



UNIALFA – CENTRO UNIVERSITÁRIO ALVES FARIA
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU*
MESTRADO ACADÊMICO EM DIREITO CONSTITUCIONAL ECONÔMICO

SELMA LINHARES GOES

**POR UMA POLÍTICA PÚBLICA PREVENTIVA DE PROTEÇÃO
DOS DADOS PESSOAIS DIGITAIS DO CIDADÃO,
NA DIMENSÃO ECONÔMICA CONSTITUCIONAL DO CONSUMIDOR -
*Análise de vazamentos de dados no caso do ChatGPT.***

GOIÂNIA
AGOSTO DE 2023



UNIALFA – CENTRO UNIVERSITÁRIO ALVES FARIA
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU*
MESTRADO ACADÊMICO EM DIREITO CONSTITUCIONAL ECONÔMICO

SELMA LINHARES GOES

POR UMA POLÍTICA PÚBLICA PREVENTIVA DE PROTEÇÃO
DOS DADOS PESSOAIS DIGITAIS DO CIDADÃO,
NA DIMENSÃO ECONÔMICA CONSTITUCIONAL DO CONSUMIDOR -
Análise de vazamentos de dados no caso do ChatGPT.

Dissertação apresentada na qualificação do Curso de Pós-graduação em Direito Constitucional Econômico do Centro Universitário Alves Faria – UNIALFA, como requisito parcial para a obtenção do título de Mestre em Direito Constitucional Econômico.

Orientador: Professor Dr. Túlio Tayano Afonso.

GOIÂNIA
AGOSTO DE 2023



UNIALFA - CENTRO UNIVERSITÁRIO ALVES FARIA
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU
MESTRADO ACADÊMICO EM DIREITO CONSTITUCIONAL ECONÔMICO

POR UMA POLÍTICA PÚBLICA PREVENTIVA DE PROTEÇÃO
DOS DADOS PESSOAIS DIGITAIS DO CIDADÃO,
NA DIMENSÃO ECONÔMICA CONSTITUCIONAL DO CONSUMIDOR -
Análise de vazamentos de dados no caso do ChatGPT.

Dissertação apresentada na qualificação do Curso de Mestrado em Direito Constitucional Econômico do Centro Universitário Alves Faria– UNIALFA, visando à obtenção do título de Mestre em Direito Constitucional Econômico.

Goiânia, 30 de agosto de 2023.

Componentes da banca examinadora:

Professor Doutor Túlio Tayano Afonso
Centro Universitário Alves Faria

Professora Doutora (Examinadora – Membro externo)

Professor Doutor (Examinador)
Centro Universitário Alves Faria

AGRADECIMENTOS

Agradeço ao meu orientador, Professor Doutor Túlio Tayano Afonso por me apontar os melhores caminhos para o conhecimento, por me ajudar a superar os obstáculos e redefinir rumos para tornar possível a finalização deste trabalho.

A Professora Doutora ____ e ao Professor Doutor ____ componentes da banca examinadora.

Aproveito a oportunidade para agradecer aos Professores da UNIALFA pelas lições e pelo aprendizado contínuo, de maneira especial à coordenadora Professora Doutora Marina Faraco.

Não poderia deixar de agradecer aos meus Filhos, Aline Mendes Linhares Goes e Souza, Amanda Mendes Linhares Goes e Souza e José Goes Pery de Souza Neto, aos meus Pais, José Goes Nogueira *in memoriam*, e Maria dos Anjos Linhares Goes, por estarem sempre ao meu lado independente do tamanho do obstáculo a ser vencido.

Por fim, agradeço a Deus por permitir essa oportunidade de aprendizado jamais idealizada e, por me fazer uma pessoa melhor pela convivência e boas amizades que jamais abrirei mão.

Pela Internet

Criar meu web site
Fazer minha home-page
Com quantos gigabytes
Se faz uma jangada
Um barco que veleje

Criar meu web site
Fazer minha home-page
Com quantos gigabytes
Se faz uma jangada
Um barco que veleje

Que veleje nesse informar
Que aproveite a vazante da infomaré
Que leve um oriki do meu velho orixá
Ao porto de um disquete de um micro em Taipé

Um barco que veleje nesse infomar
Que aproveite a vazante da infomaré
Que leve meu e-mail até Calcutá
Depois de um hot-link
Num site de Helsinque
Para abastecer

Eu quero entrar na rede
Promover um debate
Juntar via Internet
Um grupo de tietes de Connecticut

Eu quero entrar na rede
Promover um debate
Juntar via Internet
Um grupo de tietes de Connecticut

De Connecticut de acessar
O chefe da Mac Milícia de Milão
Um hacker mafioso acaba de soltar
Um vírus para atacar os programas no Japão

Eu quero entrar na rede para contactar
Os lares do Nepal, os bares do Gabão
Que o chefe da polícia carioca avisa pelo celular
Que lá na praça Onze
Tem um videopôquer para se jogar

(Gilberto Gil, 1996)

RESUMO

Este trabalho é um estudo sistemático sobre a necessidade de criação de uma política pública de regras preventivas para a defesa da privacidade dos dados digitais das pessoas, na dimensão dos consumidores, bem como para a garantia do princípio da ordem econômica da defesa do consumidor. O Caso do robô ChatGPT é utilizado neste estudo como um exemplo de vazamento de dados de grande repercussão, que demonstra a vulnerabilidade a que os consumidores estão submetidos. Portanto, os dados dos consumidores estão em risco e devem ser protegidos em atenção ao direito fundamental humano à privacidade. O objetivo deste estudo é mostrar a necessidade de criação desta política de regras preventivas para a proteção dos mencionados dados, a fim de que o princípio constitucional da ordem econômica da defesa do consumidor seja garantido. Nossa hipótese é a de que urge a criação de uma política de regras preventivas para a proteção dos dados pessoais digitais dos consumidores, diminuindo os riscos de tratamento inadequado e ilegal, das informações pessoais dos cidadãos, tais como os vazamentos de dados, mitigando as consequências negativas que as inteligências artificiais, neste aspecto, podem causar a sociedade como um todo e em específico às relações de consumo. A metodologia utilizada para essas reflexões é a da pesquisa qualitativa, por meio de pesquisas bibliográficas e documentais e uso da técnica da documentação indireta.

Palavras-chave: Proteção dos dados pessoais. Garantia do princípio constitucional econômico da defesa do Consumidor. Privacidade. Vazamento de dados. ChatGPT. Política pública preventiva.

ABSTRACT

This work is a systematic study on the need to create a public policy of preventive rules to defend the privacy of people's digital data, in the dimension of consumers, as well as to guarantee the principle of economic order of consumer protection. The case of the ChatGPT robot is used in this study as an example of a high-profile data leak, which demonstrates the vulnerability to which consumers are subjected. Therefore, consumer data is at risk and must be protected in keeping with the fundamental human right to privacy. The objective of this study is to show the need to create this policy of preventive rules for the protection of the aforementioned data, so that the constitutional principle of the economic order of consumer protection is guaranteed. Our hypothesis is that it is urgent to create a policy of preventive rules for the protection of consumers' digital personal data, reducing the risks of inadequate and illegal treatment of citizens' personal information, such as data leaks, mitigating the consequences negative effects that artificial intelligences, in this regard, can cause society as a whole and specifically consumer relations. The methodology used for these reflections is that of qualitative research, through bibliographical and documentary research and use of the technique of indirect documentation.

Keywords: Protection of personal data. Guarantee of the economic constitutional principle of consumer protection. Privacy. Data leak. ChatGPT. Preventive public policy

LISTA DE ABREVIATURAS E SIGLAS

ANPD – Autoridade Nacional de Proteção de Dados

DPDC – Departamento de Proteção e Defesa do Consumidor

LGPD – Lei Geral de Proteção de Dados

CDC - Código de Defesa do Consumidor

SENACON - Secretaria Nacional do Consumidor

PROCON - Programa de Proteção e Defesa do Consumidor

SNDC - Sistema Nacional de Defesa do Consumidor

LISTA DE FIGURAS

Figura 1 – Detalhamento da estrutura interna da ANPD	67
Figura 2 - Amostra do CHATGPT	76
Figura 3 - Contas Invadidas em cada país	79

SUMÁRIO

INTRODUÇÃO.....	12
 CAPÍTULO 1 A ERA DA INFORMAÇÃO.....	17
1.1 OS NOVOS TEMPOS.....	17
1.2 A SOCIEDADE DA INFORMAÇÃO E A REVOLUÇÃO 4.0.....	18
1.2.1 Evolução da Rede Mundial de Computadores.....	21
1.2.2 Data Leak (vazamento de dados)	24
1.3 A PRIVACIDADE EM RISCO.....	28
1.3.1 Os Dados Pessoais como Direito Humano Fundamental.....	29
1.3.2 Tutela da Privacidade.....	34
1.3.2.1 <i>Histórico Legal</i>	35
1.3.2.1 <i>Trajetória do Conceito de Privacidade</i>	38
 CAPÍTULO 2 AS RELAÇÕES DE CONSUMO NA ERA DIGITAL.....	43
2.1 A ORDEM ECONÔMICA BRASILEIRA.....	43
2.1.1 O Princípio da Ordem Econômica da Defesa do Consumidor.....	48
2.1.1.1 <i>Direito do Consumidor</i>	50
2.1.1.1.1 <i>Jurisprudências dos Tribunais de Justiça</i>	53
2.1.2 O Princípio do Direito do Consumidor da boa-fé objetiva.....	57
2.2 BIG DATA	60
2.3 LEI GERAL DE PROTEÇÃO DE DADOS - LGPD.....	62
2.4 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD.....	67
2.5 EM BUSCA DA BOA GOVERNANÇA.....	69
 CAPÍTULO 3 POR UMA POLÍTICA PÚBLICA PREVENTIVA DE DEFESA DOS DADOS PESSOAIS DIGITAIS DO CONSUMIDOR – ANÁLISE DE VAZAMENTOS DE DADOS NO CASO CHATGPT.....	74
3.1 INTELIGÊNCIA ARTIFICIAL.....	74
3.1.1 Origens.....	74

3.1.2 Estrutura.....	76
3.1.3 O Caso do ChatGPT.....	79
3.2 A DEFESA DO CONSUMIDOR E A PROTEÇÃO DOS DADOS PESSOAIS.	83
3.3 A NECESSIDADE DE UMA POLÍTICA REGULADORA DE PROTEÇÃO DE DADOS DOS CONSUMIDORES, NA ESFERA DIGITAL, PARA A GARANTIA DA PRIVACIDADE E DO PRINCÍPIO CONSTITUCIONAL DA ORDEM ECONÔMICA DE DEFESA DO CONSUMIDOR	86
CONSIDERAÇÕES FINAIS	93
REFERÊNCIAS.....	95

INTRODUÇÃO

O tempo, o espaço e a sociedade fazem com que novos modos de vida se definam, fazendo com que adaptações sejam imprescindíveis para a perpetuação e manutenção das espécies. O mundo já não é mais o mesmo: nosso espaço vem mudando de forma rápida, fazendo com que novos tempos surjam e as pessoas precisem se adaptar de uma maneira muito urgente a essas novas mudanças. Como um dos elementos propulsores dessas mudanças na sociedade, encontra-se a economia: é a partir dela que se formam as constituições e relações sócio econômicas cotidianas. A história econômica das sociedades forma o ser social.

Vários são os exemplos de mudanças na sociedade possibilitadas por fatores econômicos. Mundialmente, pode-se citar a luta pela influência econômica-política entre os Estados Unidos e a Rússia, responsável, inclusive, pela atual guerra entre a Rússia e a Ucrânia. No Brasil, pode-se citar o massacre indígena ocorrido recentemente com os *Yanomamis* por parte dos garimpeiros, que invadem suas terras em busca de metais preciosos.

Percebe-se uma importância primordial à economia em nosso mundo. Atualmente, na Era da Sociedade da Informação, que desencadeou uma revolução digital nunca antes vista na história da humanidade, um elemento de valor que se observa, diz respeito aos dados pessoais dos indivíduos. Doneda (2021), Bioni (2022) e Pinheiro (2023) são alguns dos autores que bem lembram esse valor quando explicam que, ao se coletar dados, uma empresa ganha mais assertividade para oferecer seus produtos ao cliente que tem mais possibilidade de adquiri-los. Quando ocorre essa transação, outros dados são gerados para serem utilizados noutras finalidades e assim se estabelece um ciclo infundável de geração de informações e oportunidades.

Não é por acaso que a defesa do consumidor é um princípio constitucional da ordem econômica e social de nosso país. É bom destacar que a proteção ao consumidor já existia, na Idade Média em Portugal, no tocante a distribuição, precificação e prevenção de fraudes ao consumidor, como registra Gonçalves (1995, p. 29 e 30):

As cidades haviam crescido, algumas delas com grande exuberância, durante os últimos tempos medievais ... Em Portugal, Lisboa [...] centro de uma área rica em produtos de todo o gênero e que ela atraía como um imã; o seu excelente porto, o melhor do

País, por onde constantemente entravam e saíam grandes e grossas mercadorias ... Chegadas as mercadorias ao porto e descarregadas na Ribeira, trazidas por terra em carreto animal ou a dorso de homem e levadas ao local de venda, ou ainda produzidas na cidade, impunha-se que todos os lisboetas pudessem ter-lhes acesso a um preço tão baixo quanto possível. Impunha-se igualmente que ninguém fosse vítima de fraude, tanto no respeitante às quantidades adquiridas como à qualidade dos produtos. Isto é, procurava-se que os direitos do consumidor fossem respeitados.

No entanto, os primeiros movimentos consumeristas de que se tem notícia originaram-se nos Estados Unidos da América, no final do séc. XIX (MARQUES; MIRAGEM, BENJAMIM, 2021).

Convém destacar, ainda, que a ordem econômica de um país é o conjunto de normas, positivadas ou não, que moldam as ações dos agentes econômicos, pessoas jurídicas ou físicas que, através de suas práticas, fazem funcionar todo o sistema econômico: famílias, comércio, indústrias, finanças, mercado, Estado e o mundo. Esses agentes econômicos possuem uma importância específica na economia de um país, sendo alguns relevantes para a demanda e outros para a oferta (ULEN; COOTER, 2010).

Neste sentido, percebe-se a abrangência da defesa do consumidor para o crescimento e desenvolvimento de um país. Justifica-se, dessa forma, a escolha pela referida temática neste estudo. É necessária uma efetiva defesa do consumidor, mais especificamente no que diz respeito aos seus dados pessoais, sobretudo na seara digital, estimulando práticas econômicas que visem à sua proteção. Fazem-se necessárias novas políticas públicas que estimulem e ensinem aos consumidores o direito à proteção de seus dados pessoais, haja vista ser este um direito fundamental do ser humano, elencado no artigo 5º da CF/88, inciso LXXXIX, elevado a esta categoria pela Emenda Constitucional n. 115/2022 (SARLET, 2022).

É isso o que se propõe aqui nesta pesquisa: a criação de uma política de regras preventivas, específica para a garantia da segurança dos dados digitais das pessoas com atenção aos dados relativos aos consumidores. O surgimento do robô ChatGPT expôs de maneira inequívoca preocupações ao mundo, na medida em que mostrou a vulnerabilidade dos dados das pessoas, dos consumidores, a partir de sua utilização para, por exemplo, práticas enganosas e injustas, utilizando-se de dados pessoais sem a devida autorização de seus detentores, conforme foi amplamente divulgado pelos meios de comunicação no mundo inteiro. É preciso,

então, que se construa condições prévias de controle, com foco em ações efetivas que reduza os vazamentos de dados pessoais.

Neste sentido, esta dissertação busca analisar a seguinte problemática: em que medida a criação de uma política pública de regras preventivas de proteção dos dados pessoais digitais dos cidadãos, com o foco nos consumidores, se constitui como uma medida eficaz na garantia e preservação do princípio da ordem econômica da defesa do consumidor? Este é, então, o objetivo geral deste trabalho: Defender a criação de uma política pública de regras preventivas para se garantir a privacidade dos dados pessoais dos consumidores, a fim de se fazer cumprir este importante princípio constitucional da ordem econômica nacional que é a defesa do consumidor.

Como objetivos específicos, têm-se: a) caracterizar a era da informação, apresentando a sociedade digital, o surgimento da inteligência artificial e o risco a privacidade das pessoas; b) descrever as relações de consumo na era digital, enfatizando o princípio da ordem econômica da defesa do consumidor; e nesta seara, demonstrar a vulnerabilidade dos dados dos consumidores; c) analisar a necessidade de criação de uma política pública de regras preventivas de manuseio dos dados dos consumidores, com vistas a se garantir a preservação da privacidade desses dados, avaliando-se a LGPD, a importância da ANPD e o caso do robô CHATGPT, no que diz respeito a apropriação dos dados das pessoas, sem a devida autorização, escancarando de maneira inequívoca que o vazamento de dados representa um sério risco a privacidade das informações pessoais dentro do universo digital.

Para tanto, esta dissertação está organizada de acordo com a seguinte estruturação: o primeiro capítulo aborda a era da informação, caracterizando a sociedade digital, o surgimento da inteligência artificial e o risco a privacidade. O segundo capítulo versa sobre as relações de consumo da era digital, explicando a LGPD, a importância da ANPD, e alertando para o descumprimento do princípio da ordem econômica da defesa do consumidor no tocante à vulnerabilidade dos seus dados pessoais digitais.

O terceiro e último capítulo apresenta a necessidade de uma política pública de regras preventivas para se fazer cumprir o princípio constitucional da defesa do consumidor em nosso país. Para isso, é aludido o caso do robô ChatGPT, com a apresentação de vazamento de dados pessoais dos consumidores e a proposição

de algumas medidas que podem ser tomadas para se evitar ao máximo, a infração ao princípio da defesa do consumidor em nosso país. Acredita-se que essa estrutura lógica textual seja suficiente para a elucidação do fenômeno em tela.

As perspectivas teóricas que conduzirão o raciocínio lógico deste trabalho se organizam em categorias temáticas, como direito constitucional econômico, direito do consumidor, direito digital e direito humano fundamental. Em Direito Constitucional Econômico, o estudioso Eros Grau se mostra como principal. Sobre Direito do Consumidor Cláudia Marques, Bruno Miragem e Antônio Herman Benjamim, Direito Digital, utilizam-se Doneda, Bioni e Pinheiro. E sobre direito humano fundamental, nada mais pertinente do que se citar Luís Roberto Barroso e Marcelo Novelino, serão alguns dos nomes bastante presentes nestes escritos.

A caracterização metodológica desta pesquisa é definida da seguinte maneira: utiliza-se uma vertente metodológica qualitativa porque se analisam questões relativas à defesa do consumidor como direito humano fundamental a privacidade, proteção de dados e a autodeterminação informativa em meio ao desenvolvimento socioeconômico. Enfatiza-se uma análise crítica sobre a questão. Quanto ao método de abordagem, utiliza-se o dedutivo porque se parte de questões gerais, como a caracterização da era da informação para se chegar ao caso do robô ChatGPT, abordando-se especificamente a questão dos vazamentos de dados. Faz-se uso do método de procedimento monográfico, uma vez que se realiza uma análise de aspectos específicos do caso do robô ChatGPT.

No que atine ao objetivo da pesquisa, tem-se a configuração de uma pesquisa descritiva-crítica. Há a intenção de se descrever a vulnerabilidade dos dados digitais na sociedade da informação, fazendo-se uma conexão entre o Consumidor, o vazamento de suas informações pessoais, destacando-se aspectos de grande repercussão sobre este tema ligados ao caso do ChatGPT, bem como, a partir desse panorama analisar a necessidade de uma política pública de regras preventivas, para a preservação da privacidade dos consumidores. E quanto ao procedimento técnico, a pesquisa se classifica como sendo bibliográfica e documental: a primeira porque aqui se utilizam obras remissivas e analíticas sobre o assunto em tela, com interpretações já produzidas por outros autores; e documental porque se analisam documentos diversos, como a LGPD. Isto ainda faz com que se afirme que a técnica da documentação aqui priorizada seja a da documentação indireta, pela razão de se analisar o objeto de estudo de maneira distanciada da

pesquisadora, não havendo interação social com ele.

Espera-se, assim, construir um estudo sistematizado e possível de ser utilizado no circuito jurídico-acadêmico das discussões sobre Direito Constitucional Econômico, especialmente no que tange à defesa do consumidor e desenvolvimento socioeconômico. Não se tem aqui a pretensão de esgotar o tema, está-se longe da completude e finalização desses debates, uma vez também que se trata de um assunto mutável, que acompanha as transformações da sociedade. Todavia, sabe-se que se tem aqui um importante objeto de pesquisa para o aperfeiçoamento dos trabalhos que visem a construção de uma justiça social verdadeiramente comprometida com as gerações atuais e futuras.

CAPÍTULO 1. A ERA DA INFORMAÇÃO

As relações sociais são baseadas no consumo.

