribunal Federal. ADPF 695/DF. Relatoria Min. Gilmar Mendes. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978671&ext=.pdf. Acesso em: 6 fev. 2024.

BRASIL. Supremo Tribunal Federal. Medida Cautelar na Ação Direta de Inconstitucionalidade - ADI 6.561/TO. Relatoria Min. Edson Fachin. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754239594. Acesso em: 7 fev. 2024.

BRASIL. Tribunal Superior Eleitoral. Processo Administrativo N. 0600231-37.2021.6.00.0000 – São Paulo. Relatoria Min. Edson Fachin. Disponível em: https://jurisprudencia.tse.jus.br/#/jurisprudencia/pesquisa?expressaoLivre=lgpd&tipoDecisao=Ac%25C3%25B3rd%25C3%25A3o%252CResolu%25C3%25A7%25C3%25A3o%252CDecis%25C3%25A3o%2520sem%2520resolu%25C3%25A7%25C3%25A3o&params=s. Acesso em: 7 fev. 2024.

BONETTI, Diego Vinicius Soares; ZAINAGHI, Maria Cristina. Liberdade de Expressão e Direitos da Personalidade na Sociedade da Informação. Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI Coordenadores: José Querino Tavares Neto; Márcia Haydée Porto de Carvalho – Florianópolis: CONPEDI, 2022. Disponível em: http://site.conpedi.org.br/publicacoes/129by0v5/l1jmsj6g/YGD6teFyS2RLbgC4.pdf>. Acesso em: 21 jan. 2024.

BURKART, Daniele Vicenzi Villares. Proteção de Dados e o Estudo da LGPD. Universidade Estadual Paulista. Programa de pós-graduação mestrado em mídia e tecnologia. Bauru – São Paulo. 2021.

CALDEIRA, Cristina. A proteção de Dados Pessoais e o Impacto nas Transferências Internacionais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). *Direito & Internet IV*: sistema de proteção de dados pessoais. São Paulo: Quartier Latin, 2019.

CASTELLS, Manuel. A Sociedade em rede. Tradução de Roneide Venancio Majer. 20. ed. rev. amp. São Paulo: Paz e Terra, 2019.

CASTELLS, Manuel. A Sociedade em Rede: do Conhecimento à Política. *In*.: CARDOSO, Gustavo; CASTELLS, Manuel (org.) *A sociedade em rede: do conhecimento à acção política.* Lisboa: Imprensa Nacional – Casa da Moeda, 2005.

CASTELLS, Manuel. *Comunicación y poder.* Madrid: Alianza Editorial. 2009. Disponível em: http://parlamidia.com/images/PDF/castells-comunicacao.pdf. Acesso em: 06 out. 2023.

CARLOTO, Selma. A Lei Geral de Proteção de Dados: enfoque nas relações de trabalho. 2. ed. São Paulo: LTr, 2021.

CAVALIERI FILHO, Sérgio. Programa de Responsabilidade Civil. São Paulo: Grupo GEN, 2020.

CAZELATTO, Caio Eduardo Costa; MORENO, Michel Henrique Timóteo. Da Sociedade da Informação Frente ao Acesso à Internet como um Direito Fundamental de Personalidade. Direito, governança e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI /UnB/UCB/IDP/ UDF; Coordenadores: Cinthia O. A. Freitas, José Renato Gaziero Cella – Florianópolis: CONPEDI, 2016. Disponível em: http://site.conpedi.org.br/publicacoes/y0ii48h0/k778x2oo/zgqAj9dBszMD3c0L.pdf. Acesso em: 21 de jan. 2024.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os Direitos da Personalidade frente à Sociedade da Vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. Revista Brasileira de Direito Civil em Perspectiva, Belém, v. 5, n. 2, Jul/Dez 2019. Disponível em: https://www.indexlaw.org/index.php/direitocivil/article/view/5778>. Acesso em: 24 jan. 2024.

CORRÊA, Adriana Espíndola. Lei de Proteção de Dados e a identificação nacional: há antinomias. Revista Consultor Jurídico. Disponível em: https://www.conjur.com.br/2019-fev-18/direito-civil-atual-lei-protecao-dados-identificacao-nacional-antinomias#sdfootnote2sym. Acesso em: 12 out. 2023.

CUNDA, Daniela Zago Gonçalves da; RAMOS, Letícia Ayres; LOUREIRO, Roberto Debacco; SIMIONI, Denizar. A Proteção e a Transparência de Dados sob a perspectiva dos Controles Externo e Social e a Governança Digital. Lei Geral de Proteção de Dados e o Poder Público / Organizadores: Daniela Copetti Cravo; Daniela Zago Gonçalves da Cunda; Rafael

Ramos. Porto Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021. 223 p. Disponível em: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 30 jan. 2024.

CUNHA, Maria Alexandra. *Smart cities* [recurso eletrônico]: transformação digital de cidades / Maria Alexandra Cunha, Erico; Przeybilovicz, Javiera Fernanda Medina Macaya e Fernando Burgos. – São Paulo: Programa Gestão Pública e Cidadania - PGPC, 2016. 161 p. ISBN: 978-85-87426-29-1. Pg 33. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/18386. Acesso em: 07 de out. de 2023.

DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. Revista da Faculdade de Direito, Universidade de São Paulo, *[S. l.]*, v. 97, p. 239-253, 2002. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/67544. Acesso em: 9 fev. 2024.

DANTAS, Marcos. A Lógica do Capital Informação: monopólio e monopolização dos fragmentos num mundo de comunicações globais. Rio de Janeiro: Contraponto, 1996.

DIAS, José de Aguiar. Da Responsabilidade Civil. 11. ed. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. A proteção de Dados Pessoais como um Direito Fundamental. Revista Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul/dez. 2011. Disponível em: https://dialnet.unirioja.es/descarga/articulo/4555153.pdf. Acesso em: 11 out. 2023.

DONEDA, Danilo. A LGPD como Elemento Estruturante do Modelo Brasileiro de Proteção de Dados. P. 243. A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) a caminho da efetividade: contribuições para a implementação da LGPD / Obra coletiva: Ricardo Villas Bôas Cueva. Danilo Doneda. Laura Schertel Mendes. Coordenadores. São Paulo: Thomson Reuters Brasil, 2020.

DRUMOND, Thomaz Carneiro. LGPD e a Administração Pública: alguns desafios. 2022, disponível em: https://www.conferencebr.com/conteudo/arquivo/1-1661557785.pdf. Acesso em: 30 jan. 2024.

DUTTON, William H. *Putting Things to Work: social and policy challenges for the internet of things.* info. V. 16. N. 3. P. 1-21. 2014.

FARINIUK, Tharsila Maynardes Dallabona; SIMÃO, Marcela de Moraes Batista; FIRMINO, Rodrigo José; MENDONÇA, Juliana Helen Krebs Moreira Braga de. O Estereótipo Smart City no Brasil e sua Relação com o Meio Urbano. Perspectivas em Gestão & Conhecimento, [S. l.], v. 10, n. 2, p. 159–179, 2020. Disponível em: https://periodicos.ufpb.br/index.php/pgc/article/view/47105. Acesso em: 26 jan. 2024.

FERNANDES, Cassiane de Melo; NETO, Chade Rezek. A Sociedade da Informação como Ambiente de Transmissão de Dados. A Direito, governança e novas tecnologias organização CONPEDI/UdelaR/Unisinos/URI/UFSM /Univali/UPF/FURG; Coordenadores: Marcelo

Eduardo Bauza Reilly, Rosane Leal Da Silva – Florianópolis: CONPEDI, 2016. Disponível em: http://site.conpedi.org.br/publicacoes/9105o6b2/v4u5j0t6/7Pqc1td8SULcFAg8.pdf>. Acesso em: 22 jan. 2024.

FLÔRES, Mariana Rocha de; SILVA, Rosane Leal da. Desafios e perspectivas da proteção de dados pessoais sensíveis em poder da administração pública: entre o dever público de informar e o direito do cidadão de ser tutelado. Revista de Direito, [S. l.], v. 12, n. 02, p. 01–34, 2020. DOI: 10.32361/2020120210327. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10327. Acesso em: 11 out. 2023.

FRITZ, Karina Nunes. Jurisprudência comentada dos tribunais alemães. Indaiatuba: Editora Foco, 2021, p. 114.

GOMES, Daniel Machado; ROCHA, Luiz Augusto Castello Branco de Lacerca Marca da. Direito à Informação e Exclusividade do Interesse Privado: Um Diálogo entre STEFANO RODOTÁ e HANNAH ARENDT. Direito e novas tecnologias [Recurso eletrônico on-line] organização CONPEDI/UFS; Coordenadores: José Renato Gaziero Cella, Aires Jose Rover, Valéria Ribas Do Nascimento, Florianópolis: CONPEDI, 2015. Disponível em: http://site.conpedi.org.br/publicacoes/c178h0tg/vwk790q7/n77Dck6S55E3qPW8.pdf. Acesso em: 23 jan. 2024.