(Zygmunt Bauman)

Este capítulo apresenta a sociedade da era da informação, descrevendo o avanço da tecnologia no século XXI, o surgimento da inteligência artificial e minuciando sobre o risco a privacidade nos novos tempos.

1.1 OS NOVOS TEMPOS

O mundo do século XXI sofreu muitas transformações ao longo dos anos. As diversas revoluções sociais e a implementação da automação em níveis cada vez mais complexos possibilitaram a substituição da força humana pelas máquinas. Ao longo dos tempos, a primeira grande revolução vivenciada pela sociedade ocorreu entre os séculos XVIII e XIX: foi marcada pela mecanização, produção em larga escala e energia a vapor. A segunda grande mudança ficou conhecida como Era da Eletricidade; a terceira como Era da Automação; e, por sua vez, a mais recente a Era da 4ª Revolução Industrial, ou Indústria 4.0, caracterizada pelos sistemas *cyber*¹ físicos, inteligência artificial, Internet das coisas e automação dos *softwares*. A chamada 4ª revolução industrial, decorre dos avanços tecnológicos de caráter disruptivo, apresenta rápidas transformações ao fluxo das inter-relações, sobretudo no meio virtual, acontece na sociedade globalizada em todos os setores, a todo o momento (BRASILEIRO, 2022)

Atualmente, a economia, o comércio e o mercado de trabalho vêm sofrendo grande influência da Indústria 4.0, pois o mundo ainda está experimentando as mudanças daí advindas e aguardando a transição para a 5ª fase da revolução

¹ Os sistemas ciber físicos (ou CPS, na sigla em inglês para Cyber-Physical Systems) são integrações que envolvem **computação, comunicação e controle** através de redes e processos físicos. Por intermédio desses sistemas, as empresas têm a oportunidade de representar a realidade do mundo físico em ambientes digitais [https://certi.org.br/blog/sistemas-ciber-isicos/#:~:text=Os%20sistemas%20ciber%20f%C3%ADsicos%20\(ou,mundo%20f%C3%ADsico%20em%20ambientes%20digitais](https://certi.org.br/blog/sistemas-ciber-isicos/#:~:text=Os%20sistemas%20ciber%20f%C3%ADsicos%20(ou,mundo%20f%C3%ADsico%20em%20ambientes%20digitais)

industrial. “A indústria 5.0 é o processo de inserção do ser humano junto às tecnologias automatizadas, criando um campo onde ambos se complementam” (NEVES, 2023).

Nesse sentido, o que se pode perceber é que o uso da inteligência artificial, da computação em nuvem, do *Big Data*, da internet das coisas e dos robôs autônomos fez surgir novas formas de trabalho, de consumo, de negócios, de vida. Tudo ainda é muito novo e, inicialmente, a percepção é a de que estão desprotegidas, sem regulamentação jurídica clara e eficaz, gerando-se uma situação de risco e desamparo dentro de cada uma dessas relações.

A título de exemplo, pode-se citar no mundo das relações de consumo, as formas de abordagem à clientes, vendas e ofertas realizadas por robôs. Tais modalidades de serviços virtuais oferecidas ao consumidor apresentam vantagens e desvantagens sob várias óticas. As pessoas interessadas podem aderir facilmente aos serviços e ofertas de consumo em diversas plataformas para satisfazerem os seus desejos de adquirirem mercadorias ou serviços, tudo de uma forma conveniente e adequada as suas rotinas. Isso faz movimentar esse tipo de economia e contribui para o crescimento da economia informal.

No entanto, o que se verifica é que o consumidor está bastante e, ainda mais, vulnerável nesse meio virtual, uma vez que os seus dados passaram a ser manipulados por computadores que fazem uso dessas informações a todo instante, sem o devido controle e cuidado com elas.

1.2 A SOCIEDADE DA INFORMAÇÃO E A REVOLUÇÃO 4.0

No âmbito dos diversos conceitos de sociedade da informação, aborda-se neste trabalho aquele que define a sociedade atual como da informação a partir da visão de aproximação entre os países desenvolvidos e em desenvolvimento, no aspecto de ampliação de mercado e estímulo a globalização, impulsionados pelas conquistas tecnológicas na área da Tecnologia da Informação e das Comunicações – TIC.

Nessa linha, tem-se que:

[...] no final do século XX, quando a maioria dos países desenvolvidos já

havia construído a infraestrutura das TIC, e seus mercados começam a se saturar, intensificam-se as pressões com relação aos países em desenvolvimento para que deixem a via livre ao investimento das empresas de telecomunicações e informática em busca de novos mercados para absorver seus excedentes de lucros (BURCH, 2005).

Por causa do grande avanço da internet e das TICs, como abordado acima, a partir de 1995, nos encontros das nações mais desenvolvidas do planeta (G7 depois G8), nos fóruns da União Europeia e OCDE, foi incluído o assunto com a denominação de Sociedade da Informação. Na mesma época o termo foi encampado pelos Estados Unidos e pela ONU. Tudo isso gerou uma grande repercussão midiática em torno do tema (BURCH, 2005).

A partir de 1998, esse nome foi cotado para constar como título das Cúpulas Mundiais que se realizaram nos anos de 2003 e 2005. Explica Burch (2005 p. 55), sobre o contexto ideológico político que norteou a utilização da expressão àquela época:

[...] o conceito de “sociedade da informação” como construção política e ideológica se desenvolveu das mãos da globalização neoliberal, cuja principal meta foi acelerar a instauração de um mercado mundial aberto e “auto-regulado”. Política que contou com a estreita colaboração de organismos multilaterais como a Organização Mundial do Comércio (OMC), o Fundo Monetário Internacional (FMI) e o Banco Mundial, para que os países fracos abandonem as regulamentações nacionais ou medidas protecionistas que “desencorajassem” o investimento; tudo isso com o conhecido resultado da escandalosa intensificação dos abismos entre ricos e pobres no mundo.

Sendo assim, o conceito que se refere a *Sociedade da Informação* passou a ser utilizado a partir do desenvolvimento da Tecnologia da Informação e Comunicação no final do século XX e primeira década do século XXI.

Em nossos dias, esse termo é compreendido como, a sociedade onde o conhecimento, as tecnologias da informação e comunicação são os elementos centrais que governam a economia, sendo essenciais para a obtenção de êxito nos negócios e nas demais áreas de atuação em um mundo de mercados mais competitivos e internacionalizados (MARQUES, 2022).

O impacto de toda essa tecnologia na economia e, conseqüentemente, nas relações de consumo, em âmbito mundial, é resultado da evolução no meio industrial, mais conhecida como Indústria 4.0 ou Revolução 4.0. A cadeia produtiva está marcada pela era digital, pela interação de humanos com robôs e máquinas, apresentando características próprias como velocidade, amplitude, profundidade e

impacto sistêmico. (SCHWAB, 2016)

Nesse contexto, surgiu o trabalho em plataformas digitais, bem como a oferta de serviços *on-demanda*² e *just-in-time*³, por meio de aplicativos, a exemplo do *iFood*, *UBER* e *Rappi*. Há também outras modalidades como *Airbnb*, *Facebook*, *Google* e *crowdwork*.

Acerca do tema, leciona Hillary Christine Piedade Inácio (2021, p. 2) em artigo publicado na Revista Eletrônica do TRT da Bahia, *in verbis*:

Assim, as empresas de plataformas (Facebook, Google, Amazon, Netflix) são paradigmas dessa indústria 4.0, nas quais os meios de produção são, em síntese, a capacidade de processamento de informações. Na atualidade, inclusive, essas empresas digitais detêm valor muito maior do que as típicas empresas fabris e, como consequência, ocorrem transformações e novos arranjos no modo de trabalhar, especialmente através dessas plataformas digitais.

Esses serviços, dentre outros, são frutos da *gig economy*, que se caracteriza pela flexibilidade, inovação e trabalho *freelance*. Economia alternativa que surgiu para suprir incertezas financeiras. Ademais, alguns desses serviços também fazem parte da economia de compartilhamento que consiste em disponibilizar um bem de propriedade particular para alcançar um aumento de renda (COOK, 2016, apud RAMALHO et al, 2020).

A sociedade pós-industrial ou da revolução 4.0 passou, portanto, a vivenciar momentos de ofertas de serviços e consumo com novas exigências, mas, sem a devida adequação às normas de proteção de dados. Tal conjuntura econômica gerou situações de insegurança jurídica e desproteção ao consumidor, que se encontra, *a priori*, destituído de garantias legais em face de compras, trocas e da proteção de dados sobretudo. (MARQUES, 2022).

Exsurge daí um problema social que ganha cada vez mais espaço na seara do Direito, diante das novas formas de relações de consumo, qual seja, a insegurança jurídica do consumidor no tocante à proteção de seus dados.

A Quarta Revolução Industrial e a adoção de novas tecnologias impactaram a sociedade de um modo geral, com mudanças em proporções fenomenais, fazendo com que organizações promovessem debates sobre o assunto e sobre o futuro das

² Sob demanda, disponível em: <https://www.linguee.com.br/ingles-portugues/traducao/on+demand.html>

³ Na hora certa, disponível em: <https://www.linguee.com.br/ingles-portugues/traducao/on+demand.html>

relações de consumo, a exemplo do Fórum Econômico Mundial (SCHWAB, 2016).

Sobre este aspecto Wentzel (2016), acrescenta:

A edição deste ano (2016) do Fórum Econômico Mundial, em curso em Davos, na Suíça, tem como tema central a chamada "Quarta Revolução Industrial". Essa realidade, que já começamos a experimentar no dia a dia, significa uma economia com forte presença de tecnologias digitais, mobilidade e conectividade de pessoas, na qual as diferenças entre homens e máquinas se dissolvem e cujo valor central é a informação.

A fase pós-moderna, chamada de modernidade líquida por Bauman (2001, p.58), apresenta uma:

sociedade marcada pela agitação, pela ansiedade e acima de tudo pela incapacidade de obter uma experiência profunda de felicidade e bem-estar, a disposição consumista desponta como uma forma compensatória do indivíduo vir a obter um razoável nível de prazer em sua vida cotidiana.

Portanto, há uma flexibilização do conceito tradicional de consumo, dando espaço para o dinamismo, autonomia e certa liberdade aos fornecedores na prestação dos serviços e produtos, rompendo antigos paradigmas em virtude da globalização e gerando um aumento da insegurança jurídica no tocante à privacidade dos dados pessoais dos consumidores. (DONEDA, 2021)

A título de exemplo, hoje em dia o consumidor pode fazer uma compra, em alguns minutos, estando no Brasil e adquirindo um produto da China. Tudo por meio de aplicativos das lojas. Basta inserir seus dados pessoais que tudo é realizado. É aí onde se encontra um grave problema: a vulnerabilidade dos dados do consumidor.

Diante desse contexto, importante discorrer brevemente sobre a evolução da rede mundial de computadores, para que se possa perceber a dimensão global do fluxo dos dados.

1.2.1 Evolução da Rede Mundial de Computadores

Já no início da automação das atividades da sociedade moderna, quando o uso dos computadores era individualizado ou interligado em pequenas redes locais, a forma de armazenamento de dados sofreu grandes e rápidas transformações. Tornou-se possível o arquivamento, a recuperação e a alteração das informações com precisão, em grande quantidade e com rapidez. As antigas máquinas de escrever foram rapidamente aposentadas. Os dados que eram guardados em

imensos arquivos físicos, registrados em livros e fichas, passaram a ser arquivados em dispositivos eletrônicos.

Lins (2013, p.15) explica ainda que:

Os primeiros computadores comerciais já vinham com processadores específicos para comunicação de dados (“datacomm processors”) que operavam com protocolos, os conjuntos de regras para troca de mensagens organizadas entre máquinas, ainda bastante simples. O objetivo era a comunicação ponto a ponto, ou seja, entre dois equipamentos diretamente conectados. Um computador podia então trocar dados diretamente com outros computadores ou com terminais de vídeo, que se limitavam a inserir comandos ou dados diretamente no equipamento a que estavam ligados. As trocas de mensagens entre vários computadores eram, nesse contexto, controladas por um equipamento central, que enviava e recebia dados dos demais.

Esta realidade ganhou um impulso muito significativo no final da década de 60 e anos 70, do século XX, quando obtiveram êxito os estudos voltados à transmissão de dados em redes de longo alcance. Os Estados Unidos, que tomaram a dianteira nessa área, a princípio concentraram as pesquisas no campo dos interesses militares, mas, com os primeiros resultados positivos, as universidades também se engajaram.

A primeira conexão foi realizada em 1969, na Califórnia-USA, entre computadores da Universidade da Califórnia (UCLA) e do Stanford Research Institute (SRI). Ressalte-se que, apesar de os ingleses já estarem desenvolvendo experimentos sobre redes de longa distância, foram os americanos que a tornaram realidade (LINS, 2013)

As pesquisas americanas deram um importante passo com a primeira rede de computadores por via telefônica. Entretanto, foi em 1973 que a ARPANET, como foi batizada, obteve uma grande adesão no meio científico e acadêmico, quando foram interligados cerca de quarenta pontos, entre máquinas locais a outras países como Reino Unido e Noruega. Em pouco tempo centenas de universidades americanas estavam conectadas. a Arpanet foi, portanto, o embrião de uma rede mundial, a “rede de redes”, a Internet que hoje conhecemos. (LINS, 2013)

Outro importante marco dessa trajetória foi a entrada no mercado do microcomputador nos moldes em que foi lançado em 1977, pois proporcionou a junção que faltava, para que as conexões da época, máquina pessoal e acesso à linha telefônica, se desenvolvessem até atingir o alto padrão tecnológico dos nossos

dias.

Abre-se aqui um parêntese para explicar o surgimento do termo Internet. Em 1983, com a padronização dos nodos ou pontos de acessos, ou seja, endereços dos computadores ligados a rede das redes, generalizou-se o uso do termo "Internet" para a estrutura constituída pelas redes que usavam os protocolos TCP/IP⁴ ou que eram capazes de comunicar com as redes TCP/IP (LINS, 2013).

Todo o processo de ajuste de programação, sistemas, padrão de equipamentos, armazenamento e manipulação de dados, integrantes da rede mundial de computadores foi aperfeiçoado no período compreendido entre o final da década de 70 e início da década de 90, quando a internet se tornou pública e avançou de uma maneira extremamente rápida no cotidiano das pessoas, praticamente em todo planeta.

Esse momento, de acesso público à internet transformou a vida contemporânea: nasce assim a hiperconexão. Surgiram ainda as novas características dessa massiva conectividade: a datificação, processo de monitoramento de toda e qualquer conexão em redes digitais, que proporciona a captura dos dados pessoais e sobretudo alimenta o *big data* com altos volumes de informações, em uma escala astronômica; a economia de dados, baseada na comercialização dos conteúdos obtidos pela datificação, transformando essas informações na principal fonte de produção de riqueza e inteligência para os negócios; e por fim a exposição nas redes sociais, espaço em que as pessoas compartilham e trocam mensagens sobre suas experiências e, até mesmo, sobre sua intimidade. (BENTES, 2022)

Dentro desse contexto, não se pode perder de vista, como destaca Bentes (2022), que a privacidade é um direito fundamental, garantido pela Constituição Federal de 1988. Isso significa que se trata de uma parte inerente ao cidadão que deve ser protegida de violações.

Por fim, uma vez que o conceito sobre a proteção à privacidade se tornou mais amplo, provocado pelo grande volume de dados privados disponibilizados na

⁴ O TCP/IP é fundamental para a rede de internet. Esses dois protocolos garantem que pacotes de informações cheguem a seu destino de forma correta e segura. Soyo, Ricardo. <https://tecnoblog.net/responde/o-que-e-tcp-ip/>, acesso em: agosto, 2023

rede digital, sujeitos a diversos critérios de manipulação, autorizados ou não, necessária se torna a proteção dessas informações pessoais, reunindo-se o direito à privacidade ao direito a proteção dos dados pessoais.

Nota-se que, além da mudança de conteúdo, alterou-se a denominação do instituto, ora nomeado por privacidade, agrega hoje, por conseguinte, a proteção de dados pessoais.

No Brasil, o conceito de defesa à privacidade acompanhou toda essa evolução tecnológica ligada à proteção de dados pessoais. Foram adotados, pela doutrina brasileira, os princípios consolidados em âmbito internacional, bem como na jurisprudência, como na produção legislativa.

Quanto ao fluxo de dados pessoais dos brasileiros na internet, a situação não é diferente da população do resto do mundo. As redes de computadores no Brasil, que foram criadas, como em outros países, com propósitos governamentais, hoje já integram a teia mundial de informação. (LINS, 2013).

Todavia, essa evolução gerou também uma enorme preocupação com relação aos vazamentos desses dados.

Trata-se do fenômeno da *data leak* ele ocorre quando os dados confidenciais de uma pessoa ou de uma organização são indevidamente acessados, coletados e divulgados na internet ou repassados a terceiros (ANPD, 2020).

1.2.1 Data Leak (vazamento de dados)

Esse termo é originado da língua inglesa e quer dizer objetivamente vazamento de dados.

Existem vários casos de *data leak* históricos na sociedade da informação. Para fins introdutórios, é importante se saber dos tipos de dados que podem vazar:

[...] credenciais de acesso, como nomes de usuário e senhas, informações financeiras, como números de contas bancárias e de cartões de crédito documentos, como CPF, RG e carteira de habilitação informações de contato, como endereços e números de telefone registros de saúde, como resultados de exames e prontuários médicos outros dados, como data de nascimento e nomes de familiares (ANPD, 2020).

Vazados esses dados, o consumidor fica vulnerável a ataques futuros em suas contas de e-mails, mensagens de texto e ligações telefônicas. Informações

vazadas trazem o risco de expor o consumidor e sua família, podendo ser vítimas de abertura de contas falsas, dívidas ou golpes.

A ANPD (2020) apresenta uma gama de possibilidades de riscos a que o consumidor pode ser submetido:

FURTO DE IDENTIDADE E INVASÃO DE CONTAS ON LINE: abertura de contas em seu nome; tentativas de adivinhação de senhas ou para responder perguntas de segurança; uso de senhas vazadas para invadir outros serviços onde a mesma senha é usada, se não se tiver ativado algum mecanismo de segurança adicional como verificação em duas etapas, ou autorização prévia de dispositivos;

FURTO DE IDENTIDADE LEVANDO A PREJUÍZOS FINANCEIROS: criação de cartões de crédito, contas bancárias e empréstimos, levando a dívidas ou transações ilícitas em seu nome; movimentações financeiras indevidas em suas contas bancárias ou cartões de crédito; transferência de bens móveis ou imóveis;

VIOLAÇÃO DE PRIVACIDADE: exposição de informações privadas, como dados médicos ou conversas particulares;

TENTATIVAS DE GOLPES: extorsão, onde o atacante faz chantagem para não expor os seus dados; quanto mais informações um atacante tiver, mais convincente ele será, e mais facilmente enganará outras pessoas; os dados vazados podem ser usados, por exemplo: em tentativas de *phishing* direcionado e personalizado (*spear phishing* – uma espécie de pesca de presas para aplicação de golpes, com a utilização de sites clonados); para convencê-lo a revelar mais informações; para induzi-lo a efetivar transações; para se passar por você;

Percebe-se, por conseguinte, que o vazamento de dados é na verdade um incidente de segurança cibernética que vem a público com informações sensíveis, que podem ser vistas, copiadas, apropriadas, repassadas ou usadas sem acesso autorizado.

Surpreendentemente, inúmeras causas de invasões não são provocadas por roubos ou ação de hackers⁵ como malware⁶, spyware⁷, ransomware⁸, etc, mas por outras falhas, consideradas simples, atribuídas a configurações de segurança que

⁵ É uma palavra da língua inglesa que, no âmbito da informática, designa alguém capaz de invadir dispositivos eletrônicos, redes e sistemas de computação.

<https://www.significados.com.br/hacker/#:~:text=hacker%20c3%a9%20uma%20palavra%20da,ou%20para%20praticar%20atos%20il%20c3%adritos>

⁶ Malware é um termo amplo que é usado para classificar todo tipo de software malicioso usado para causar prejuízo. <https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghml>

⁷ Software malicioso que tenta infectar seu computador ou dispositivo móvel e que coleta informações sobre você, sua navegação e seus hábitos de uso da Internet, bem como outros dados. *Idem*

⁸ É um software de extorsão que pode bloquear o seu computador e depois exigir um resgate para desbloqueá-lo. *Idem*

poderiam ser corrigidas. Diferentes causas podem ser incluídas, tais como, funcionários descontentes ou desonestos, erros de colaboradores, pouco conhecimento técnico para proteger os dados (MANDARINO JR.; CANONGIA, 2010).

A título de exemplo, alguns casos de vazamentos de dados, com repercussão, podem ser citados.

Yahoo: em 2017, com 3 bilhões de contas invadidas por *spear phishing*⁹:

Esse é, até hoje, e de maneira disparada, o maior caso de vazamento de dados da história. Acontecido em 2013, mas apenas descoberto anos depois quando a Yahoo foi vendida para a Verizon, causou uma perda de 350 milhões de dólares no valor de venda da Yahoo. Foram roubados nomes, datas de nascimento, telefones e senhas armazenadas com criptografia fraca (GATINFOSEC, 2023).

Aadhaar: em 2018, com 1,1 bilhões de pessoas prejudicadas por falha na API de sites etc:

Aadhaar é o sistema nacional de identidade da Índia, contém dados biométricos como impressões digitais, entre outros dados demográficos, da identidade de mais de 1.1 bilhões de cidadãos indianos. Os indianos são praticamente obrigados a se cadastrar na Aadhaar para acessar os serviços públicos. Todas essas informações foram vazadas (GATINFOSEC, 2023).

First American Corporation, em 2019, uma quantidade extraordinária de registros vazados, cerca de 885 milhões, por falha na estrutura do aplicativo:

A empresa de seguros e serviços financeiros vazou dados extremamente sensíveis contendo, por exemplo, informações bancárias detalhadas. Os documentos eram cópias digitalizadas que podiam ser acessadas via o site da empresa firstam.com. Eram documentos destinados à visualização apenas das partes envolvidas em uma transação (em grande parte de compra e venda de imóvel) que estavam acessíveis para qualquer um com o link, apenas alterando um único dígito e sem proteção de login, senha ou duplo fator de autenticação. O desenvolvedor Ben Shoval descobriu a falha da pior maneira possível: após visitar um link de seus próprios documentos (GATINFOSEC, 2023).

Verifications.io⁹, também em 2019, neste caso foram 763 milhões de emails invadidos, por inconsistência no banco de dados:

Os 763 milhões de emails foram encontrados por um pesquisador em

⁹ É um ataque que persegue um único alvo, que pode ser um indivíduo, organização ou empresa. <https://www.cloudflare.com/pt-br/learning/access-management/spear-phishing/#:~:text=Embora%20phishing%20seja%20um%20termo,um%20indiv%C3%ADduo%20C%20organiza%C3%A7%C3%A3o%20ou%20empresa. Empresa que faz validação de e-mails para companhias de e-mail marketing.>

uma instância MongoDB exposta publicamente. Além dos emails alguns registros continham telefones, nomes e outras informações sensíveis coletadas a partir do serviço de verificação de emails Verifications.io (GATINFOSEC, 2023).

Marriot/Standford: em 2018, com 500 milhões de pessoas atingidas por possível infecção de *RAT (Remote Access Trojan) por phishing*:

As informações expostas incluíam nomes, números de passaporte, informações de contato e outras informações pessoais. As informações de cartão de crédito e débito estavam criptografadas, o que não garante que não foram também acessadas. O sistema da Starwood foi invadido em 2014 e o acesso não autorizado permaneceu até depois da compra da Starwood pela Marriot em 2016. A invasão foi descoberta apenas em 2018 (GATINFOSEC, 2023).

FriendFinder¹⁰, em 2016, utilizaram-se do *exploit*, atingindo 412 milhões de pessoas, interligadas em pelas redes da empresa:

Foram vazados 6 bancos de dados que incluíam nomes, emails, senhas da empresa que é dona de sites como o Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com. Entretanto, informações sensíveis como preferências sexuais não foram vazadas como em um incidente em 2015 da mesma empresa que teve 4 milhões de contas expostas. A maioria das senhas estava desprotegida ou contava apenas com um fraco algoritmo de criptografia SHA-1 (GATINFOSEC, 2023).

Muitos são os eventos de invasão digital de dados em todo mundo:

De acordo com levantamento da Tenable 2,29 bilhões de registros foram expostos em 2022, enquanto mais de 800 milhões foram vazados devido à negligência na proteção dos bancos de dados. O relatório anual da companhia sobre o cenário de ameaças no ano passado também destacou que foram expostos 257 terabytes de dados ao redor do planeta, desse número, 112 terabytes apenas no Brasil. (...) No Brasil, por exemplo, o ransomware foi a causa de mais 52% dos ciberataques, contra 35,4% da média global. O governo foi o segmento mais afetado registrando 42%, seguido pelo varejo (19%) e pelo setor de financeiro e de seguros (9%). Em um cenário global, os segmentos de saúde e assistência social continuam sendo os setores com maior número de casos de violação, com 35,4% de todos os casos analisados (SILVA, 2023).

Portanto, o impacto da Indústria 4.0 tem, ao mesmo tempo, consequências positivas e negativas na cadeia consumidora, mas são as últimas que geram uma vulnerabilidade cada vez maior nas relações de consumo, o que expõe a exploração do consumidor em benefício do capital e da economia.

Bauman (2021) explica que, na atual sociedade da informação, o bem mais valioso é a própria informação. E são as informações dos consumidores que estão em jogo.

Dentro desta dinâmica de armazenamento e tratamento dos dados que circulam nas redes digitais, nasce o *big data*, um dos maiores responsáveis pelas mudanças atuais nas relações de consumo. Trata-se de tecnologia de arquivo das informações coletadas, que permite a estruturação e organização dos dados para determinadas finalidades, em grande volume e em velocidade instantânea, o que marca a fase mais atual da denominada Sociedade da Informação (OLIVEIRA, 2021, p. 34):

A realidade posta pelas transformações tecnológicas, pelo surgimento da Sociedade da Informação e pela informação como insumo da economia capitalista refletem o novo papel que os dados pessoais possuem. Os recursos, os produtos e os serviços de informação são identificados na Internet com o nome genérico de conteúdo, de modo que qualquer usuário, em caráter individual ou institucional, possa vir a ser produtor, intermediário e usuário de conteúdo, a exemplo do que ocorre com o Facebook. É por meio da operação de redes de conteúdos de forma generalizada que a sociedade atual se move para a Sociedade da Informação.

Os bancos de dados são, portanto, a finalidade da administração de conteúdos, do acúmulo do conhecimento e da absorção do aprendizado na Sociedade da Informação. O risco do tratamento e cruzamento dos dados armazenados em grandes repositórios, torna-se evidente, como visto nos exemplos anteriores. Em razão disso, as consequências identificadas pela ligação entre Sociedade da Informação e Sociedade de Consumo levam ao debate sobre o direito à privacidade, que sabidamente, abrange um universo além da proteção à intimidade da pessoa, alcançando a personalidade de milhões de cidadãos, que têm seus dados coletados, arquivados, tratados e cruzados diuturnamente entre bancos de dados através dos recursos da tecnologia da informação.

1.3 A PRIVACIDADE EM RISCO

Nos dias de hoje, os cadastros dos clientes em um comércio já não são feitos como antigamente, através de fichas ou livros. As empresas buscam informações sobre potenciais clientes, antes mesmo de conhecê-los, ou até mesmo antes de eles manifestarem o desejo de adquirir um produto em determinada loja, causando com este procedimento um verdadeiro risco a privacidade do cidadão.

Dando subsídio a esse tipo de ação para o meio empresarial, está a coleta, o tratamento e a comercialização de dados pessoais, que vão possibilitar a

ampliação da base de clientes, a oferta de novos serviços aos clientes antigos, a tomada de decisões a respeito do ambiente competitivo, o aumento da eficiência no processo produtivo, e ainda a diminuição dos riscos das operações. Mas, os mecanismos de obtenção de dados pessoais, dos usuários/consumidores nas redes sociais e em outras plataformas digitais privadas, precisam ser analisados com cuidado.

A coleta de dados digitais passa despercebida por grande parte dos usuários da internet. Isso porque são dados extraídos por meio dos valores gerados da nossa atenção e dos rastros dos nossos comportamentos on-line: a relação entre o tempo de conexão à rede (*internet*), coleta de dados, armazenamento de informações e produção de ativos para as empresas de tecnologia, na economia digital, é extremamente relevante e rentável. Quanto mais tempo de acesso às plataformas digitais, maior é a possibilidade de se fornecer informações que possibilitem gerar conteúdos de identificação úteis a individualizar o usuário/consumidor (BENTES, 2021).

Em outra vertente, o poder público, por sua vez, também é um grande detentor de dados pessoais e dados sensíveis dos cidadãos. A coleta dessas informações é, em muitos casos, obrigatória, o que gera maior responsabilidade no tratamento desses dados.

Ressalta-se, ainda, que o fluxo dos dados em um espaço sem fronteiras cria um novo tipo de poder. Coletar, controlar dados, com a finalidade de prever comportamento, tem-se tornado frequente na sociedade da informação.

A importância dos dados pessoais para a sociedade moderna é tamanha, como se pode observar na realidade dos dias atuais, que estes foram reconhecidos como parte integrante da dignidade da pessoa humana.

Para que se possa discorrer sobre esse viés, fazem-se necessários alguns esclarecimentos a esse respeito.

1.3.1 Os dados pessoais como direito humano fundamental

A ideia de direitos humanos, como compreendida hoje, era estranha ao pensamento das pessoas até o final da Idade Média. Conforme registros, não havia

um termo que caracterizasse a ideia de direito, na forma de direito individual. O conceito atual de direitos humanos principia a criar forma no fim da Idade Moderna, tendo como base o Renascimento, a criação do Estado Moderno, a Reforma Protestante, a Revolução Científica, e, no século XVIII, o Iluminismo, tendo neste seu impulso decisivo. Mais adiante, ganha reforço com a Declaração dos Direitos do Homem e do Cidadão, em 1789, marco da Revolução Francesa, que trouxe consigo direitos naturais, inalienáveis e sagrados do homem (BARROSO, 2019).

Entretanto, com advento da Segunda Guerra Mundial, de 1939 a 1945, notou-se a falta de proteção aos direitos inerentes à pessoa humana, haja vista todas as crueldades praticadas pelos nazistas contra a individualidade da pessoa humana e contra a própria humanidade. Dessa forma, era necessária uma tutela fundamental que assegurasse a personalidade humana, garantindo assim a própria raça humana. Intrinsecamente, nesse contexto, surge, em 1948, a Declaração Universal de Direitos Humanos (FARIAS; ROSENVALD, 2015).

A Declaração Universal de Direitos Humanos, em seu art. 1º, determina que “Todos os seres humanos nasçam livres e iguais em dignidade e direitos. São dotados de razão e consciência e devem agir em relação uns aos outros com espírito de fraternidade.” (ONU, 1948).

No final dos anos 40, século XX, o termo dignidade da pessoa humana começou a fazer parte do preâmbulo ou do corpo das novas Constituições, principiando-se pela Carta Constitucional da Alemanha em 1949 e, posteriormente, pela Itália, Japão, Portugal, entre outros. Visando à proteção dos direitos humanos, cortes internacionais foram criadas, tais como a Corte Europeia de Direitos Humanos, a Corte Interamericana de Direitos Humanos e o Tribunal Africano dos Direitos do Homem e dos Povos (BARROSO, 2019).

No Brasil, encontra-se expressa no inciso III, do art. 1º, da Constituição Federal de 1988, a dignidade da pessoa humana, que tem um papel de destaque entre os fundamentos constitucionais do Brasil. A dignidade é centro axiológico do constitucionalismo contemporâneo, sendo o valor supremo na Constituição. Dessa forma, deve servir como diretriz para a elaboração, interpretação e aplicação das normas do ordenamento jurídico brasileiro e do sistema de direitos fundamentais, além de ser usado como base para julgar casos concretos (NOVELINO, 2016).

Com absoluta supremacia das normas constitucionais e o princípio da dignidade da pessoa humana, como um dos fundamentos da Constituição, impõem-se ao intérprete, principalmente ao Poder Judiciário, a aplicação de norma mais favorável à proteção dos Direitos Humanos, como também a interpretação de forma a aplicar e garantir maior e ampla proteção (MORAES, 2020).

A dignidade, para Moraes (2020), exprime um valor tanto espiritual como moral intrínseco à pessoa, que se revela na autodeterminação consciente e responsável da própria vida, tem em sua essência a necessidade de respeito por parte das demais pessoas, revelando-se um valor indispensável a ser tutelado pelo ordenamento jurídico. Ocorre, por vezes, relativização a aplicação dos direitos fundamentais, somente em casos excepcionais, mas sempre buscando preservar o apreço ao ser humano e buscando o Direito à Felicidade.

Segundo Novellino (2016), a dignidade em si não constitui um direito, mas uma qualidade inerente a todo ser humano, não se pode levar em consideração características como origem, sexo, idade, condição social ou demais requisitos. A dignidade possui caráter absoluto, não comporta gradações, ou seja, não existem pessoas com mais ou menos dignidade. No entanto, o princípio da dignidade não é absoluto, pois, apesar do seu peso elevado na ponderação, o seu cumprimento ocorre em diferentes graus, a depender das possibilidades fáticas e jurídicas presentes no caso concreto, assim como ocorre com os demais princípios.

Em uma concepção minimalista, identifica-se três elementos que compõem a dignidade humana: o valor intrínseco da pessoa humana; autonomia individual; e o valor comunitário.

O valor intrínseco significa que ninguém é um meio pelo qual outras pessoas se utilizem para realização de projetos pessoais ou de metas coletivas, pois a dignidade não tem preço. Quanto ao plano jurídico, o valor intrínseco é fundamento de diversos direitos fundamentais, tais como, o direito à vida, à igualdade - incluindo-se aqui a igualdade formal, pois não pode haver discriminação arbitrária na lei ou perante a lei -, à integridade física – destaca-se a proibição de tortura, do trabalho escravo e as penas cruéis -, e à integridade moral ou psíquica - englobando a privacidade, a honra e a imagem (BARROSO, 2019).

No tocante a autonomia individual, trata-se do elemento ético da dignidade no

plano filosófico. A autonomia é a capacidade do indivíduo de se autodeterminar, o poder de decidir sozinho suas escolhas e viver seu ideal de vida, devendo, ser-lhe garantido um mínimo existencial, ou seja, o acesso aos bens vitais para que não lhes seja privado.

No plano jurídico, a autonomia envolve uma dimensão privada, uma dimensão pública, além de um pressuposto da satisfação de um mínimo existencial.

A primeira, autonomia privada, está ligada aos direitos individuais, a liberdade de expressão, de trabalho e outras.

Por sua vez, a autonomia pública está ligada aos direitos políticos e de participação na condução da coisa pública, por meio de votos, de debates públicos e de organização social. Portanto, O mínimo existencial é o pressuposto necessário para que se possa exercer plenamente a autonomia privada e pública, sendo caracterizado pela satisfação das necessidades indispensáveis à existência física e psíquica (BARROSO, 2019).

Por último, o valor comunitário, que se revela na dimensão social da dignidade humana, trata-se da limitação da autonomia diante de valores, costumes e direitos das outras pessoas na sociedade, e de imposição de normas válidas. Com seu valor coletivo, a dignidade visa a promoção da defesa dos direitos de terceiros - pois a autonomia individual deve respeitar a autonomia das demais pessoas, que também possuem direitos e liberdades.

Ao Estado está reservado o direito de proteção dos direitos do indivíduo contra si próprio – ou seja, o direito de proteger a pessoa contra atos que possam lesioná-la, como ocorre com a obrigação de usar cinto de segurança -, e dos direitos de valores sociais - que correspondem à moral social compartilhada pela sociedade. A imposição forçada de valores sociais, tanto pelo legislador como pelo juiz, necessita de fundamentação racional sólida e deve levar em conta a existência de consenso social e de risco ao direito de outras pessoas. No entanto, é preciso evitar o paternalismo, o moralismo e a tirania das majorias (BARROSO, 2019).

Para Novellino (2016), a dignidade da pessoa humana, enquanto fundamento da Constituição consagrado no inciso III, do art. 1º, da CF/88, possui tripla dimensão normativa. A primeira é uma metanorma, servindo-se como diretriz para a elaboração e interpretação das normas do ordenamento jurídico brasileiro. A

segunda é um princípio, impondo ao Estado o dever de proteção da dignidade, assim como a promoção de valores, bens e demais itens indispensáveis a uma vida digna. A terceira é uma regra que determina ao Estado e à terceiros o dever de respeito à dignidade, pois ninguém pode ser tratado como objeto, ou seja, com desprezo.

A dignidade da pessoa humana e os direitos fundamentais estão interligados por uma relação de dependência mútua. Os direitos fundamentais surgiram como uma exigência da dignidade, a fim de proporcionar um pleno desenvolvimento da pessoa humana, mas, apesar disso, é necessária a existência desses direitos fundamentais para que haja o respeito, proteção e promoção da dignidade. Compreende-se, por isso, que o princípio da dignidade da pessoa manifesta juridicamente a ideia de ser humano, consagrada por um conjunto de direitos fundamentais.

O reconhecimento de alguns direitos fundamentais decorre da primazia da dignidade da pessoa humana, que se trata do núcleo valorativo da Constituição. Os direitos fundamentais derivam da dignidade da pessoa humana, mas não com a mesma intensidade, pois alguns derivam de forma direta, tais como a vida, a liberdade e a igualdade, e outros de forma indireta (NOVELINO, 2016).

Ao disciplinar diversos institutos claramente civilistas, tais como a família, a propriedade, dentre outros, o legislador redimensionou a norma privada, determinando os parâmetros fundamentais a serem utilizados na sua interpretação: estabeleceu como princípios norteadores do Brasil a dignidade da pessoa humana (art. 1º, inciso III, da CF), a solidariedade social (art. 3º, da CF) e a igualdade substancial (arts. 3º e 5º, da CF), incluindo ainda a erradicação da pobreza e redução das desigualdades sociais, com a finalidade de promover o bem de toda a população (art. 3º, incisos III e IV, CF). Sendo assim, tanto o Direito Público quanto o Privado, sujeitam-se aos princípios fundamentais insertos na Constituição, que tutelam a dignidade da pessoa humana (FARIAS; ROSENVALD, 2015).

O reconhecimento do princípio da dignidade da pessoa humana como fundamento obriga que os civilistas modernos tomem uma nova postura, pois devem garantir à vida humana de maneira prioritária e integral ao interpretar e aplicar as normas e conceitos jurídicos. Verifica-se que todas as normas jurídicas do Direito

Civil, assim como as dos demais ramos da ciência jurídica referentes à personalidade jurídica têm que estar direcionadas à dignidade do homem (FARIAS; ROSENVALD, 2015).

Infere-se assim que o direito de dados pessoais protegidos é um direito humano fundamental, assegurado pela Constituição, como forma de garantia da dignidade da pessoa humana. É uma afronta à Constituição, e ao próprio Estado Democrático de Direito, a violação dos dados pessoais das pessoas em uma sociedade da tecnologia. Novas configurações se formam nessa nova sociedade e, por conseguinte, novos valores também. A necessidade de proteção dos dados pessoais é um desses novos valores da atualidade.

1.3.2 Tutela da Privacidade

Na Era da Sociedade da Informação, a preocupação mais debatida no meio jurídico, cinge-se a questão da privacidade. Este instituto se relaciona com nosso direito de monitorar as formas de compartilhamento e utilização dos dados relativos as nossas vidas, para quem ou para que, e como serão usados. O direito à privacidade é um dos direitos humanos fundamentais para a dignidade humana e para a autodeterminação informativa.

Os limites entre o público e o pessoal, dependem da cultura, dos costumes de cada lugar, bem como do contexto histórico no qual estão inseridos. Ao pensarmos, no ambiente digital, nos deparamos com a dificuldade da padronização indevida, construída em uma extensão que navega por diversas culturas, sem se preocupar se o público e o privado de uma região se encaixam com os conceitos de outras, priorizando-se, não raro, o perfil comercial mais lucrativo.

Nas redes digitais e fora delas, a legislação brasileira garante o direito à privacidade a todos. Quando há necessidade legal de violação à privacidade de uma pessoa, essa ação deve ser justificada, obedecendo-se aos princípios da razoabilidade e proporcionalidade.

O impasse que nos aflige sobre os nossos dados inseridos nas redes sociais é o seguinte: quem acessa nossas informações pessoais o que fazem com elas? O controle desses cliques, na *internet*, foge de nossas mãos, mesmo que o interlocutor

digital garanta que somente amigos e familiares verão tais dados, não nos sentimos seguros.

Sendo assim, a saída para tal embaraço está na aplicação urgente das normas limitadoras desse universo digital, maravilhoso e ao mesmo assustador.

A seguir, apresenta-se um breve histórico a respeito da preocupação mundial com a tutela da privacidade.

1.3.2.1 Histórico Legal

A preocupação com o direito à privacidade é uma das teses basilares do direito estadunidense. Entretanto, as primeiras tentativas de normatizar o uso dos dados é alemã, por volta dos anos 70, com a Lei de Proteção de Dados pessoais do Lande de Hesse. Ao longo das décadas, foram surgindo diversas regulações específicas, como a sueca, a francesa, dinamarquesa, entre outras (FERREIRA; PINHEIRO; MARQUES, 2022).