GROPP, Maria Eduarda; MOTTA, Jefferson Holliver. A Mineração de Dados e os Direitos de Personalidade dos Consumidores: Análise da Privacidade na Era Digital. Em Governança e Direitos Fundamentais: Revisitando o debate entre o Público e o Privado. Fábio da Silva Veiga e Ruben Miranda Gonçalves (Diretores) – Solon Henriques de Sá e Benevides e Francisco de Sales Gaudêncio Coordenadores. Instituto Ibero-americano de Estudos Jurídicos. 2020. 417 páginas. ISBN: 978-84-09-17702-8.

GUIMARÃES, Gabriel Stagni. A importância da lei geral de proteção de dados pessoais em face do avanço tecnológico da sociedade: a proteção dos dados pessoais como direito fundamental. 2021. Dissertação (Mestrado em Direito) - Programa de Estudos Pós-Graduados em Direito da Pontifícia Universidade Católica de São Paulo, São Paulo, 2021. Disponível em: https://repositorio.pucsp.br/bitstream/handle/24864/1/Gabriel%20Stagni%20Guimar%c3%a3es.pdf. Acesso em: 10 out. 2023.

HINTZBERGEN, Jule [et al.]. Fundamentos de segurança da informação: com base na ISO 27001 e na ISO 27002; tradução Alan de Sá – Ed. Brasport, Rio de Janeiro, 2018.

HIROKI, Stella Marina Yurí. Parâmetros para identificação dos estágios de desenvolvimento das cidades inteligentes no Brasil. Pontifícia Universidade Católica de São Paulo – Programa de Pós-Graduação em Tecnologias da Inteligência e Design Digital. Doutorado em Tecnologias da Inteligência e Design Digital. São Paulo, 2019.

JUNIOR, Irineu Francisco Barreto; VIGLIAR, José Marcelo Menezes. As funções da jurisprudência na sociedade da informação. Ver. Fac. Direito UFMG, Belo Horizonte, n. 73, pp. 3910417, jul/dez. 2018.

JUNIOR, Paulo Hamilton Siqueira. Direito Informacional: Direito da Sociedade da Informação. Revista dos Tribunais, v. 859, p. 743-759, maio 2007.

LANNES, Yuri Nathan da Costa; FACHIN, Jéssica Amanda; VERONESE, Alexandre. Políticas Públicas de Acesso à Universalização da Internet no Brasil e Cidadania Digital. Revista de Direito Brasileira – RDB. V. 32. N. 12. 2022. Disponível em: https://indexlaw.org/index.php/rdb/article/view/8982/6475. Acesso em: 9 fev. 2024.

LEMOS, André; LEVY, Pierre. O Futuro da Internet: em direção a uma ciberdemocracia. São Paulo: Paulus, 2014.

LIMA, Cintia Rosa Pereira. BIONI, Bruno Ricardo. A proteção dos dados pessoais na fase de coleta: apontamentos sobre a adjetivação do consentimento implementada pelo artigo 7, incisos VIII e IX do Marco Civil da Internet a partir da human computes interaction e da privacy by default. In: LUCCA, Newton de; SIMAO FILHO, Adalberto; LIMA, Cintia Pereira de (Coord.). Direito & Internet III: Marco Civil da Internet: Lei n. 12.965/2014. São Paulo: Ed. Quartier Latin, 2015.

LISBOA, Roberto Senise. Direito na Sociedade da Informação. Revista dos Tribunais, 2006. Disponível em:
https://www.researchgate.net/profile/Roberto-Lisboa/publication/341219107_DIREITO_NA_SOCIEDADE_DA_INFORMACAO/links/5eb45124a6fdcc1f1dc80db8/DIREITO-NA-SOCIEDADE-DA-INFORMACAO.pdf.
Acesso em: 6 out. 2023.

LISBOA, Roberto Senise. Proteção do Consumidor na Sociedade da Informação. Revista de Direito Privado da UEL – Universidade Estadual de Londrina. V. 2. nº 1, jan/abril, 2009.

LONGUI, João Victor Rozatti. Responsabilidade civil e redes sociais: retirada de conteúdo, perfis falsos, discurso de ódio e fake News. Idaiatuba, SP: Editora Foco, 2020.