Em 1981, o Conselho da Europa cria a Convenção 108, incitando a adoção de normas específicas para o tratamento desses elementos sob seus próprios parâmetros. Essa convenção tem uma perspectiva universal, não sendo criada apenas para os países europeus. Já em 1995, surge a Diretiva 95/46/CE, estabelecendo uma definição básica de dados pessoais e outras delimitações importantes para a discussão do tema, além do incentivo ao comércio. O Regulamento Geral de Proteção de Dados (GDPR) assume o lugar dessa diretiva, em 2018, sendo diretamente aplicada a todos os países-membros da União Europeia (FERREIRA; PINHEIRO; MARQUES, 2022).

Sob o recorte brasileiro, o direito à privacidade das informações pessoais é assegurado pela Constituição, como disposto pelo inciso XII do art 5º:

[...] 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.

Acrescentado pela Emenda Constitucional nº 115/2022, que alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e

garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Além disso, outros códigos já desenhavam a segurança dos dados pessoais. Podemos citar, por exemplo, o Código do Consumidor, a Lei de Acesso à Informação e, em especial, o Marco Civil da Internet, primeira a estabelecer no Brasil, de maneira direta os princípios, garantias, direitos e deveres para a utilização da Internet.

O Código de Defesa do Consumidor, sancionado em 1990, previsto pelo art. 48 do ADCT - Ato das Disposições Constitucionais Transitórias da CF/1988, veio em defesa da parte frágil nos negócios consumerista celebrados. Este diploma estabelece normas de proteção e defesa do consumidor, sendo estas de ordem pública e de interesse social, nos termos dos já citados, arts. 5º, inciso XXXII; 170, inciso V, da Constituição Federal . e ainda o art. 48 das Disposições Transitórias. Define o consumidor, como sendo toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final (BRASIL,1990)

No que concerne, mais especificamente, aos bancos de dados, o CDC em seus artigos 43 e 44, dispõem sobre o acesso do titular das informações aos cadastros, fichas, registros e dados pessoais e de consumo, arquivados sobre ele, bem como sobre as suas respectivas fontes; e ainda, sobre as reclamações a respeito de fornecedores de produtos e serviços, que deverão ser registradas e divulgadas anualmente com o devido resultado (BRASIL, 1990).

A Lei 12.527/2011, regula o acesso a informações previsto no inciso XXXIII do art. 5º, da Constituição Federal. Sobre a proteção de dados, aduz em seu capítulo II que cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar: a proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e, a proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

A Lei 12.965/2014, Marco Civil da Internet, apresenta os princípios de proteção à privacidade e aos dados pessoais, estabelece ainda, garantias, direitos e deveres para o uso da rede digital no Brasil de maneira objetiva.

Em seu art. 7º, dispõe sobre os direitos dos usuários da *internet*, da seguinte

forma: inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; e aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet (BRASIL, 2014)

Uma seção exclusiva é dedicada à proteção aos registros, aos dados pessoais e às comunicações privadas, que determina o seguinte: em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros (BRASIL, 2014)

Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular, exceto nas hipóteses previstas na Lei que dispõe sobre a proteção de dados pessoais (BRASIL, 2014)

Os legisladores brasileiros, motivados pelas ações internacionais de vazamento de dados pessoais, sentiram a necessidade de compilar essas normas em um código específico, de forma a favorecer o acesso normativo a todos.

Surgem, então, os primeiros esboços da Lei 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), que dispõe, de maneira específica, sobre a proteção

dos dados pessoais, como uma alternativa ao Marco Civil da Internet (TOMASEVICIUS FILHO; FALEIROS JÚNIOR; DALESE, 2023).

Trata-se de mais um passo na evolução da regulação dos arquivos gerados a partir das relações de consumo. Ela fez expressa menção a proteção do consumidor (arts. 2º; 18, § 8º; e 45), assegurando um diálogo entre estas fontes. Com ela, o Brasil se junta a diversos países que já possuem legislação sobre o tema. O texto da lei disciplina a forma como as informações são coletadas e tratadas, especialmente em meios digitais, como dados pessoais sensíveis, aqueles que dizem respeito somente a pessoa, e sobre sua intimidade (CARVALHO; FERREIRA, 2018)

A defesa do consumidor hoje, avançou em todo o planeta para o conceito de direito à privacidade, pois nele se compreende não apenas a privacidade, a intimidade e o segredo, mas, igualmente, que o cidadão — e o consumidor — pode determinar a quem e como permitirá o acesso a seus dados, bem como o alcance deste acesso, isto é, os limites ao uso desses dados pelo terceiro (CARVALHO; FERREIRA, 2018)

Não é sem razão que o dia 28 de janeiro foi consagrado como o Dia Internacional da Privacidade de Dados. Iniciativa que veio em 2006, com o propósito de propagar boas práticas de segurança e conscientizar ainda mais quanto a importância de se proteger os dados pessoais, das empresas e das pessoas. A data, pode-se dizer uma homenagem ao dia em que foi assinada na Europa a Convenção 108, de 28 de janeiro de 1981.

1.3.2.2 Trajetória do Conceito de Privacidade

A privacidade como direito positivado, bem jurídico tutelado e elevado à categoria de direito fundamental, por ser inerente a formação da personalidade do indivíduo, consolidou-se recentemente. Esta construção teve seu marco inicial a partir do final do século XIX. Por outro lado, a privacidade, em si, não é um tema novo, está presente em diversas fases da sociedade humana, com uma conotação vinculada às características de cada época, como se pode observar das palavras de DONEDA (2021, p. 111):

Praticamente não havia lugar para a tutela jurídica da privacidade em sociedades nas quais as condutas humanas estavam condicionadas a outra ordem de mecanismos – fosse uma rígida hierarquia social ou então uma determinada arquitetura dos espaços públicos e privados; fosse porque eventuais pretensões a esse respeito fossem neutralizadas por um ordenamento jurídico de caráter corporativo e patrimonialista; fosse, então, em determinadas sociedades nas quais a privacidade representasse não mais que um sentimento subjetivo que não poderia nem deveria ser tutelado.

Doneda (2001, p. 12) explica a história da privacidade:

Durante a Idade Média, ainda não era possível reconhecer um sistemático anseio das pessoas pela privacidade ou pelo isolamento, podia-se, no máximo, constatar que alguns poucos privilegiados podiam se isolar dos demais, como os senhores feudais que o desejassem, ou, então, as pessoas que teriam optado pela solidão, como alguns religiosos e místicos. Ao fim da Idade Média, entre os senhores feudais bem colocados na sociedade, havia manifestações que poderiam ser entendidas como indícios de surgimento de uma esfera privada em moldes similares aos atuais. Somente no século XVI iniciou-se um processo de mudança de costumes no que se refere à vida cotidiana, surgindo aí uma nova disposição arquitetônica das casas e cidades, tornando-se mais propícias à separação de classes e categorias, bem como mais favorável ao isolamento

Antes do século XIX a defesa da privacidade, portanto, era exercida de forma indireta, ou seja, era alcançada por fundamentos adjacentes ou reflexos, por intermédio de ações de defesa da liberdade, da propriedade e da honra (VIDAL, 2014).

Na segunda metade deste século, as transformações ocorridas pela percepção sobre o sentido da privacidade da pessoa levaram a diversas discussões doutrinárias, principalmente na Alemanha. Essa efervescência do debate surgiu dentre outros motivos, pelas constantes publicações da “mídia impressa e escrita” a respeito da intimidade de políticos e de pessoas famosas (ROBL FILHO, 2006, p. 185-186).

A origem do direito à privacidade foi fortalecida pelas teses filosóficas de John Locke e John Stuart Mills. Locke (1999, p. 68) desenvolveu sua ideia de liberdade “como autonomia para dispor, como bem lhe pareça de sua pessoa, de seus atos, de seus bens e de tudo quanto lhe pertença”. Já Mills (2008, p. 24) sustentava que “os únicos aspectos da conduta humana que produzem deveres e responsabilidades sociais seriam aqueles que afetassem os demais”. Para Mills (2008, p. 25), “os aspectos que só dizem respeito ao indivíduo são absolutamente independentes, sendo o indivíduo soberano sobre si, seu corpo e sua mente”.

Assim, “o surgimento da privacidade pode ser historicamente associado à desagregação da sociedade feudal, onde os indivíduos eram ligados por uma complexa série de relações que se refletiam na própria organização da vida cotidiana” (MACHADO, 2014, p. 341). O isolamento era privilégio de uma minoria eleita ou daqueles que, por opção ou necessidade, viviam longe da comunidade:

Assim, a privacidade configurava-se como uma possibilidade da classe burguesa, devido às transformações socioeconômicas referentes à Revolução Industrial. Neste contexto, pode-se afirmar que, no século XIX, a propriedade era concebida como essencial ao desenvolvimento da personalidade do indivíduo e que o direito de propriedade era condição indispensável para se chegar à privacidade (MACHADO, 2014, p. 342).

Esse instituto passa a ser prerrogativa de uma emergente classe burguesa, com componente fortemente individualista, utilizando-se da privacidade para marcar sua identidade na sociedade e para proporcionar que a burguesia se isole dentro de sua própria classe.

A ideia de privacidade parece, então, estar muito associada à ideia de exclusão, uma vez que apenas as classes mais privilegiadas economicamente tinham o domínio das propriedades. Estas faziam com que as pessoas precisassem se isolar das demais, a fim de proteger seus bens, e isso fazia com que personalidades fossem se formando. As pessoas iam se distanciando umas das e, assim, a ideia de privacidade ia se construindo. Trata-se, então, de um conceito muito próprio dos ideais liberais individualistas de nossa sociedade.

O primeiro artigo que discute a questão da privacidade como um direito é o artigo de Samuel D. Warren e Louis D. Brandeis, publicado na *Harvard Law Review*, em 15 de dezembro de 1890.

Warren e Brandeis trazem a ideia do direito à privacidade não mais ligado à propriedade individual privada, mas sim como um direito fundamentado na inviolabilidade da personalidade. Em uma abordagem bastante completa e inovadora, à época, eles redefinem o tema, suas funções e seus limites (CANCELIER, 2017, p. 221). O situam no domínio dos direitos de proteção da personalidade e da segurança do indivíduo.

Sobre o posicionamento dos referidos autores americanos, CANCELIER, (2017, p. 225), analisa um exemplo citado por eles, constante no texto do artigo em comento:

Tomando como exemplo os pensamentos de um pai escritos em uma carta para o seu filho ou em seu diário, revelando alguma informação íntima, defendem que ninguém que tenha acesso a tal documento poderia divulgá-lo, mesmo que o acesso tenha ocorrido de forma legítima; a proibição não seria restrita à publicação de uma cópia da carta ou do diário em si, sendo mais ampla, atingindo o conteúdo. O que se protege não é o ato intelectual de expressar ideias em um pedaço de papel, mas os fatos que estão sendo impressos. A proteção concedida a pensamentos, sentimentos e emoções, expressados por qualquer meio é uma das instâncias de aplicação do direito a estar só, do direito a ser deixado em paz.

Já, Mendes (2014, p. 28), identifica os limites estabelecidos por Warren e Brandeis, a respeito do direito à privacidade, da seguinte forma:

a) o direito à privacidade não impede a publicação do que é de interesse geral; (b) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer sob a guarda da lei, como, por exemplo, em um Tribunal ou em uma Assembleia Legislativa, não há violação desse direito; (c) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos; (d) o consentimento do afetado exclui a violação do direito; (e) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; e (f) a ausência de dolo também não exclui a violação desse direito.

Pois bem, dentro da trajetória evolutiva do conceito de privacidade, tomando-se como referencial, o artigo publicado por *Warren e Brandeis*, pode-se identificar três fases.

A primeira, anterior ao ponto de referência, corresponde ao individualismo exagerado, traduzido no direito de ser deixado só; num segundo momento, iniciado pela redefinição do tema, o entendimento sobre privacidade se mostra ligado a uma crescente consciência de realização humana e desenvolvimento da personalidade; e, na atualidade, a terceira fase, um novo paradigma em construção, entende-se a privacidade como um desdobramento de situações de grande complexidade, que teve início com a mudança do relacionamento entre cidadão e Estado, no contexto do *welfare state*¹⁰, bem como no crescimento do fluxo de informações provocado pelo desenvolvimento tecnológico (DONEDA, 2021)

Reforçando esse entendimento, no tocante ao desenrolar histórico do direito à privacidade, merece igual atenção a construção feita por Mendes (2014, p 29):

No decorrer do século XX, a transformação da função do Estado, aliada à revolução tecnológica, contribuiu para modificar o sentido e o alcance do direito à privacidade. De um direito com uma dimensão estritamente

¹⁰ O *welfare state* é um modelo de Estado assistencialista e intervencionista, fundado a partir dos direitos sociais universais dos cidadãos – fonte?

negativa e com uma conotação quase egoísta, passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático. É nesse sentido que se pode afirmar que o século passado vivenciou um “processo de inexorável reinvenção da privacidade.

Dentro desse contexto, o direito à privacidade, tornou-se reconhecido em âmbito internacional, abrindo caminho para a dimensão da proteção de dados pessoais, em razão das transformações no armazenamento e manipulação das informações de pessoas naturais em ambiente digital, bem como por representar, nos dias atuais, um novo paradigma ao ordenamento jurídico (MENDES, 2014).

Convém destacar, que a preocupação com o right of privacy é uma das teses basilares do direito estadunidense, mas, no entanto, as leis iniciais que tratam diretamente acerca da proteção de informações pessoais surgiram nos anos 70

Diversos países, há mais de 4 décadas, demonstraram sua precaução com os dados pessoais em arquivos eletrônicos, editando leis específicas sobre o assunto, como é o caso da Alemanha, que foi a primeira a promulgar Lei de Proteção de Dados Pessoais, em seu Estado de Land Hesse.

Ao longo dos anos, foram surgindo diversas regulações específicas, como a sueca, a francesa, dinamarquesa, entre outras. A primeira geração das normas de proteção de dados pessoais surgiu como reação ao processamento eletrônico de dados nas administrações públicas e nas empresas privadas, bem como às ideias de centralização dos bancos de dados nacionais gigantescos. (TINOCO, 2020)

A partir desse desdobramento do conceito de privacidade, aborda-se no capítulo 2, sobre o viés das relações de consumo na era digital.

CAPÍTULO 2. AS RELAÇÕES DE CONSUMO NA ERA DIGITAL

Falar em relações de consumo na era digital sem antes esclarecer a ordem econômica nacional é como iniciar um assunto abordando as consequências de algo sem mencionar as suas origens. Assim, faz-se necessário abordar aqui questões gerais sobre a ordem econômica.

2.1 A ORDEM ECONÔMICA BRASILEIRA

A ordem econômica brasileira é um complexo de normas que comandam o sistema econômico do Brasil. Trata-se, mais especificamente, do conjunto de normas positivadas ou não, que regulam o comportamento dos agentes econômicos - pessoas jurídicas ou físicas que, através de suas ações, contribuem para o pleno funcionamento do sistema econômico - famílias, empresas, mercado, Estado e o mundo. Cada um desses agentes econômicos possui uma importância específica na economia de um país, sendo alguns relevantes para a demanda e outros para a oferta (ULEN; COOTER, 2010).

A Constituição brasileira de 1988, em seu art. 170, disciplina que a ordem econômica tem por fundamentos a livre iniciativa e a valorização do trabalho humano. Isso significa dizer que cada cidadão brasileiro ou residente no país pode ingressar no mercado sem a prévia concordância do Estado: ou seja, se existe a chance de abrir uma empresa, vender um produto e negociar o preço que lhe for mais justo, isto se dá em função do princípio da livre iniciativa, portanto, pode-se fazê-lo (ULEN; COOTER, 2010).

O objetivo da ordem econômico, ainda com previsão no artigo supra, é a existência digna a todos e à justiça social. Para que o direito de gozar de uma existência digna e justa socialmente, seja para todos. Ninguém pode ser explorado economicamente e ao ponto de se privar de uma vida humana, socialmente falando:

A associação entre liberalismo econômico e justiça social forma as bases do verdadeiro Estado Social. Do ponto de vista de uma economia periférica, como a brasileira, esse modelo busca garantir que o desenvolvimento econômico esteja necessariamente associado à concretização dos direitos da pessoa humana (TAVARES; GAMA, 2022, p. 32).

Gama (2022) pontua que, destina-se a Constituição em seu título VII à introdução da chamada Ordem Econômica e Financeira, trazendo ainda, no capítulo I, os princípios constitucionais da atividade econômica: soberania nacional, propriedade privada, função social da propriedade, livre concorrência, defesa do consumidor e do meio ambiente, inclusive mediante tratamento diferenciado conforme o impacto ambiental dos produtos e serviços e de seus processos de elaboração e prestação, redução das desigualdades regionais e sociais, busca do pleno emprego e tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no país.

Esses seriam, então, os fundamentos, finalidades e princípios da ordem econômica. E é nessa seara que está inserido o Direito Econômico. Um ramo do Direito formado por normas jurídicas adstritas a regular a produção e a circulação de produtos e serviços, com vista ao desenvolvimento econômico do país, principalmente no tocante ao controle do mercado interno, à luta e disputa lá estabelecida entre as empresas, bem como aos acertos e arranjos feitos para explorarem o mercado (CARVALHOSA, 2013).

A economia de um país possui regras naturais que não podem sofrer abuso do poder estatal no que se refere ao seu modo de acontecer.

O Direito Econômico debruça-se sobre os limites de intervenção do Estado na economia de um país. Vale lembrar que, quando se menciona meios de intervenção do Estado na economia, consideram-se as privatizações, o fomento, as parcerias entre o setor Público e o Privado e a regulamentação.

Assim, o Estado estabelece políticas específicas - a exemplo da não taxação do IPVA de veículos automotores movidos a eletricidade em prol do incentivo à sustentabilidade; impede condutas – como formação de cartéis para atingir lucros arbitrários e concentração de renda -, estabelece formas de fiscalização, regulação e participação do Estado na atividade econômica; determina a divisão de competências tributárias dos entes federativos, por exemplo – que são fiscalizadas pelos órgãos competentes com base nos fundamentos do Direito Econômico dentre outros.

Ressalte-se que, somente na CF/88, o Direito Econômico foi nominal e positivamente incluído, em seu art. 24, inciso I, onde se aduz atribuições

concorrentemente à União, Estados e Distrito Federal para legislar sobre o assunto:

Assim sendo, a União é competente para o estabelecimento de normas gerais (art. 24, § 1º), cabendo aos Estados a competência suplementar em tais casos (art. 24, § 2º). Em não havendo normas gerais sobre determinado tema, os Estados exercerão competência legislativa plena sob suas peculiaridades (art. 24, § 3º), sendo a eficácia da lei estadual suspensa quando da superveniência de lei federal (art. 24, § 4º) (TOLEDO SILVEIRA, 1997).

Sobre suas origens:

Alguns autores consideram o Direito Econômico como surgido na década de vinte, quando, após a Primeira Guerra, as condições econômicas dos países e, conseqüentemente, de sua população estavam completamente desfavoráveis, chegando este desequilíbrio a culminar na famosa crise de 29. Alternativas foram-se criando para o contorno daquela instabilidade financeira e recessão por que se passava. Dentre elas surgiram as socializações, a reforma agrária, o controle de preços e de câmbios. Todas essas situações tratavam de questões econômicas, não tendo sido cabíveis em nenhum dos ramos do Direito vigente à época. Seu agrupamento, apesar de não codificado, teria originado o Direito Econômico (TOLEDO SILVEIRA, 1997).

O Direito Econômico também possui um agrupamento de normas reguladoras ou disciplinadoras construídas culturalmente de natureza jurídica a que se denominam de institutos:

Trata-se da reunião de diversas normas que lidem, abordem, disponham sobre fatos concretos, reais, empíricos, interrelacionados entre si e que possuam alguma relevância jurídica. Através deste agrupamento de normas, cria-se uma sistematização das mesmas, de forma a facilitar sua compreensão como características de determinado ramo do Direito. Assim como as regras de Direito Econômico, os institutos funcionam como importante mecanismo no qual o intérprete da lei pode-se pautar para a complementação e enriquecimento do conhecimento, de forma a se obter uma hermenêutica fundamentada (TOLEDO SILVEIRA, 1997).

Os institutos do Direito Econômico, podem ser assim compreendidos: intervenção, repartição, planejamento, produção, circulação e consumo. A intervenção citada em linhas anteriores, consiste em medidas que restringem uma iniciativa privada em determinada área econômica. No que tange a repartição, trata-se da criação de política econômicas instituídas com a finalidade de atribuir a cada componente da sociedade uma parcela da riqueza, quais sejam renda, salário, lucro, juros. Já o planejamento consiste na produção da minuta técnica até se chegar a Lei do Plano, onde o Estado define suas metas e forma para atingi-las. A produção, matéria-prima, trabalho, capital e organização. O Mercado, este se materializa na lei da oferta e da procura, moeda, crédito, preços. Por último o consumo, tema objeto

deste estudo.