NETO, Amadeu Alakra. Lei Geral de Proteção de Dados Pessoais (LGPD): O Instituto do Consentimento nas Relações Trabalhistas. Universidade do Valo do Itajaí – UNIVALI. Curso de Mestrado em Ciência Jurídica – CMCJ. Dissertação. Itajái – Santa Catarina, 2023. Disponível em: https://www.univali.br/Lists/TrabalhosMestrado/Attachments/3150/2023%20-%20DISSERTA%C3%87%C3%83O%20-%20AMADEU%20ALAKRA%20NETO.pdf>.
Acesso em: 10 out. 2023.

NIKE, Política de Privacidade Nike FUELBAND. Disponível em Disponível em: https://securenikeplus.nike.com/plus/support#answers/detail/a_id/21061/kw/privacy%20policy. Acesso em: 23 jan. 2024

MACHADO, Joana de Moraes Souza. A tutela da privacidade na sociedade da informação: a proteção dos dados pessoais no Brasil. Porto Alegre, RS: Editora Fi, 2018. *E-book*. Disponível em: https://www.editorafi.org/494joana. Acesso em: 11 out. 2023.

MAGALHÃES, Filipa Matias; PEREIRA, Maria Leitão. Regulamento Geral de Proteção de Dados: Manual Prático. 3. Ed. Porto: Vida Econômica, 2020.

MARINELI, Marcelo Romão. Privacidade e Redes Sociais Virtuais: Sob a égide da Lei 12.965/2014 – Marco Civil da Internet e da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais. 2ª Ed. Revista, atualizada e Ampliada. São Paulo: Thomson Reuters Brasil, 2019.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. *Compliance* Digital e responsabilidade civil na Lei Geral de Proteção de Dados. *In*: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.) Responsabilidade Civil e novas tecnologias. Idaiatuba: Foco: 2020, p. 293.

MENDES, Laura Schertel; BIONI, Bruno Ricardo. O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência. Revista dos Tribunais. 2019. Revista de Direito do Consumidor, São Paulo, v. 28, n. 124, p. 157-180, jul./ago. 2019. Disponível em: https://bd.tjdft.jus.br/jspui/handle/tjdft/45866. Acesso em: 28 jan. 2024.

OLIVEIRA, Nairobi Spiecker de; GOMES, Moises Alexandre; LOPES, Ronaldo; NOBRE, Jeferson C. Segurança da informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). Revista Eletrônica de Iniciação Científica em Computação, v. 17 n. 4, 2019. Disponível em: https://seer.ufrgs.br/reic/article/view/88790>. Acesso em: 13 out. 2023.

ORTIGOSA, Adrián Palma. Contexto normativo de la protección de datos personales. In: CABRERA, Sara Lorenzo Cabrera; ORTIGOSA, Adrían Palma. Protección de dados, responsabilidad activa y técnicas de garantia. Saragoça: Reus, 2018. Adaptado a la nueva Ley Orgánica 3/2018, de 5 deciembre, de Protección de Datos Personales y garantia de los derechos digitales.

PAESANI, Lilian Minardi (coord.). O Direito na Sociedade da Informação. São Paulo: Atlas, 2007.

PARANÁ. Cartilha Encarregado pelo Tratamento de Dados Pessoais. Controladoria Geral do Estado do Paraná. Disponível em:
https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_encarregado_de_dados.pdf>. Acesso em: 30 jan. 2024.

PARANÁ. Manual de Implementação da LGPD. Controladoria Geral do Estado do Paraná. Disponível em:
https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-06/manual_implementacao_lgpd.pdf>. Acesso em: 26 jan. 2024.

PARENTONI, Leonardo. O Direito ao Esquecimento [Right to Oblivion]. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota (coord.). *Direito & Internet III*: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015, p. 540.

PARISER, Eli. *How the New Personalized web is changing what we read and how we thing. New York:* Penguin Books, 2012.

PELCERMAN, Sérgio Eliezer. Reflexos da Lei Geral de Proteção de Dados nas relações de trabalho: desligamento de empregados por justo motivo em decorrência de incidentes de segurança de dados sob o prisma da LGPD. 2023. 112 f. Dissertação (Mestrado em Direito, Desenvolvimento e Justiça) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2022. Disponível em: https://repositorio.idp.edu.br/bitstream/123456789/4237/1/DISSERTA%c3%87%c3%83O_SERGIO%20ELIEZER_MESTRADO%20EM%20DIREITO.pdf. Acesso em: 10 out. 2023.

PEZZI, Ana Paula Jacobus. A Necessidade de Proteção de Dados Pessoais nos Arquivos de Consumo: em busca da concretização do direito à privacidade. Orientadora: Têmis Limberger. 2007. 216 f. Dissertação (Mestrado). Curso de Direito, Universidade do Vale do Rio dos Sinos – UNISINOS, 2007. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf. Acesso em: 12 out. 2023.

POLIDO, Fabrício B. Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves; MACHADO, Diego Carvalho; OLIVEIRA, Davi Teófilo Nunes. GDPR e suas repercussões no direito brasileiro: primeiras impressões de análise comparativa. Instituto de Referência em Internet e Sociedade (IRIS), [*s.l*], 7. Nov. 2018. Disponível em: https://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-Primeiras-impress%C3%B5es-de-an%C3%A1lise-comparativa-PT.pdf. Acesso em: 20 de janeiro de 2024.

PORTAL G1. Veja os Principais pontos da Operação que investiga Espionagem Ilegal da ABIN. Brasília. Disponível em: https://g1.globo.com/politica/noticia/2024/01/26/veja-os-principais-pontos-da-operacao-que-investiga-espionagem-ilegal-da-abin.ghtml#0. Acesso em: 26 jan. 2024.

QUEIROZ, Renata Capriolli Zocatelli. A proteção de dados pessoais: a LGPD e a Disciplina Jurírica do Encarregado de Proteção de Dados Pessoais. Universidade de São Paulo (USP) – Faculdade de Direito. São Paulo – SP. 2021. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2131/tde-23082022-085834/publico/11550929DIO.pdf. Acesso em: 10 out. 2023

RIZZON, Fernanda, BERTELLI, Janine, MATTE, Juliana, GRAEBIN, Rosani Elisabete, MACKE, Janaina. *Smart City*: um conceito em construção. Revista metropolitana de sustentabilidade – RMS, São Paulo. V. 07. Número 3. Set/Dez.2017. P. 127-128

RODOTÁ, Stefano. A vida na sociedade de vigilância – a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODOTÁ, Stefano. Il mondo nella rete quali diritti, quali i vinculi. Roma Laterza, 2014.

ROGERS, David L. Transformação Digital: repensando o seu negócio para a era digital. São Paulo: Autêntica Business, 2019.

ROSENVALD, Nelson. As funções da Responsabilidade Civil: A Reparação e a Pena Civil. São Paulo: Saraiva, 2017.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro. O direito à proteção de dados pessoais na sociedade da informação. Revista Direito, Estado e Sociedade Programa de Pós-Graduação em Direito da PUC-Rio, Rio de Janeiro, n. 36, p. 191-192. 12 set. 2010. DOI: http://dx.doi.org/10.17808/des.36.212. Disponível em: https://revistades.jur.puc-rio.br/index.php/revistades/article/view/212/191. Acesso em: 11 out. 2023.

SCHREIBER, Anderson. Responsabilidade Civil na Lei Geral de Proteção de Dados. *In:* DONEDA, Danilo *et. al.* Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

SCHWAB, Klaus. A quarta Revolução Industrial. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SEMIDÃO, Rafael Aparecido Moron. Dados, Informação e Conhecimento enquanto Elementos de Compreensão do Universo Conceitual da Ciência da Informação: contribuições teóricas. Pág. 70. 2014. Disponível em: https://www.marilia.unesp.br/Home/Pos-Graduacao/CienciadaInformacao/Dissertacoes/semidao_ram_me_mar.pdf. Acesso em: 06 out. 2023.

SILVEIRA, Sérgio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais | Privacy and the market of personal data. Liinc em Revista, *[S. l.]*, v. 12, n. 2, 2016. DOI: 10.18617/liinc.v12i2.902. Disponível em: https://revista.ibict.br/liinc/article/view/3719. Acesso em: 7 out. 2023.

SRNICEK, Nick. Platform Capitalism. 1 edition. Cambridge, ukMalden, ma: Polity, 2016.