Ainda existem as regras do Direito Econômico, que aqui se citam apenas para fins didáticos: equilíbrio, equivalência, recompensa, liberdade de ação, primazia da realidade social, interesse social, indexação, utilidade pública, oportunidade, razão, irreversibilidade e precaução.

Como princípios do Direito Econômico, e aqui não se confunde com os princípios da ordem econômica, tem-se: a Economicidade – quando o Estado foca suas políticas públicas de planejamento em atividades economicamente viáveis (art. 70; 3º, II; 170, caput e 174, caput, CF/88); a Subsidiariedade - Ao Estado só é permitido atuar na Economia subsidiariamente – esse princípio está relacionado à intervenção do Estado no domínio Econômico em sentido estrito (art. 173 da CF/88) (SOUZA, 1980).

Vale lembrar que, no princípio da economicidade:

Muitas vezes, a solução mais vantajosa para a situação não se trata daquela mais lucrativa em termos financeiros, capitalistas. Tudo dependerá da finalidade que se busca atingir. Se se almeja, por exemplo, o alcance da instalação telefônica em meios rurais de difícil acesso, apesar de ser uma obra extremamente dispendiosa e de pouco retorno financeiro, em se concretizando tal meta, o objetivo social terá sido realizado, embora não sejam auferidos lucros em matéria de rendas e sim de benefícios para a população (TOLEDO SILVEIRA, 1997).

Note-se ainda, uma:

[...] necessidade de flexibilidade das normas de Direito Econômico face às diversas circunstâncias com que este se depara, ao longo da trajetória econômica de um país. Um mesmo fato em contextos distintos pode levar a decisões inteiramente contrárias, sem a ocorrência de qualquer contradição. Trata-se de simples ajuste ao dispositivo constitucional adequado para situações individualizadas, realizado pelo instrumento harmonizador da economicidade. (...) Essa 'maior vantagem' há de ser adequada aos objetivos constitucionalmente definidos. Permite, destarte, a opção mais justa ou recomendável, em política econômica, a ser realizada pelo aplicador ou intérprete da norma, quando da realização concreta de situações hipoteticamente previstas. O ideal é que se consiga conciliar aquilo tomado como certo economicamente, com o considerado justo juridicamente. Em caso de incompatibilidade, deve prevalecer o justo. Afinal a 'linha de maior vantagem' é pautada em termos do 'valor justiça'. Restringe-se o arbítrio, o poder de decidir do aplicador, o qual se deve ater às disposições constitucionais e princípios hermenêuticos, preterindo-se qualquer subjetividade (TOLEDO SILVEIRA, 1997).

Observe-se a ponderação do princípio tomando-se como base, segundo Souza (1961), o fundamento e o objetivo da ordem econômica nacional vigente:

No caso brasileiro atual, a ideologia que se adotou com a Constituição Federal de 1988 foi a neoliberal, isto é, conciliaram-se ditames puramente liberais com outros socializantes. Se se considerar a Constituição Federal de 1891, notar-se-á, claramente, a ideologia estritamente liberal da mesma (TOLEDO SILVEIRA, 1997).

Passemos, portanto, aos princípios constitucionais da ordem econômica, constantes no art. 170 da CF/88. São nove os ditos princípios constitucionais: soberania nacional; propriedade privada; função social da propriedade; o já transcrito acima princípio da livre concorrência; defesa do consumidor; defesa do meio ambiente, redução das desigualdades regionais e sociais; busca de pleno emprego; e tratamento favorecido para as empresas de pequeno porte, constituída sob as leis brasileiras, que tenham sua sede e administração no país (GRAU, 2018). De todos eles, interessa a este estudo o princípio da defesa do consumidor.

Isso porque ele se imiscui aos princípios do Direito do Consumidor. Trata-se de um princípio promotor de uma existência digna à pessoa humana, e garantidor da justiça social. O princípio da defesa do consumidor é um demonstrativo de que a ordem econômica não pode ser concebida como um entrave à efetivação do estado de bem-estar social e digno do consumidor (MARQUES; MIRAGEM; BENJAMIM, 2021).

O Direito Constitucional Econômico é um conjunto de normas constitucionais que tratam da política econômica do Estado, elaborada a partir da ideologia adotada. Essa política econômica se apresenta na Constituição como temas econômicos, constituindo-se assim na conhecida Constituição Econômica (FERREIRA FILHO, 2022). Trata-se, basicamente, do assunto econômico se juridicizando em grau constitucional:

Em síntese, política econômica estatal é um conjunto de decisões públicas dirigidas a satisfazer as necessidades sociais e individuais, com um menor esforço, diante de um quadro de carência de meios. É, ainda, uma das espécies do gênero políticas públicas (CLARK, 2008).

Nesse sentido, é importante que se entenda que a Constituição Econômica precisa primar pelo desenvolvimento econômico do país (BERCOVICI, 2005). Dentre essas ações econômicas, pode-se citar a:

[...] compra e venda de moeda estrangeira; elevação ou redução dos

tributos; ampliação do volume da moeda nacional na economia; edição de normas legais de remessa de lucros ao exterior, de repressão ao poder econômico e de defesa do consumidor; emissão de títulos públicos no sistema financeiro que conseqüentemente influenciarão nos juros a serem pagos pelo Estado (CLARK, 2008).

A depender dessas ações econômicas do Estado, pode-se ter a:

[...] concessão de créditos subsidiados a setores econômicos; cessão de terras públicas ou redução de exigências burocráticas a fim incentivar o turismo; realização de obras governamentais em prol do crescimento modernizante; estatização ou nacionalização de atividades econômicas; criação de agências reguladoras produtoras de marcos legais para o mercado; abertura de empresas estatais fabricantes de bens e prestadoras de serviços, voltadas ao desenvolvimento sustentável (CLARK, 2008).

No conjunto dessas medidas em busca do desenvolvimento econômico do país, é preciso estar embutido o respeito ao consumidor, especialmente à privacidade de seus dados, por este ser um direito humano fundamental presente em nossa Constituição. É neste momento em que aparecem os princípios constitucionais econômicos: trata-se de princípios da Constituição que abordam questões da ordem econômica nacional. Entende-se aqui que eles devem estar imbrincados com o interesse de proteção à privacidade dos dados do consumidor, bem como com a dignidade da pessoa humana (MARQUES; BENJAMIM; MIRAGEM, 2021).

No caso do Brasil, defende-se aqui a importância de um direito constitucional econômico com viés de proteção à privacidade dos dados do consumidor. Acredita-se que isso é possível com o entrelaçamento do princípio da boa-fé objetiva ao princípio da ordem econômica do Estado.

2.1.1 O Princípio da Ordem Econômica da Defesa do Consumidor

A Constituição Federal de 1988, trata sobre a Defesa do Consumidor em dois dispositivos. No artigo 5º, inc. XXXII – onde diz que é responsabilidade do Estado promover, na forma da lei, a defesa do consumidor, e no art. 170, sobre a ordem econômica, no seu inciso V, a defesa do consumidor é um dos princípios a serem observados, a fim de se manter os fundamentos econômicos da valorização do trabalho humano e da livre iniciativa, buscando assegurar a todos existências dignas conforme os ditames da justiça.

O princípio constitucional da ordem econômica da defesa do consumidor, como nos ensina Eros Grau (2018, p. 245), tem dupla função, cumpre a ele assegurar a todos existência digna e ainda assume o caráter de diretriz, justificando a reivindicação pela realização de políticas públicas.

Sob a direção definida pelas ordens constitucionais contidas no princípio econômico constitucional em estudo, faz-se aqui a análise do desenrolar das relações de consumo nas últimas década na busca de identificar qual política pública se faz necessária a proteção dos dados pessoais dos consumidores em função de garantir o princípio em referência e suas diretrizes.

As relações de consumo nas últimas décadas vêm sofrendo grandes mudanças em função dos avanços tecnológicos, principalmente na área das telecomunicações.

Dentro desse contexto, alterações ocorreram no modo de produção dos bens de consumo, visando a atender um mercado consumidor hiper estimulado a buscar produtos considerados de rápida substituição. Esse fenômeno ocorre pela constante atualização das mercadorias, ou pela satisfação de se adquirir um produto novo a cada “estação”, instigado pelo marketing do consumismo veiculado massivamente pelos meios de comunicações digitais.

Essas transformações, podem ser também associadas à redução da produção em alta escala de bens padronizados, que ocorreu ao longo dos últimos trinta anos, em virtude da saturação dos mercados consumidores. Passou-se, nessa ocasião, a adotar novas estratégias comerciais, como é o caso da economia customizada ou flexível, que surgiu com a finalidade de atender o consumidor em suas expectativas mais individuais.

A partir dessas remodelações do mercado, os dados pessoais assumiram uma enorme importância. O armazenamento eletrônico das informações das pessoas em imensos arquivos potencializou essas movimentações nas relações de consumo.

Sendo assim, o consumo cresceu em número e em espécie. O mercado vem demonstrando, a cada dia mais, que o ganho assume, em muitos aspectos, a faceta do “lucro a qualquer custo”. De um lado está o consumidor, a mercê das manobras do mercado, e do outro, os empresários e investidores implacáveis, justificados

pelos conceitos da economia pautada no liberalismo.

Tem-se, portanto, uma relação de consumo onde o consumidor se caracteriza por ser a parte vulnerável, ou hipossuficiente, em matéria de força e decisão, como nunca antes visto.

Nesse contexto, o Direito assume o importante papel de impor limites, reprimindo os excessos, direcionando as práticas para o interesse da coletividade e, ao mesmo tempo, tutelando tanto as ações do comércio, da indústria, quanto as do consumidor, no sentido de garantir as partes envolvidas as suas prerrogativas, nas relações consumeristas.

Por conseguinte, as normas de defesa do consumidor ganharam destaque, pois reconhecem neste a parte vulnerável dentro das citadas relações de consumo. Sempre levando em conta que no âmbito da tutela especial do consumidor, considerando a sua vulnerabilidade, ele é sem dúvida a parte mais fraca, quando se observa que os possuidores dos meios de produção é quem detêm todo o controle do mercado, sobre o que produzir, como produzir e para quem produzir, sem falar-se na fixação de suas margens de lucro (GRINOVER; OLIVEIRA FILHO; BRAGA, 2022, p. 111).

Percebe-se que a defesa do consumidor é, antes de tudo, uma defesa da dignidade da pessoa humana. Sobre isso, Sarlet (1998) afirma que:

Inicialmente cumpre salientar que a dignidade, como qualidade intrínseca da pessoa humana, é algo que simplesmente existe, sendo irrenunciável e inalienável, na medida em que constitui elemento que qualifica o ser como tal e dele não pode ser destacado, de tal sorte que não se pode cogitar na possibilidade de determinada pessoa ser titular de uma pretensão a que lhe seja concedida a dignidade. (1998, p. 104)

Sendo o consumidor a parte mais frágil em uma relação de consumo, a sua dignidade igualmente é a sua parte mais vulnerável. Nas relações comerciais, a pessoa se torna um simples objeto necessário para o funcionamento da estrutura consumerista. É preciso se humanizar essa visão, atribuindo ao consumidor direitos da pessoa humana e tornando essas relações de consumo mais sociais e dignas. É preciso se conceber, antes de tudo, relações econômicas mais humanizadas.

2.1.1.1 Direito do Consumidor

Na legislação brasileira, a lei protetiva do consumidor estabelece que aquela, pessoa física ou jurídica, que adquire um produto ou serviço como destinatário final é considerado consumidor (art. 2º, caput, do CDC), a ele se equiparando qualquer pessoa, determinável ou não, exposta às práticas comerciais de oferta, publicidade e colocação de contratos de fornecimento de produtos e serviços no mercado (art. 29 do CDC). Por conta dessa equiparação, deve-se verificar quando se aplica a Lei nº 8.078, de 11.9.1990, na sociedade da informação, no meio virtual e fora dele (LISBOA, 2009).

Mendes (2014) afirma que se vive uma economia da informação desde os anos 70, na qual os dados constituem sua força motriz. Essa dinâmica manteve a máquina capitalista voraz em busca de perspectivas de lucro sempre mais elevadas, como se pode observar nos dias de hoje.

A história da defesa do consumidor no Brasil passa por momentos importantes a partir de 1970, quando surgiram os primeiros órgãos de defesa do consumidor; em 1976, foram fundadas a Associação de Proteção ao Consumidor de Porto Alegre (APC), a Associação de Defesa e Orientação do Consumidor de Curitiba (ADOC) e o Grupo Executivo de Proteção ao Consumidor (atual Fundação PROCON São Paulo); no ano de 1985 foi criado o Conselho nacional de defesa do consumidor, para assessorar o presidente da república na elaboração das políticas nacionais de defesa do consumidor; em maio de 2012, foi criada a Secretaria Nacional do Consumidor – SENACON -, vinculada ao ministério da justiça nacional, e o Departamento de Proteção e Defesa do Consumidor – DPDC -, órgão de suporte e subordinação da SENACON (SAYEG, 2004).

A SENACON tem a responsabilidade de representar internacionalmente a proteção do consumidor brasileira, cabendo à esta Secretaria participar de comissões, fóruns e comitês nacionais e internacionais (SAYEG, 2004).

Em 1985 a Organização das Nações Unidas (ONU) estabeleceu em sua 106ª Sessão Plenária a Resolução nº 39/248 “o princípio da vulnerabilidade do consumidor”, reconhecendo-o como a parte mais fraca na relação de consumo, e tornando-o merecedor de tutela jurídica específica.

A vulnerabilidade do consumidor reconhecida pela ONU, tornou-se uma garantia fundamental decorrente da dignidade da pessoa humana. Este direito

fundamental está exposto no art. 1º, IV da CF/88. Assim, violar direito do consumidor significa violar um princípio fundamental. (MARQUES; BENJAMIM; MIRAGEM, 2021).

No que diz respeito ao Código de Defesa do Consumidor (Lei nº 8.078/90), este é formado por um microssistema vinculado às ordens constitucionais. Há de se distinguir, portanto, o sistema político do sistema normativo de defesa do consumidor. O SNDC – Secretaria Nacional de Direito Econômico, representa a face do sistema político, enquanto o sistema normativo decorre da própria lei. Pode-se dizer que o CDC é uma lei principiológica, enquanto encerra em si princípios gerais cujo objetivo primeiro é o de abranger todas as situações envolvendo o consumo, sem especificar cada caso. Sendo, assim, um sistema de cláusulas abertas, dando margem para a interpretação do julgador quando o assunto da ação proposta fizer parte das relações de consumo (SANTOS, 2020).

Sendo assim, o Código de Defesa do Consumidor parece abranger e regular as relações do mundo virtual, disciplinando os contratos feitos em transações online, mas, contudo, através de um olhar mais atento é possível verificar que essas relações não são tão simples.

Pode-se afirmar que o CDC, é capaz de resolver, legitimar a grande maioria dos contratos realizados pela via virtual, contudo este mesmo código não prevê, até agora, meios para dirimir a assinatura de instrumentos contratuais com graves falhas de segurança, vazamento de informações, e não tem mecanismos, ainda, para aperfeiçoar os contratos.

Ao entender-se que, há um aumento significativo do uso da internet em contratações virtuais, e esse número está em elevação, entende-se que é necessária uma atualização do CDC para que seja possível a previsão de situações que possam levar a uma lesão ao consumidor (SANTOS, 2020)

O Código de Defesa do Consumidor, promulgado na década de 1990, ainda que seja um microssistema de proteção e que seja aplicado de forma análoga ao *e-commerce*, tem sido insuficiente para mitigar o impacto da globalização, principalmente diante de fragmentação e heterogeneidade da sociedade da informação

É necessário esclarecer que “o contrato de consumo eletrônico internacional

rege-se pelas cláusulas propostas pelo fornecedor estrangeiro, às quais adere o consumidor brasileiro” (COELHO, 2009, p.43), assim, não comporta a aplicação do CDC, conforme indicado no artigo 9º, §2º da LICC (BRASIL, 1942). Nota-se, que se tem utilizado, para se conquistar a credibilidade junto aos consumidores virtuais, alguns códigos de condutas provenientes das boas práticas comerciais virtuais. Essa certificação, é expressa por meio de logotipos ou marcas identificativas, dando possibilidades de garantias aos consumidores virtuais, que farão suas compras com uma maior segurança junto aos "estabelecimentos virtuais" identificados na rede mundial.

O “mercado virtual”, nesse caso, tende a se autorregular, tendo em vista que a propaganda negativa é rápida, de uma empresa que não agiu corretamente com seus clientes.

Diante, desse exemplo citado, pode-se dizer que aumenta a importância do princípio da boa-fé objetiva a essas relações econômicas, tema que será abordado no item 2.1, deste estudo.

Antes, porém, importante conferir as jurisprudências de alguns Tribunais de Justiça brasileiros.

1.2.2.1 Jurisprudências dos Tribunais de Justiça

Pertinente destacar neste estudo alguns exemplos de jurisprudências, coletados através de pesquisas realizadas em três dos maiores Tribunais de Justiça do país, TJ de São Paulo, TJ Rio Grande do Sul e TJ de Minas Gerais.

Fez-se um apanhado de julgamentos sobre vazamentos de dados dos consumidores, para se chegar a uma ideia, mesmo sendo representativa de uma pequena amostra, do posicionamento do poder judiciário sobre o tema.

No Tribunal de Justiça de São Paulo, três decisões abordam as seguintes temáticas: fraude por meio de invasão aos dados em aparelho de celular; empréstimo fraudulento realizado por terceiro que se passa por gerente do banco; e o golpe do motoboy – violação de dados do consumidor que viabilizam a fraude.

APELAÇÃO. CONSUMIDOR. PRESTAÇÃO DE SERVIÇOS. AÇÃO DE INDENIZAÇÃO POR DANOS MATERIAIS E MORAIS. TELEFONIA CELULAR. PRELIMINAR DE ILEGITIMIDADE PASSIVA DA OPERADORA

DE TELEFONIA REJEITADA. TEORIA DA ASSERÇÃO¹¹. FRAUDE. GOLPE DO "SIM SWAP".

Fraudador que teve acesso aos dados pessoais, contatos e aplicativos do celular da autora vinculados à linha telefônica. Culpa exclusiva de terceiro não verificada. Clonagem de linha telefônica móvel. Cabia à ré provar a existência de fato impeditivo, modificativo ou extintivo do direito da autora (art. 373, II, do CPC). Ausência de segurança no sistema da ré. (...) Danos Morais caracterizados. Situação que ultrapassa a esfera do mero aborrecimento. Indenização arbitrada em R\$ 5.000,00, valor justo

(TJSP; Apelação Cível **1035797-48.2022.8.26.0002**; Relator (a): Deborah Ciocci; Órgão Julgador: 28ª Câmara de Direito Privado; Foro Regional II - Santo Amaro - 15ª Vara Cível; Data do Julgamento: 15/08/2023; Data de Registro: 21/08/2023) (grifei)

APELAÇÃO - AÇÃO DE OBRIGAÇÃO DE FAZER C/C INDENIZAÇÃO POR DANOS MORAIS. FRAUDE BANCÁRIA. EMPRÉSTIMOS EFETUADOS DE MODO FRAUDULENTO POR TERCEIROS SE PASSANDO POR FUNCIONÁRIOS DO BANCO. MOVIMENTAÇÕES ATÍPICAS DO PERFIL DA CLIENTE. VALORES TRANSFERIDOS PARA TITULARES DESCONHECIDOS EM CURTO ESPAÇO DE TEMPO. PRETENSÃO DA AUTORA DE CANCELAMENTO DO CONTRATO E CONDENAÇÃO DO RÉU AO PAGAMENTO DE INDENIZAÇÃO POR DANOS MORAIS. SENTENÇA DE PARCIAL PROCEDÊNCIA. PRETENSÃO DA AUTORA DE REFORMA.

INADMISSIBILIDADE: Elementos dos autos que demonstram a existência de falha na prestação dos serviços, uma vez que o Banco permitiu transações que fogem do perfil da cliente. Também houve provável vazamento de informações sigilosas a respeito da conta corrente da autora, que eram de conhecimento dos fraudadores, denotando descuido e má prestação de serviço. Dever de cancelamento do contrato que se impõe. A inexistência dos débitos referentes ao contrato nº 000804438681 já foi reconhecida na r. sentença e contra ela não há recurso do Banco réu. Ademais, o conjunto probatório não demonstrou o dano moral. Não há prova de que a apelante tenha sofrido qualquer dor moral ou grande aborrecimento ou abalo em sua imagem. Sentença mantida. RECURSO DESPROVIDO.