TABORDA, Luiz Edemir. Lei geral de proteção de dados pessoais (LGPD) e violência financeira contra a pessoa idosa no mercado de consumo. 2022. Dissertação (Mestrado em Ciências Socais Aplicadas) - Universidade Estadual de Ponta Grossa. Ponta Grossa. 2022. Disponível em: https://tede2.uepg.br/jspui/bitstream/prefix/3681/1/Luiz%20Edemir%20Taborda.pdf. Acesso em:10 out. 2023

TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. In: ONODERA, Marcus Vinicius Kiyoshi; FILIPPO, Thiago Baldani Gomes de (Coords.). Brasil e EUA: Temas de Direito Comparado. São Paulo: Escola Paulista da Magistratura, 2017. Disponível em: https://api.tjsp.jus.br/Handlers/Handler/FileFetch.ashx?codigo=94288. Acesso em: 11 out. 2023

TEIXEIRA, Tarcísio; PASSI, Renata Capriolli Zocatelli Queiroz. Privacidade na Internet: a formação de bancos de dados e a transformação das pessoas em mercadorias. Revista dos Tribunais, São Paulo, n. 990, Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/120071. Acesso em: 18 jan. 2024

TEPEDINO, Gustavo. Liberdades, Tecnologia e Teoria da Interpretação. Revista Forense, v. 419, jan/jun. 2014.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio da Cruz. Fundamentos do Direito Civil: Responsabilidade Civil. São Paulo. Grupo GEN, 2020, v. 4.

THE WORLD'S most valuable resource is no longer oil, but data. *The Economist*, 6 maio 2017. Disponível em: www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em: 07 de out. 2023.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. Resolução CSI Nº 1, de 09 de novembro de 2021. Comitê de Segurança da Informação. Política de Proteção de Dados Pessoais da UFRGS. 2021. Disponível em: https://www.ufrgs.br/proprivacidade/docs/UFRGS-PoliticaProtecaoDadosPessoais.pdf Acesso em 9 fev. 2024.

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL. Tratamento de Dados Pessoais. 2023. Disponível em: http://www.ufrgs.br/ufrgs/acessoainformacao/tratamento-de-dados-pessoais. Acesso em: 9 fev. 2024.

VAINZOF, Rony. Conceito, perfil, papéis e responsabilidades do encarregado. In: BLUM, Renato Ópice, VAINZOF, Rony, MORAES, Henrique Fabretti (coord.). Data Protection Officer: teoria e prática de acordo com a LGPD e o GDPR. 1. Ed. São Paulo: Thomson Reuters Brasil, 2020. E-book.

VALOR, Globo. Maior vazamento de dados da história expõe brasileiros. 2024, disponível em: https://valor.globo.com/empresas/noticia/2024/01/25/maior-vazamento-de-dados-da-historia-atinge-brasileiros-veja-como-checar.ghtml. Acesso em: 24 jan. 2024.

WALDMAN, Ricardo Libel; MATHEUS, Rosemeire Solidade da Silva. O Brasil na Sociedade da Informação: Remissão História e seu Panorama Atual com Destaque na COVID-19. Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI Coordenadores: Aires Jose Rover; Danielle Jacon Ayres Pinto; Fabiano Hartmann Peixoto; José Renato Gaziero Cella – Florianópolis: CONPEDI, 2020. Disponível em: http://site.conpedi.org.br/publicacoes/nl6180k3/m4tcws6j/5x5ZCS66DidNWk19.pdf>. Acesso em: 21 jan. 2024.

WARREN, Samuel; BRANDEIS, Louis. The Right of Privacy. 2013. Civilistica.com, a.2 n.3, 2013. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/127/97. Acesso em: 23 jan. 2024.

WERTHEIN, Jorge. A Sociedade da Informação e seus Desafios. 2000. Scielo, BRASIL. Disponível em: https://doi.org/10.1590/S0100-19652000000200009. Acesso em: 21 de jan. 2024.

ZIEGLER, Joici Antonia; PIAIA, Thami Covatti. A proteção e a regulação dos dados pessoais dos internautas brasileiros. Direito e novas tecnologias organização CONPEDI/UFS; Coordenadores: José Renato Gaziero Cella, Aires Jose Rover, Valéria Ribas Do Nascimento – Florianópolis: CONPEDI, 2015. Disponível em: http://site.conpedi.org.br/publicacoes/c178h0tg/vwk790q7/n77Dck6S55E3qPW8.pdf>. Acesso em: 22 jan. 2024.

ZUBOFF, Shoshana. *Big Other:* Capitalismo de Vigilância e Perspectivas para uma Civilização de Informação. Tecnopolíticas da vigilância: perspectivas da margem. Organização Fernanda Bruno, Bruno Cardoso, Marta Kanashiro, Luciana Guilhon e Lucas Melgaço. São Paulo: Boitempo, 2018.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: the flight for a human future at the new frontier of power*. Nova Iorque: Profile Books, 2019.