(TJSP; Apelação Cível 1002850-84.2022.8.26.0019; Relator (a): Ernani Desco Filho; Órgão Julgador: 18ª Câmara de Direito Privado; Foro de Americana - 4ª Vara Cível; Data do Julgamento: 18/08/2023; Data de Registro: 18/08/2023) (grifei)

AÇÃO DE INDENIZAÇÃO. SENTENÇA DE PROCEDÊNCIA. APELAÇÃO DO BANCO RÉU IMPROVIDA. CONSUMIDOR. PRESTAÇÃO DE SERVIÇOS BANCÁRIOS. FRAUDE. GOLPE DO MOTOBOY. VIOLAÇÃO DE DADOS DO CONSUMIDOR QUE VIABILIZOU O GOLPE. RESPONSABILIDADE OBJETIVA. APLICAÇÃO DA SÚMULA 479 DO STJ. FALHA NO SETOR DE FRAUDE DA INSTITUIÇÃO FINANCEIRA. AUSÊNCIA DE CULPA EXCLUSIVA DO CONSUMIDOR. DANOS MORAIS. RECONHECIMENTO.

Ação declaratória cumulada com pedido de indenização. Sentença de

¹¹ A teoria da asserção defende que as questões relacionadas às condições da ação, como a legitimidade passiva, são aferidas à luz do que o autor afirma na petição inicial, adstritas ao exame da possibilidade, em tese, da existência do vínculo jurídico-obrigacional entre as partes, e não do direito provado Disponível em: <https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/jurisprudencia-em-detahes/condicoes-da-acao/teoria-da-assercao-2013-condicoes-da-acao#:~:text=A%20teoria%20da%20asser%C3%A7%C3%A3o%20defende,2..> Acessado em 20 de agosto, 2023

procedência. Recurso do banco réu. Primeiro, reconheço a falha na prestação dos serviços pelo réu. Golpe do motoboy. Falha do serviço bancário. Vazamento de dados como nexos causal determinante para sucesso da fraude. Além disso, o perfil das compras mostrou-se manifestamente suspeito: foram realizados dois "pix" em favor de terceiro, ambos no valor de R\$ 800,00, duas transferências bancárias de R\$ 1.200,00 cada e um empréstimo de R\$ 1.512,00 – ou seja, completamente fora do padrão de gastos da autora e altamente questionável. Falha no serviço de segurança reconhecida. Fortuito interno caracterizado. Súmula 479 do STJ. Responsabilidade do réu pelo fato do serviço. Inexigibilidade dos débitos. Restituição dos valores oriundos das transações impugnadas. Retorno das partes ao estado anterior. E segundo, mantenho a reparação dos danos morais. A consumidora idosa experimentou dissabores, transtornos e aborrecimentos advindos não somente da falta de segurança do sistema bancário, mas também do atendimento inadequado recebido. Mesmo em Juízo, o banco réu insistiu numa versão (sem qualquer indício) da participação no evento danoso. Indenização dos danos morais mantida no patamar de R\$ 5.000,00 (cinco mil reais), parâmetro este ajustado para singularidades do caso concreto, razoável e admitido por esta Turma julgadora em casos semelhantes. Ação parcialmente procedente. SENTENÇA MANTIDA. RECURSO DO RÉU IMPROVIDO. (TJSP; Apelação Cível 1005647-05.2021.8.26.0266; Relator (a): Alexandre David Malfatti; Órgão Julgador: 12ª Câmara de Direito Privado; Foro de Itanhaém - 3ª Vara; Data do Julgamento: 17/08/2023; Data de Registro: 17/08/2023) (grifei)

Observe-se que nos casos julgados as decisões, favoráveis aos consumidores, foram fundamentadas nas fragilidades da segurança aplicadas ao sistema de armazenamento de dados dos respectivos recorridos, nos recursos acima.

No Tribunal de Justiça do Rio Grande do Sul, buscou-se outras situações para aumentar o leque de análise. Os temas trazidos foram: contrato formulado virtualmente, com dados de biometria fácil – considerado frágil o meio de contratação; e, débito atribuído ao cartão de crédito - contratação e prova do consumo não demonstrados.

RECURSOS INOMINADOS. DECLARATÓRIA DE NULIDADE DE NEGÓCIO JURÍDICO BANCÁRIO C/C REPETIÇÃO DE INDÉBITO E REPARAÇÃO DE DANOS MORAIS. EMPRÉSTIMO CONSIGNADO PARA APOSENTADOS. NEGATIVA DA VONTADE DE CONTRATAR, PELO CONSUMIDOR. CONTRATO FORMALIZADO VIRTUALMENTE, COM DADOS DE BIOMETRIA FACIAL E CÓPIA DE DOCUMENTO PESSOAL. FRAGILIDADE DO MEIO DE CONTRATAÇÃO, PORQUANTO NÃO COMPROVA A MANIFESTAÇÃO DA VONTADE DE ADERIR AO CONTRATO.

Exposição das informações dos consumidores, através de vazamento massivo de dados, deflagra a fragilidade do meio virtual de contratação. Necessidade de juntada da gravação do contato prévio entre as partes. Desatendimento ao disposto no art. 373, II, do CPC.

Cancelamento do contrato. Repetição dobrada do indébito, pelo réu, e devolução do valor do empréstimo, pela parte autora. Admitida a compensação dos créditos. Multa cominatória arbitrada em valor e periodicidade desconformes aos critérios desta quarta turma. Alteração da sentença apenas nesse aspecto. Danos morais. Ausente prova de ofensa aos atributos da personalidade. Danos não presumidos. Recurso do réu provido em parte. Desprovido o recurso da autora. (grifei)

RECURSO INOMINADO. AÇÃO DE INEXIGIBILIDADE DE DÉBITO C/C INDENIAÇÃO POR DANOS MORAIS. CONSUMIDOR.

Cartão de Crédito. Inscrição nos Cadastros de Inadimplentes. Negócio Jurídico não reconhecido pela autora. Origem da Dívida, Contratação e Prova do consumo não demonstrados pelo réu. Ausentes provas indiciárias da regularidade da avença. Fragilidade dos meios de formalização dos contratos, notadamente após os mega vazamentos de dados pessoais havidos no país. Pedidos procedentes. Reforma da sentença, unicamente, para reduzir o valor da condenação por danos morais para r\$4.000,00. Atualização pela taxa SELIC. Recurso provido em parte. (Recurso Inominado, Nº 50028883020228211001, Quarta Turma Recursal Cível, Turmas Recursais, Relator: Jerson Moacir Gubert, Julgado em: 19-04-2023, j. 19/04/23) (grifei)

Interessante observar nos julgamentos do TJRS, as situações de risco a privacidade dos dados dos consumidores, ambas decisões foram fundamentadas na fragilidade do meio de formalização do contrato, levando-se em conta o grande vazamento de dados ocorrido a época.

Já no Tribunal de Justiça de Minas Gerais, apesar de envolver instituição financeira, a fraude acontece de uma forma diferente, refere-se ao golpe do boleto falso, que se materializou em virtude de vazamento de dados do consumidor;

EMENTA: APELAÇÃO CÍVEL. PRELIMINAR DE AUSÊNCIA DE DIALETICIDADE. REJEIÇÃO. PRELIMINARES DE ILEGITIMIDADE PASSIVA E DENUNCIAÇÃO DA LIDE. REJEIÇÃO. AÇÃO DECLARATÓRIA. CONTRATO DE FINANCIAMENTO COM CLÁUSULA DE ALIENAÇÃO FIDUCIÁRIA. GOLPE DO BOLETO FALSO. FALHA NA PRESTAÇÃO DE SERVIÇOS. RESPONSABILIDADE OBJETIVA DA INSTITUIÇÃO FINANCEIRA. SÚMULA 479 DO STJ. RECONHECIMENTO DO PAGAMENTO E AMORTIZAÇÃO DO DÉBITO. POSSIBILIDADE. RECURSO IMPROVIDO. SENTENÇA MANTIDA.

- Não viola o princípio da dialeticidade o recurso que impugna, de modo conciso, os fundamentos da sentença.
- O Código de Defesa do Consumidor é aplicável aos contratos bancários.
- Nos termos do art. 14 do CDC, 'o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos'.
- Segundo a Súmula 479 do STJ, "as instituições financeiras

respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

[...]

- Verificada a ocorrência de falha na prestação do serviço, que culminou no pagamento de boleto fraudulento por meio de vazamento de dados do consumidor, imperioso o reconhecimento do pagamento efetuado com a amortização do débito.

Apelação Cível, 5001827-62.2021.8.13.0106, Relator(a): Des.(a) José Marcos Vieira, j. 09/08/2023 . (grifei)

Analisando as jurisprudências citadas, percebe-se que o problema dos vazamentos de dados, ocorre de maneira importante e se torna um grande risco ao consumidor na medida em que os sistemas digitais de armazenamento dessas informações não apresentam a segurança necessária a garantia dos direitos desse ator econômico, vulnerável, mas de fundamental importância para uma economia equilibrada e justa.

Nesse contexto, passa-se a seguir a análise do Princípio do Direito do Consumidor da boa-fé objetiva.

2.1.1 O Princípio do Direito do Consumidor da boa-fé objetiva

A instituição do princípio da boa-fé objetiva ocorreu com a promulgação do Código de Defesa do Consumidor, em seu artigo 4º, inciso III, fundamentado em raciocínio de interpretação, e 'no art. 51, inciso IV, como cláusula geral. Trata-se de um princípio essencial do direito do consumidor, a partir do qual as partes possuem o dever de agir baseadas em valores éticos e morais da sociedade. Desses preceitos, surgem outros deveres anexos, como lealdade, transparência e colaboração, a serem observados em todas as fases do contrato.

Analisando aqui, o diálogo entre fontes, destaca-se que no art. 6º da LGPD, tem-se a obrigatoriedade do uso do princípio da boa-fé, além de outros que contribuem para uma maior efetivação deste instituto, quais sejam: finalidade: realização do tratamento dos dados para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018)

Capiberibe (2012, p. 119) bem distingue o princípio da boa-fé objetiva do princípio da boa-fé subjetiva:

[...] neste é necessário fazer uma análise da percepção individual do agente cuja conduta está sendo analisada, visando a verificar se este acreditava que tal agir era correto, mesmo que esse não seja o padrão de conduta normal do homem médio naquela situação. Já a boa-fé objetiva estipula regras de conduta que prescrevem um comportamento fundado na lealdade, a ser observado por todos, que devem considerar as expectativas geradas por terceiros. (...) Tais regras atuam como verdadeiros paradigmas de condutas objetivas, as quais são traçadas tendo como parâmetro a figura do homem médio. Exige-se, assim, que as partes se portem de forma plausível, com a devida prudência, alinhando sua conduta a comportamentos de cuidados suficientes e razoáveis.

Nota-se que o princípio da boa-fé, se aplicado nas relações de consumo no tocante ao tratamento de dados pessoais dos consumidores, pode resolver grande parte dos problemas no que concerne ao resguardo da privacidade desses dados. Seria necessária uma política de *compliance* muito consistente nas empresas, que

visassem esse fim.

O termo *compliance* se origina do verbo em inglês *to comply*, que significa "cumprir". Trata-se de cumprir e se fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição, bem como evitar, detectar e tratar quaisquer desvios ou inconformidades que possam vir a ocorrer (MANZI, 2008, p. 26). É um verdadeiro trabalho de prevenção do ilícito, inserindo-se princípios e valores morais e éticos às ações tomadas. Por isso, GÓIS (2013, p. 100) a define como sendo:

[...] uma política regulatória anticorrupção para o setor privado em suas relações com o Estado, concebendo um conjunto de procedimentos de fiscalização, ética corporativa e auditoria para as empresas enquanto setor econômico privado.

Manzi (2008, p. 27) explica que o *compliance* teve origem nas instituições financeiras, com a criação do Banco Central Americano, em 1913, que objetivou a formação de um sistema financeiro mais flexível, seguro e estável. Logo após a quebra da Bolsa de Nova York de 1929, foi criada a Política Intervencionista New Deal, em uma tentativa de intervir na economia para corrigir as distorções naturais do capitalismo. Em 1977, foi promulgada a lei anticorrupção transnacional norte-americana: as empresas passariam a manter livros e registros que descrevessem, de maneira detalhada, as suas transações e a estabelecer um sistema adequado de controles internos.

Para Santos (2011, p. 85):

[...] discutir compliance é compreender a natureza e a dinâmica da corrupção e da fraude nas organizações, independentemente de seu ramo de atividade. Entretanto, para as organizações que possuem suas atividades controladas por órgãos reguladores do poder público, por se tratarem de atividades de prestação de serviço ao público, como, por exemplo, instituições financeiras, distribuidoras de energia, comunicação, aviação, entre outras, há uma série de exigências legais que devem cumprir, sob pena de até mesmo serem impedidas de exercerem suas atividades, sofrerem danos à sua imagem ou ainda sanções às organizações. Prevenção e combate à corrupção no Brasil 185 e aos indivíduos (podendo gerar processos administrativos ou até mesmo criminais).

Assim, em 2013, o Brasil promulga a Lei Anticorrupção para o setor privado (Lei Nº 12.846), estabelecendo a necessidade de *compliance*. A norma busca responsabilizar as pessoas jurídicas pela prática de atos lesivos à administração

pública. A idoneidade moral e ética necessária ao *compliance* estão estreitamente ligados à probidade exigida pelo princípio da boa-fé objetiva nas relações de consumo, sobretudo quando do tratamento com os dados pessoais dos consumidores.

O mundo contemporâneo dominado pelas novas tecnologias está dotado de sistemas avançados como a inteligência artificial, a robótica avançada, a internet das coisas, a computação em nuvem, o *Big Data*, a manufatura digital, a integração de sistemas, os sistemas de simulação e a digitalização. Estas estão mudando as formas de produção e os modelos de negócios no Brasil e no mundo (SCHWAB, 2016).

Este é o momento de, para fins de contextualização deste estudo, abordar-se o *big data*, que se relaciona com os dados pessoais dos consumidores.

2.2 BIG DATA

Na perspectiva social, percebe-se que as novas tecnologias, com a coleta de dados pessoais, vêm transformando profundamente as relações do mercado, uma vez que os indivíduos têm acesso ao mundo virtual com maior rapidez e menor custo, o que foi ampliado com a internet 5G. Um novo produto de enorme valor surgiu no mundo: os dados pessoais das pessoas. O mercado se transforma de maneira a criar necessidades para as pessoas. A nova necessidade agora são os dados.

Big data, na tradução de forma literal, significa grande quantidade de dados. Esse termo, no contexto digital, quer dizer um enorme banco de dados. Trata-se de um espaço virtual onde se armazena informações, em formato eletrônico, alimentado e acessado ininterruptamente, com a finalidade de abastecer as diversas atividades desempenhadas na sociedade, por entes públicos ou privados; são conteúdos úteis, com possibilidade de serem combinados, avaliados e tratados, ou seja, utilizados para fins particulares, coletivos, econômicos, governamentais e até mesmo para ilicitudes de grupos criminosos organizados (RODRIGUES MACHADO, 2018).

Big Data indica um grande volume de dados, capazes de impactar significativamente o dia a dia das empresas. Esse conceito não se limita à

questão da quantidade, mas também à quantidade de dados e, principalmente, o que as empresas fazem com ele (RODRIGUES MACHADO, 2018, p. 23).

Importante destacar, a princípio, algumas condições favoráveis que propiciaram o nascimento do extraordinário volume de dados em ambiente digital, como explica MACHADO (2018, p. 25):

A era do Big Data só se materializou com a confluência de alguns fatores. Caiu o custo de armazenar dados. Há duas décadas, estocar 1 gigabyte saía por 1000 dólares. Hoje, custa 6 centavos. Os processadores tornaram-se velozes, os programas ficaram mais inteligentes e a quantidade de dados cresce exponencialmente. Tudo isso junto é o berço do Big Data.

O Big Data, portanto, é um banco de dados de tráfico intenso, situado na internet, onde se encontram diversos tipos de informações, pessoais sensíveis, governamentais ou públicas; sigilosas; comerciais e diversas outras.

Esse universo imenso de informações, está dividido em duas formas de armazenamento: dados estruturados e dados não estruturados. Os dados estruturados são aqueles submetidos a um controle, são conferidos, organizados e filtrados. Já os dados não estruturados, a maior parte do acervo, são considerados lixo eletrônico. Tais informações, ao serem analisadas, proporcionam correlações de opiniões, preferências, padrões de comportamento, revelando aspectos importantes para se identificar com segurança grupo de consumidores, carências de produtos no mercado, dados de interesse público, perfis relacionados à saúde da população em geral, bem como de uma determinada área ou faixa etária (MACHADO, 2018).

O tratamento ou manipulação desses dados revelaram que eles têm um alto valor econômico, haja vista a sociedade humana, de forma global, estar inserida na era da informação digital com um horizonte de grandes e rápidas transformações, num patamar nunca imaginado. Em matéria de controle da comercialização dos dados, a normatização é ferramenta necessária para o equilíbrio do uso dessas tecnologias, no que tange a não ferir à privacidade das pessoas (RODRIGUES MACHADO, 2018).

Um dos pontos de maior vulnerabilidade no cruzamento e comercialização de dados na internet consiste na exposição pública sem autorização, bem como na venda de dados pessoais dos usuários da rede. Como foi dito anteriormente, *no Big Data* nem todos os dados são controlados; sendo assim, o risco de exposição e

comercialização de dados pessoais sensíveis é muito grande. A exposição da vida privada do indivíduo pode causar-lhe diversas consequências, seja no âmbito pessoal, psicológico, econômico, profissional, ou no campo social, como as discriminações, o isolamento de atividades em grupo, dentre outras formas de ofensas coletivas (MACHADO, 2018).

Já se abordou aqui alguns casos de vazamento de dados ocorridos mundialmente. A legislação brasileira hoje está mais severa, com o surgimento da Lei Geral de Proteção de Dados – LGPD, da qual se trata adiante.

2.3 LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

A LGPD, Lei 13.709 de 2018, Lei Geral de Proteção de Dados, tem sua estrutura apoiada na tríade da Confidencialidade, Integridade e Disponibilidade. Isso significa que um dado seguro só o será de fato, se ele estiver acessível somente a quem efetivamente deva tê-lo, que esse mesmo dado não seja vulnerável a qualquer tipo de corrupção, ou seja edição indesejada, exclusão, manipulação, e esteja sempre disponível para que se possa utilizá-lo.

Nesta seção, será descrito seus preceitos referentes a questões relacionadas as especificidades da proteção dos dados das pessoas.

Assim, em seu art. 2º, tem-se, inicialmente, a apresentação dos fundamentos da proteção de dados pessoais como sendo

- I - o respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O art. 3º inclusive, reforça que a LGPD deve ser uma lei aplicada “a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado”, onde quer que estejam os dados. Ou seja: é obrigatória a sua utilização quando o assunto for dados pessoais, caso se queiram manipular os

dados das pessoas lícitamente. Hoje em dia, todas as empresas e órgãos públicos são obrigados a se adequarem à LGPD.

Excluem-se da lei apenas o tratamento de dados pessoais relativos à pessoa natural para fins exclusivamente particulares e não econômicos, fins exclusivamente jornalístico, artísticos ou acadêmicos, fins exclusivos de segurança pública, defesa nacional ou atividades de investigação e repressão de infrações penais, ou mesmo provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, conforme previsto em seu art. 4º.

A Lei ainda, define conceitos fundamentais, no art. 5º, como dado pessoal, banco de dados e tratamento de dados.

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

(...)

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (...)

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O importante tema sobre a boa-fé e princípios vem descrito, no art. 6º da Lei, como citado em item anterior.

O art. 7º da referida lei ainda é taxativa ao elencar as hipóteses em que os dados das pessoas podem ser manipulados. Apenas em casos de fornecimento de consentimento pelo titular, cumprimento de obrigação legal ou regulatória pelo controlador, 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, para a realização de estudos por órgão de pesquisa, execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados, para o exercício regular de direitos em processo judicial, administrativo ou arbitral, proteção da vida ou da incolumidade física do titular ou de terceiro, tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária, 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 para a proteção do crédito.

Em seu art. 8º, a LGPD aduz que “o consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular”.

E, no art. 9º, a LGPD prevê que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, e estes deverão ser disponibilizados de forma clara, apresentando seus direitos, com toda uma descrição de quem as produziu, seus fins, a forma e duração do tratamento, observados os segredos comercial e industrial, informações acerca do uso compartilhado de dados pelo controlador e responsabilidades dos agentes que realizarão o tratamento. Nota-se uma necessidade de clareza de todas as informações para o titular dos dados, a fim de que este sinta segurança na forma de manipulação dos seus dados. E tenha notícias detalhadas de toda a movimentação que acontece com eles.

A LGPD é expressa, em seu art. 10, ao aduzir que o controlador não tem o poder de tratar os dados do titular da maneira que quiser e quando quiser, muito menos para fins quaisquer. Ele deve fundamentar o tratamento dos dados pessoais para os fins de apoio e promoção de suas atividades, e proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

Quanto ao tratamento dos dados, há uma seção especial para o procedimento. O art. 11 asseve que apenas pode haver esse tratamento quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas. Se não houver esse consentimento, deverá haver o cumprimento de obrigação legal ou regulatória pelo controlador, o tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis, o exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, a proteção da vida ou da incolumidade

física do titular ou de terceiro, a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou a garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

E esse tratamento não é *ad infinitum*: ele tem um fim temporal que ocorrerá dentro das seguintes hipóteses, segundo o art. 15 da Lei: quando da verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada, quando do pedido do titular, ou por determinação da autoridade nacional. E os dados manipulados deverão ser eliminados do alcance de terceiros. Só haverá a sua conservação para as seguintes finalidades: cumprimento de obrigação legal ou regulatória pelo controlador, estudo por órgão de pesquisa, transferência a terceiro ou uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Isso está previsto no art. 16 da LGPD.

O tratamento dos dados pessoais pelo poder público requer uma seção especial. O art. 23 aduz que o tratamento desses dados 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. Vale notar que, mesmo assim, devem ser respeitados os seguintes limites:

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;

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei;

Isso é importante porque retira o poder pleno do poder público de manipulação dos dados dos cidadãos, mesmo porque as pessoas são obrigadas a fornecer os dados pessoais para os órgãos públicos em muitas das atividades de seu dia a dia. Nada mais justo que esse poder de tratamento dos dados pessoais seja limitado pelo órgão público. Isso também vale para as empresas públicas e as sociedades de economia mista que atuam em regime de concorrência: terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares.

Vale lembrar também que todos esses dados pessoais dos cidadãos deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. Não pode haver armazenamento que bloqueie ou dificulte a execução dessas atividades públicas, como previsto no art. 25 da Lei. E o art. 26 garante o direito à proteção desses dados usados para esses fins.

Sobre a comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado, o art. 27 explica que “será informado à autoridade nacional e dependerá de consentimento do titular, exceto”:

- I - nas hipóteses de dispensa de consentimento previstas nesta Lei;
 - II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
 - III - nas exceções constantes do § 1º do art. 26 desta Lei.
- Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação.

Vale mencionar que, no art. 29, “a autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei”. O art. 30 ainda deixa para a autoridade nacional a competência de poder “estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais”.

É clarividente a preocupação do legislador, quando da elaboração dessa lei, com a preservação da privacidade dos dados pessoais dos titulares. O consumidor se apresenta novamente como uma figura hipossuficiente nesse processo de manipulação de dados. Isso porque ele não tem informações necessárias sobre se realmente os dados utilizados foram eliminados do sistema após o seu tratamento. Um exemplo disso é que, ao se fazer uma pesquisa no *google*, sobre um produto, automaticamente o consumidor passará a receber anúncios desse mesmo produto em outras redes sociais desvinculadas do *google*. Ou seja: quem permitiu isso ocorrer? Como essa permuta ocorreu? Quais dados foram repassados para as demais redes sociais? São muitas as dúvidas que pairam nesse momento.

2.4 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD

A Autoridade Nacional de Proteção de Dados, foi criada pela LGPD n. 13.709/2018, regulamentada pelo Decreto 10.747/2020, é dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal.

A ANPD, possui hoje a natureza jurídica de autarquia em regime especial, vinculada ao Ministério da Justiça e Segurança Pública, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade, além do livre desenvolvimento da personalidade da pessoa natural, segundo as disposições previstas na legislação de proteção de dados.

Dentre suas atribuições estão: zelar pela proteção de dados pessoais; elaborar diretrizes para a Política Nacional de Proteção de Dados e da Privacidade; orientar os agentes em relação à aplicação de normas e regulamentos relativos à proteção de dados; cooperar com órgãos nacionais e internacionais responsáveis pelo tratamento de dados.

Detalhamento da estrutura interna da ANPD:

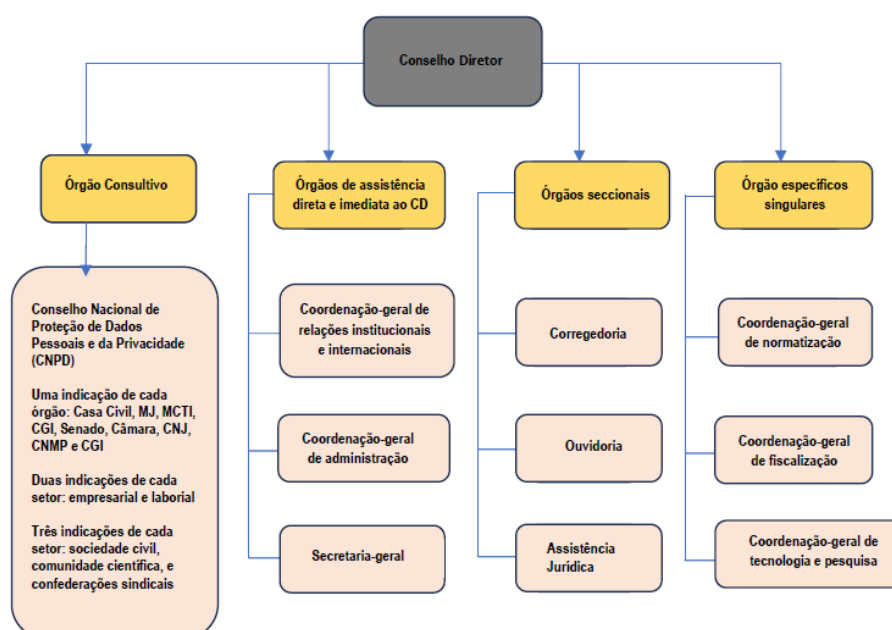


Figura 1 : Estrutura Organizacional da ANPD

Fonte: Mestranda

A fiscalização e a regulação da LGPD estão a cargo da Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Trata-se de uma tarefa essencial para que a autoridade nacional atue como um órgão a serviço do cidadão. A ANPD ainda se apresenta como um elo entre sociedade e governo, permitindo que as pessoas enviem dúvidas, sugestões e denúncias ligadas à LGPD para apuração:

Tem também um importante papel de orientadora e de apoiadora dos órgãos de governo e empresas em relação às situações em que elas podem ou não tratar dados pessoais do cidadão. A proposta da ANPD é orientar, orientar e orientar, preventivamente. Após isso, fiscalizar, advertir e, somente após tudo isso, penalizar, se a LGPD continuar sendo descumprida (SERPRO, 2023).

O processo de fiscalização das leis é tarefa não só dos órgãos públicos, mas principalmente da população. É importante a difusão dos direitos dos cidadãos pela comunidade jurídica sobretudo, a fim de que se construa uma sociedade cada vez mais consciente de seus direitos e deveres. Só assim se poderá exigir mais do poder judiciário no tocante ao cumprimento das leis, e mais de nossos representantes políticos no que se refere à produção e execução fiel das leis.

A ANPD aplicou agora em julho de 2023 a primeira sanção por indícios de infração à Lei Geral de Proteção de Dados Pessoais (LGPD). Uma microempresa de telecomunicações recebeu advertência e multa total de R\$ 14,4 mil. A advertência, sem imposição de medidas corretivas, deu-se por falta de indicação do encarregado pelo tratamento de dados pessoais. Já a multa foi aplicada por descumprimento dos deveres relativos à fiscalização da ANPD e das hipóteses em que é permitido o tratamento de dados pessoais

Trata-se de um valor simbólico para a empresa, mas um alerta para os órgãos públicos e privados de que a privacidade dos consumidores e o cumprimento da LGPD precisam ser assegurados porque as autoridades de fiscalização estão alertas.

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade – CNPDPP - é o órgão consultivo da ANPD e tem sua composição e competências definidas pela Lei nº 13.709, de 2018 e pelo Decreto nº 10.474, de 2020.

Aqui se pretende apresentar a necessidade de uma política pública de regras

para o trato dos dados pessoais dos consumidores em atenção à preservação da privacidade dos mesmos, em ambiente da inteligência artificial, e efetivação do princípio constitucional da ordem econômica da defesa do consumidor. Com vistas nisso, a criação desses órgãos é um exemplo de boa governança no tocante aos dados pessoais dos consumidores.

2.5 EM BUSCA DA BOA GOVERNANÇA

Governança pública é o “conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade” (TCU, 2020).

Observe-se que se trata do gerenciamento do Estado, o modo de como administrar a máquina pública, enaltecendo-se mecanismos considerados importantes para o sucesso de uma política de governança, se reforçando a importância da construção e da coordenação de políticas focadas no cidadão. Percebe-se que a governança serve para se fortalecer a confiança nas instituições públicas, fomentar a coerência das ações públicas e promover a sua coordenação e, estabelecer diretrizes para a tomada de ações.

Por isso é importante que a sociedade se questione sobre qual o Estado que ela quer: quer o Estado corrupto, desonesto, ou um Estado probo, ético e justo? O clamor público já deixou clarividente que a sociedade deseja um Estado honesto, tal qual ela mesma em geral. Mas outra questão surge nesse momento: como se pode alcançar esse Estado?

Existem alguns indicadores de governança que os Estados podem seguir para atingir uma boa governança. Eles estão ordenados em princípios, apresentados no Decreto 9.203, de 2017. Foram construídos a partir das “recomendações mais atuais de organizações internacionais especializadas no tema, em especial a OCDE e o Banco Mundial e de referenciais de governança do Tribunal de Contas da União. Dentre esses princípios, citem-se: a capacidade de resposta, integridade, confiabilidade, melhoria regulatória, prestação de contas e responsabilidade, e transparência. Eles devem permear todos os trabalhos de governança, a fim de que

alcance o seu mais alto grau de eficácia na atuação pública (CASA, 2018):

[...] a primeira função pretendida para os princípios e diretrizes de governança é servir como um elemento de conexão entre esses princípios constitucionais e a atuação do agente público. Dessa forma, pretende-se que este tenha preceitos mais práticos para que sua atuação se mantenha centrada no cidadão e no cumprimento cada vez mais fiel de sua missão pública. Espera-se, além disso, que a aplicação dos princípios e diretrizes de governança reforce o conteúdo normativo dos princípios constitucionais, expandindo seus respectivos campos de interpretação (CASA, 2018, p. 37).

A criação dos referidos princípios de governança são, antes de tudo, uma tentativa de se fazer cumprir, no âmbito da administração pública, os princípios constitucionais da legalidade – “ao administrador somente é dado realizar o que estiver previsto na lei” -, moralidade – “necessidade de toda a atividade administrativa atender a um só tempo à lei, à moral e à equidade, em suma, aos deveres da boa e honesta administração” -, impessoalidade – “a atuação do administrador público seja voltada ao atendimento impessoal e geral, ainda que venha a interessar a pessoas determinadas, não sendo a atuação atribuída ao agente público, mas à entidade estatal a que se vincula” -, eficácia – “necessidade de adoção, pelo administrador, de critérios técnicos e profissionais, que assegurem o melhor resultado possível, rechaçando-se qualquer forma de atuação amadorística e ineficiente do Poder Público” - e publicidade – “é obrigatória a divulgação e o fornecimento de informações de todos os atos praticados pela Administração Pública” - previstos no art. 37, da CF/88 (SPITZCOVSKY; LENZA, 2023, p. 55).

Isso se faz importante porque para a administração pública, cumprir o princípio da privacidade é necessária à efetivação do princípio constitucional da defesa do consumidor no tocante à proteção de dados dos consumidores, precisa-se estar envolta da lisura necessária à execução dessa atividade. Atos de corrupção, por exemplo, não podem fazer parte da boa governança no que diz respeito ao direito fundamental humano da privacidade dos consumidores.

A Administração Pública detém prerrogativas e sujeições, com o fito de suprir as necessidades decorrentes do interesse coletivo, o que permite, muitas vezes, em virtude da supremacia do interesse público sobre o particular, o condicionamento ou limitação do exercício de direitos e liberdades individuais. Para alcançar o bem público, o Estado exerce determinadas atividades, tais como a manutenção da ordem interna e a execução de serviços para o bem-estar e o progresso da coletividade. Entre as funções do Estado, podemos identificar: a função legislativa, que consiste na elaboração das normas que irão disciplinar a vida social; a

função judiciária, que consiste na interpretação e aplicação do direito em situações concretas, e a função administrativa, que se relaciona ao atendimento das necessidades materiais do povo (PINTO, 2008, p. 131).

Apenas a título de exemplo, no caso da Lava Jato, um dos maiores e recentes escândalos presenciados pelos brasileiros, nota-se uma afronta aos princípios constitucionais da administração pública, pois envolveu informações sigilosas na Petrobrás e empresas contratadas. Houve ilicitude no procedimento de licitação no âmbito público, fato este que infringiu os princípios éticos da boa-fé, probidade e deveres da boa administração.

O princípio da moralidade foi abalado na medida em que condutas desonestas com outras empresas privadas eram realizadas no âmbito da licitação. O Código de Ética Profissional do Servidor Público Federal, aprovado pelo Decreto n. 1.171 de 1994, enaltece o princípio da moralidade administrativa, dispondo textualmente que o servidor jamais poderá desprezar o elemento ético de sua conduta, devendo decidir não somente entre 'legal e o ilegal, o justo e o injusto, o conveniente do inconveniente, o oportuno do inoportuno, mas principalmente o honesto do desonesto':

Por considerações de Direito e de Moral, o ato administrativo não terá que obedecer somente a lei jurídica, mas também a lei ética da própria instituição, porque nem tudo que é legal é honesto, conforme já proclamava os romanos: "non omne quod licet honestum est". A moral comum é imposta ao homem para sua conduta externa e a moral administrativa é imposta ao agente público para sua conduta interna para se atingir o tão almejado bem comum. (...) A atividade dos administradores, além de traduzir a vontade de obter o máximo de eficiência administrativa, terá ainda que corresponder à vontade constante de viver honestamente, de não prejudicar outrem e de dar a cada um o que lhe pertence princípios de Direito Natural já lapidamente formulados pelos litisconsultos romanos (ZANON JR, 2014, p. 18).

E houve infração ao princípio da impessoalidade uma vez que:

a igualdade de tratamento que a administração deve dispensar aos administrados que estejam na mesma situação jurídica. Exige, também, a necessidade de que a atuação administrativa seja impessoal e genérica, com vistas a satisfazer o interesse coletivo. Esta é a razão pela qual deve ser imputada a atuação administrativa ao órgão ou entidade estatal executora da medida, e não ao agente público, pessoa física. Forçoso convir que, em decorrência do princípio da impessoalidade, é vedado tratamento discriminatório aos administrados que se encontrem nas mesmas situações. A impessoalidade encontra-se relacionada com a finalidade, ou seja, com o fim previsto na lei, cujo desrespeito configura desvio, o que invalida o ato administrativo. O princípio da impessoalidade

também combate o desvirtuamento da atuação do administrador público como meio de promoção pessoal, sendo, portanto, vedada a utilização de nomes, símbolos e imagens nas realizações da administração, que, em prejuízo do interesse público, promovam partidos políticos e agentes públicos, comprometendo a legítima atuação administrativa, que deve ser impessoal, abstrata e genérica (PINTO, 2008, p. 134).

A boa governança no setor público deve ser um fator indispensável no assunto de proteção de dados dos consumidores. A lisura, probidade, licitude, transparência, boa-fé, moralidade, legalidade, moralidade e impessoalidade devem ser princípios *sine quae non* no âmbito público, principalmente quando se trata aqui da elaboração de uma política pública passível de ser aplicada nacionalmente.

Outra preocupação deste estudo é o de que a população carente tenha acesso democrático às políticas públicas de proteção aos seus dados, para que esse assunto não se elitize e se torne apenas uma preocupação das classes mais privilegiadas economicamente. Trata-se de assuntos que deveriam ser de conhecimento amplo da população, uma vez que as ações afirmativas são políticas públicas feitas pelo governo ou pela iniciativa privada com o objetivo de corrigir desigualdades presentes na sociedade, acumuladas ao longo de anos. Uma ação afirmativa busca oferecer igualdade de oportunidades a todos (SZUPSZYNSKI, 2014).

Assim, no capítulo seguinte, apresenta-se aqui a necessidade de uma política pública de tratamento dos dados pessoais dos consumidores.

CAPÍTULO 3. POR UMA POLÍTICA PÚBLICA PREVENTIVA DE DEFESA DOS DADOS DIGITAIS DO CONSUMIDOR – ANÁLISE DE VAZAMENTOS DE DADOS NO CASO CHAGPT

Neste capítulo, apresentar-se-á a necessidade de uma política pública preventiva de defesa dos dados pessoais dos cidadãos na dimensão dos consumidores, em garantia do princípio constitucional econômico de defesa do consumidor, em virtude das fragilidades verificadas no caso do ChatGPT com relação a estes dados.

Talvez se trate de uma das maiores ocorrências de vazamento de dados registradas até hoje na história da tecnologia, em sendo assim, busca-se identificar as evidências aqui. Para tanto, inicia-se com uma explicação sobre a inteligência artificial, visto ser o chatGPT uma das espécies dessa linguagem tecnológica, para, só então, avaliar-se o caso de propor a política pública necessária.

3.1 INTELIGÊNCIA ARTIFICIAL

As ideias de Inteligência Artificial começaram a ser desenvolvidas já durante a Segunda Guerra Mundial. Por isso que se mencionam, paradoxalmente, os avanços de algumas guerras no mundo, pois, embora seja uma luta bélica entre nações ocasionada por fatores econômicos, a sociedade avança em termos tecnológicos pois várias experiências são testadas nesse momento. Longe de se querer dizer que as guerras são positivas para a humanidade, foi durante a Segunda Guerra Mundial quando a Medicina mais se desenvolveu, devido aos inúmeros testes realizados com os judeus, por exemplo, na época do Holocausto.

3.1.1 Origens

Assim, para se ter um parâmetro do início das pesquisas no campo da AI - inteligência artificial, o primeiro trabalho nesta área, reconhecido, foi elaborado por McCulloch e Pitts, em 1943. Estes pesquisadores desenvolveram um modelo de neurônios artificiais, que conectados em rede, tal estrutura a partir de estímulos adequados, poderiam ser capazes de aprender. Em 1950, o primeiro computador usando redes neurais, foi construído por dois alunos de Harvard, Marvin Minsky e

Dean Edmonds (RUSSELL; NORVIG, 2013, p. 41)

Também foi em 1950 que uma visão persuasiva surge com Alan Turing. em Seu artigo “Computing Machinery and Intelligence¹²” criou uma forma de avaliar se uma máquina poderia se passar por humano em uma conversa por escrito: foi o chamado experimento do “jogo da imitação”.

Em 1951, o SNARC criou uma calculadora de operações matemáticas que simulava as ligações entre neurônios, chamadas sinapses. Somente em 1956, na Conferência de Dartmouth, encontro que reuniu várias das personalidades da Tecnologia, criou-se a IA como nome do campo de pesquisa dessa conferência. Nela, percebeu-se que cada aspecto de aprendizado ou outra forma de inteligência poderia ser descrita de forma tão precisa que uma máquina poderia ser criada para simular isso. (RUSSELL; NORVIG, 2013, p. 41)

Assim, muitos investimentos começaram a ser destinados a essa área. A Agência de Pesquisa de Projetos Avançados (ARPA), mesma entidade na qual nasceu a internet, foi uma dessas empresas. Somente em 1964 foi lançado o primeiro chatbot do mundo. O ELIZA conversava de forma automática, por meio da imitação de uma psicanalista, usando respostas baseadas em palavras-chave e estrutura sintática. Já em 1969, surge o primeiro robô que unia mobilidade, fala e autonomia de ação: o Shakey. (RUSSELL; NORVIG, 2013)

Era um tempo em que a Inteligência Artificial gerava grandes expectativas porque, na prática, nada era muito concreto ou rápido. Atualmente, o medo ainda toma conta das pessoas sobre os pontos negativos que isso pode trazer. Todavia, na evolução da espécie, é preciso se arriscar, ousar, inventar, experimentar, testar, a fim de se descobrir novas tecnologias que venham a melhorar a qualidade de vida das pessoas. Ademais, sempre haverá pontos negativos em tudo na vida: a tecnologia pode ser usada para fins lícitos ou ilícitos, vai depender das pessoas.

Continuando: as décadas de 70 e 80 não foram muito frutíferas para a IA devido aos poucos investimentos e avanços no setor. Foi também um período marcado pelo advento dos sistemas especialistas, softwares responsáveis por tarefas tão complexas quanto a de humanos, mas com mais velocidade. Por

12 Máquinas de Computação e Inteligência

exemplo, hoje vemos sistemas especialistas empregados para declaração do Imposto de Renda. (RUSSELL; NORVIG, 2013)

Assim, a Inteligência Artificial é a capacidade das máquinas de pensar como seres humanos: aprender, perceber e decidir quais caminhos seguir, de forma racional, diante de determinadas situações. A Inteligência Artificial permite que os sistemas tomem decisões de forma independente, precisa e apoiada em dados digitais. Aos poucos, o sistema absorve, analisa e organiza os dados, entendendo e identificando objetos, pessoas, padrões e reações. Na medida em que o banco de dados cresce, essa máquina aprende, o que torna as decisões cada vez mais complexas. (RUSSELL; NORVIG, 2013)

A IA possui duas áreas: a Inteligência Artificial Simbólica, ligada à forma como os seres humanos raciocinam, e a Inteligência Artificial Conexionista, ligada à simulação de componentes do cérebro, as redes neurais. (RUSSELL; NORVIG, 2013)

Nota-se que a IA está, então, mais perto das pessoas do que se imagina. Por exemplo, o corretor ortográfico dos smartphones, que completa frases e usa as mais frequentes, é um exemplo de IA. Outros exemplos são os aplicativos que calculam as melhores rotas para evitar congestionamentos, as buscas personalizadas na internet e os carros autônomos. Trata-se de usos bastante úteis à sociedade. (RUSSELL; NORVIG, 2013)

Mas a IA também pode ser utilizada para fins não muito éticos, como o caso na área de Recursos Humanos, em que empresas vêm avaliando candidatos e listando os que apresentam perfis mais compatíveis as suas vagas. Isso, ao mesmo tempo em que é uma maneira de as empresas otimizarem o seu tempo, também se mostra como uma forma de se reduzir a oportunidade de muitas pessoas de se candidatarem a uma vaga de emprego nesta empresa, ou mesmo de se discriminar determinadas pessoas. (RUSSELL; NORVIG, 2013)

3.1.2 Estrutura

A IA funciona com um hardware, sua parte física – ou seja, as peças – de uma máquina, enquanto a sua outra parte é chamada de software – ou seja, a sua programação –, também chamado de “cérebro” da IA, pois comanda as suas peças.

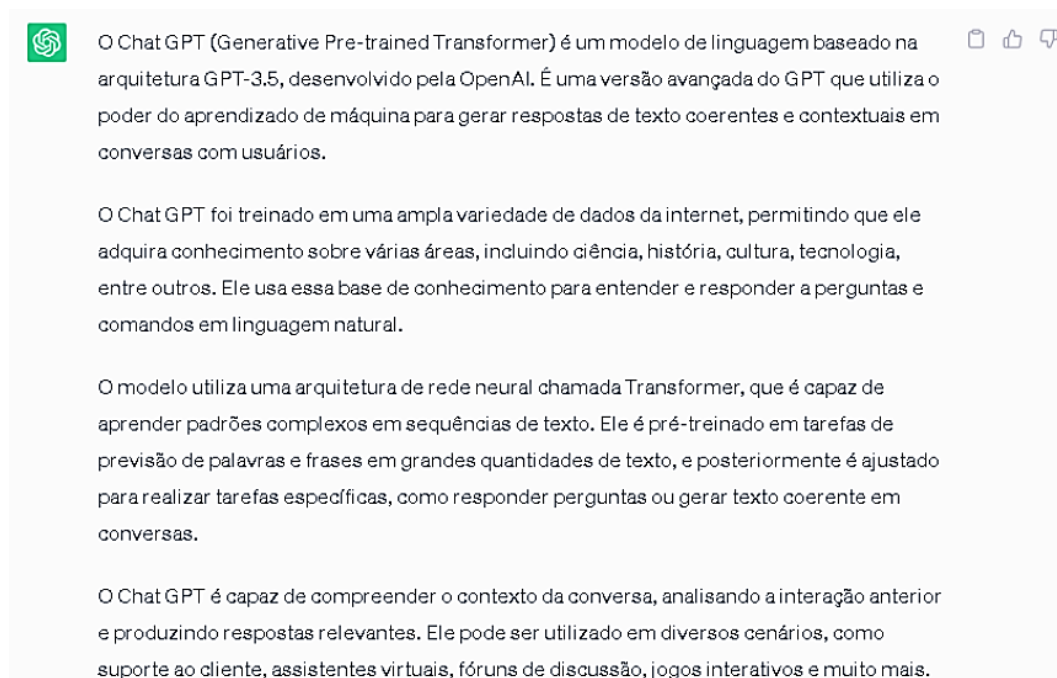
Por exemplo, o segredo para um carro andar sozinho não está nas peças, mas no programa que comanda seus movimentos.

A Ciência da Computação estuda as técnicas e modos de processamento de dados. O desenvolvimento de algoritmos é uma questão central nessa área. Algoritmos são uma sequência de instruções, operações e raciocínios que orientam o funcionamento de um software. Por sua vez, esse software pode determinar os movimentos de um hardware:

O algoritmo, na IA, trabalha com hipóteses e uma resposta para cada um deles. As máquinas escolhem, entre milhares de variáveis, respostas compatíveis aos problemas complexos. Nisso, existem diferenças entre machine learning e deep learning. Basicamente, machine learning (aprendizado de máquina) e deep learning (aprendizagem profunda) são pilares da IA. Em primeiro lugar, machine learning diz respeito ao uso de algoritmos para organizar dados, reconhecer padrões e fazer com que computadores possam aprender. Isso para gerar insights inteligentes sem necessidade de pré-programação. Já o deep learning é a parte do aprendizado de máquina que, por meio de algoritmos de alto nível, reproduz a rede neural do cérebro humano. Em resumo, podemos dizer que machine learning estabeleceu as bases para deep learning evoluir. (RUSSELL; NORVIG, 2013, p. 198)

Assim foi como surgiu o Chat GPT. Para conceituá-lo, perguntou-se a ele mesmo o que ele era e, a seguir, tem-se a resposta:

FIGURA 2 – AMOSTRA DO CHATGPT



FONTE: CHATGPT

Obviamente, a fim de se sanar uma curiosidade simples, ele se parece extremamente útil e completo. Todavia, sendo este um trabalho acadêmico, deve-se citar a fonte, que não é feito no Chat GPT. Isso levaria o cientista a ser acusado de plágio por exemplo. Seu estilo também é bastante mecânico, o que se distingue da linguagem humana escrita.

Assim, tem-se que:

O ChatGPT é um modelo de linguagem avançado desenvolvido pela OpenAI. Ele é baseado na arquitetura GPT, que significa Generative Pre-trained Transformer, em inglês, que pode ser traduzido como Inteligência Artificial Generativa. (RUSSELL; NORVIG, 2013, p. 302)

O ChatGPT é fruto da OpenAI, uma instituição sem fins lucrativos focada em pesquisa em inteligência artificial (IA). Ela foi fundada por Elon Musk e Sam Altmané. capaz de realizar diferentes atividades, como criar respostas, produzir textos e até entender a linguagem humana e códigos de programação. No Brasil, estima-se que cerca de 63% das organizações utilizam aplicações baseadas nessa tecnologia – a título de exemplo, mais de 90% das empresas brasileiras investem em ferramentas de dados e analytics com o objetivo de identificar tendências e padrões de consumo. (RUSSELL; NORVIG, 2013)

O ChatGPT é um serviço disponível gratuitamente que possui várias funções diferentes, incluindo responder perguntas, resolver equações matemáticas, escrever textos, depurar e corrigir códigos, traduzir entre idiomas, criar resumos de textos, fazer recomendações, classificar coisas e explicar o que algo faz, como um bloco de código. Ele foi treinado usando o Reinforcement Learning from Human Feedback, um método que utiliza o feedback humano para ajustar os modelos de IA. Ele não faz pesquisas na internet nem faz cruzamento de dados externos. Todo o seu raciocínio é feito a partir das informações de texto que foram inseridas nele. Inclusive, quando perguntado, o próprio ChatGPT explica que é incapaz de criar novas coisas, apenas interpretar e esclarecer com base no que já sabe. (RUSSELL; NORVIG, 2013, p. 378)

O ChatGPT possui um manuseio muito simples. Para quem utiliza assistentes virtuais como Siri ou Alexa, a ideia é a mesma: basta dar um comando e a resposta vem. O passo a passo é o seguinte: acessar o site, criar uma conta, se for a primeira vez que estiver usando, clicando em “Sign up”, insirindo um e-mail válido e cadastrando uma senha; ao entrar, a plataforma vai dar instruções; depois, seleciona-se uma categoria para o uso e se dá o comando.

Outros aplicativos geradores de imagens, como o IA DALL-E 2, também são fruto da IA. A Microsoft está lançando o Designer, site semelhante ao Canva. A Microsoft e a OpenAI também já anunciaram o DALL-E 2, que será implementado para que usuários criem imagens exclusivas. O Lensa, também, viralizou ao oferecer avatares únicos a partir das fotografias utilizando IA.

A OpenAI, apesar de tudo isso, diz que o ChatGPT ainda apresenta falhas e que o sistema de moderação precisa ser otimizado. Para diminuir os danos, a empresa criou um conjunto de diretrizes para as quais o chat seja submetido:

Respeito e imparcialidade: o ChatGPT é projetado para tratar todos os usuários com respeito e imparcialidade, independentemente de sua origem, raça, gênero, religião ou orientação sexual. O objetivo é promover uma interação inclusiva e não discriminatória;

Responsabilidade: o ChatGPT deve ser responsável por suas respostas e ações, fornecendo informações precisas e relevantes, evitando espalhar desinformação e assumindo a responsabilidade por quaisquer erros ou limitações em seu conhecimento;

Privacidade e segurança: o ChatGPT deve proteger a privacidade dos usuários e usuárias, não coletando ou compartilhando informações pessoais sem consentimento adequado. Também deve evitar o incentivo a comportamentos prejudiciais ou ilegais;

Transparência: o ChatGPT deve ser transparente sobre sua natureza como um modelo de inteligência artificial, deixando isso claro para as pessoas que estão interagindo com uma máquina. Isso ajuda a evitar mal-entendidos e expectativas incorretas. (RUSSELL; NORVIG, 2013, p. 413)

Neste momento, chama-se a atenção para a diretriz que se refere à privacidade e segurança: as informações usadas pelo ChatGPT foram retiradas de uma pesquisa contendo muitas obras analíticas e remissivas sobre diversos assuntos. Quando se consultou o conceito de chatGPT, por exemplo, o que chamou a atenção foi a ausência das fontes utilizadas. Isso significa que muitas obras com direitos autorais garantidos foram utilizadas sem a devida referência.

Recentemente, um grande vazamento de dados realizado pelo ChatGPT, foi detectado. É o que se verá a seguir.

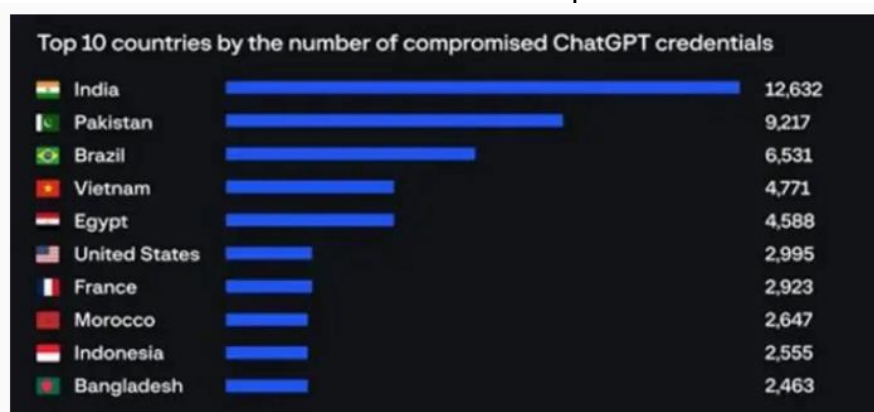
3.1.3 O Caso do ChatGPT

O ChatGPT se tornou mundialmente conhecido em virtude do banimento temporário sofrido em território italiano, determinado pela Agência de Proteção de Dados da Itália para que ele se adequasse à lei de proteção de dados vigente na União Europeia.

Neste estudo, optou-se por escolher o caso ChatGPT como exemplo de vazamento de dados dos consumidores, exatamente pela grande repercussão que suas ações inadequadas com relação ao cumprimento a Lei de Proteção a Privacidade dos dados Pessoais, alcançaram em todo o planeta.

Em março, desse ano (2023), ocorreu, um dos maiores bugs¹³ da história da tecnologia. A empresa de segurança cibernética Grey Noise detectou que o ChatGPT teria exposto um grande número de dados de clientes e fornecedores. Em 20 de março de 2023, a OpenAI sofreu um *data Breach* (brecha nos dados – violação de dados) em relação aos dados dos pagamentos de clientes que possuem seu serviço de assinatura. A seguir, tem-se a lista do número de contas invadidas em alguns países:

FIGURA 3 – Contas invadidas em cada país



FONTE: G1, 2023.

A título de cumprimento da LGPD, o que se deveria fazer em um caso como esse? Nesse panorama, como parte dos processos corporativos de gestão de incidentes (meio de reparação de prestação de serviços), é sabido que o agente de tratamento (operação desses dados) deve em primeiro lugar implementar procedimentos para a identificação e registro de violações de dados pessoais.

Conhecida a dimensão do vazamento, o segundo passo a ser dado é o estabelecimento de um canal de comunicação para as partes atingidas pela exposição desses dados e a cooperação, junto às autoridades, explicando para as

¹³ Bug de software é um erro ou falha que ocorre num sistema ou programa de computador, resultando num comportamento incorreto, inesperado ou fora do que tenha sido pretendido pelo desenvolvimento. https://www.hostinger.com.br/tutoriais/o-que-e-bug#O_Que_e_Bug, acessado em: agosto, 023

vítimas de forma clara como se deu o vazamento, o que foi vazado e o que está sendo feito para conter os danos da exposição. Ao mesmo tempo, a empresa deve comunicar à Autoridade Nacional de Proteção de Dados todos os detalhes envolvidos no vazamento.

A contenção dos danos deve ser feita por meio da adoção de reforços nos sistemas de segurança, de modo a garantir que novas exposições de informações não ocorram. Cumpre destacar que as medidas a serem tomadas não valem apenas para o vazamento criminoso de dados, mas também para qualquer tratamento inadequado, como o bug ocorrido nos sistemas Chat GPT.

Por fim, a LGPD estabelece que caso a empresa não obedeça a esses procedimentos de contenção de danos, podem haver sanções administrativas que vão desde advertência até multas simples ou diárias de até 50 milhões de reais.

Em resumo: a diretriz do ChatGPT demonstrou, que seu item privacidade e segurança, não foi cumprido. O direito fundamental humano dos consumidores não foi garantido nem efetivado. Direito este previsto constitucionalmente no ordenamento jurídico brasileiro.

Os consumidores foram violados em sua privacidade por uma empresa que deveria fornecer serviços de qualidade, com segurança, protegendo o sigilo de suas informações que lhes foram repassadas com boa-fé. O mínimo que se poderia esperar era o resguardo dessas informações.

Já a par desses problemas, a Apple, a Samsung e a Amazon são exemplos de empresas que optaram por proibir o uso do ChatGPT devido a preocupações específicas relacionadas justamente à privacidade de informações internas e à possibilidade de respostas geradas serem semelhantes a dados dos proprietários. Cada companhia optou por implementar medidas alternativas para lidar com suas necessidades de IA interna.

Apesar das garantias, inquire-se os titulares dos dados, se estão cientes do uso de dados (possivelmente sensíveis) para integrar o conhecimento da IA. Ademais, como apurar e garantir que as condições de proteção de dados pessoais asseguradas pela OpenAI foram, de fato, respeitadas? E mais: nota-se que, apesar de os filtros de segurança terem sido utilizados pelo ChatGPT, houve, inegavelmente, o tratamento de dados durante a condução da fase de treinamento

da IA. A LGPD é taxativa ao prever que o tratamento de dados pessoais é vinculado à existência de uma base legal cabível (art. 7º da Lei nº 13.709/2018). Assim, esta não foi respeitada no caso do ChatGPT.

Lamentavelmente, de acordo com a dona do ChatGPT, “a segurança online é uma responsabilidade do usuário, que deve usar antivírus e tomar cuidado com possíveis programas maliciosos” (G1, 2023). A seguir, tem-se a nota divulgada da empresa para o site Tom’s Hardware:

Os resultados do relatório de inteligência de ameaças da Group-IB são o resultado de malware de commodities nos dispositivos das pessoas e não de uma violação da OpenAI. Atualmente, estamos investigando as contas que foram expostas. A OpenAI mantém as melhores práticas do setor para autenticar e autorizar [a entrada] dos usuários em serviços, incluindo o ChatGPT, e incentivamos nossos usuários a usar senhas fortes e instalar apenas softwares verificados e confiáveis em computadores pessoais.

Por estes motivos, acredita-se aqui que a LGPD não é suficiente para lidar com a dimensão gigantesca que a IA e os dados pessoais estão atingindo na atualidade. É preciso que não só exista o encaixe de uma base legal que traga segurança ao detentor de dados, afirmando o compromisso com o direito fundamental à proteção de dados pessoais, a fim de respaldar as informações processadas durante o treinamento do ChatGPT, mas que também se delimite o entendimento legal, a fim de se proporcionar ao titular de dados pessoais uma experiência enriquecedora e útil no dia a dia, buscando um desenvolvimento consciente e justo para ambas as partes. E ainda não apenas isso: é preciso que se crie uma política pública de proteção de dados pessoais e privacidade.

De acordo com o Direito do Consumidor, sabe-se que o consumidor é a figura da relação de consume mais frágil. Por isso mesmo ele goza do princípio da hipossuficiência ou vulnerabilidade. Sob hipótese alguma, o argumento da dona da empresa do ChatGPT prospera. Trata-se de uma tentativa desesperada de se eximir de uma responsabilidade objetiva da empresa. Ademais, o consumidor possui diversos órgãos para sua proteção, e leis específicas sobre dados pessoais.

Neste sentido, o caso do robô ChatGPT mostra que a inteligência artificial é uma realidade em nossa sociedade e precisa de regulamentação urgente. Este caso

mostrou a vulnerabilidade dos dados dos consumidores, bem como a situação de negligência à LGPD. Esse exemplo ilustra a necessidade urgente de se criar uma política pública em prol da proteção dos dados dos consumidores.

3.2 A DEFESA DO CONSUMIDOR E A PROTEÇÃO DOS DADOS PESSOAIS

O Sistema Nacional de Defesa do Consumidor (SNDC) congrega Procons, Ministério Público, Defensoria Pública e entidades civis de defesa do consumidor, que atuam de forma articulada e integrada com a Secretaria Nacional do Consumidor (SENACON):

O SNDC se reúne trimestralmente para analisar conjuntamente os desafios enfrentados pelos consumidores e para a formulação de estratégias de ação, tais como, fiscalizações conjuntas, harmonização de entendimentos e elaboração de políticas públicas de proteção e defesa do consumidor. Os órgãos do SNDC têm competência concorrente e atuam de forma complementar para receber denúncias, apurar irregularidades e promover a proteção e defesa dos consumidores (MARQUES; MIRAGEM; BENJAMIM, 2021, p. 12)

Os Procons são órgãos estaduais e municipais de proteção e defesa do consumidor, criados especificamente para este fim, com competências, no âmbito de sua jurisdição, para exercer as atribuições estabelecidas pela Lei 8.078, de 11 de setembro de 1990, e pelo Decreto nº 2.181/97. São, portanto, órgãos que atuam no âmbito local, atendendo diretamente os consumidores e monitorando o mercado de consumo local, tendo papel fundamental na execução da Política Nacional de Defesa do Consumidor.

O Ministério Público e a Defensoria Pública, no âmbito de suas atribuições, também atuam na proteção e na defesa dos consumidores e na construção da Política Nacional das Relações de Consumo. O Ministério Público, de acordo com sua competência constitucional, além de fiscalizar a aplicação da lei, instaura inquéritos e propõe ações coletivas. A Defensoria, além de propor ações, defende os interesses dos desassistidos, promovendo acordos e conciliações. As entidades civis desenvolvem importante papel na proteção e defesa do consumidor. Elas representam o conjunto organizado de cidadãos em torno de uma instituição

devidamente registrada e com função estatutária de proteção e defesa dos consumidores.

A Secretaria Nacional do Consumidor, por sua vez, tem por atribuição legal a coordenação do SNDC e está voltada à análise de questões que tenham repercussão nacional e interesse geral, além do planejamento, elaboração, coordenação e execução da Política Nacional de Defesa do Consumidor, prevista no art. 5º do CDC:

Para a execução da Política Nacional das Relações de Consumo, contará o poder público com os seguintes instrumentos, entre outros:

- I - manutenção de assistência jurídica, integral e gratuita para o consumidor carente;
- II - instituição de Promotorias de Justiça de Defesa do Consumidor, no âmbito do Ministério Público;
- III - criação de delegacias de polícia especializadas no atendimento de consumidores vítimas de infrações penais de consumo;
- IV - criação de Juizados Especiais de Pequenas Causas e Varas Especializadas para a solução de litígios de consumo;
- V - concessão de estímulos à criação e desenvolvimento das Associações de Defesa do Consumidor.
- VI - instituição de mecanismos de prevenção e tratamento extrajudicial e judicial do superendividamento e de proteção do consumidor pessoa natural;
- VII - instituição de núcleos de conciliação e mediação de conflitos oriundos de superendividamento.

De maneira mais específica, sobre a proteção dos dados pessoais dos consumidores, tem-se a Autoridade Nacional de Proteção de Dados – ANPD, que já se abordou no primeiro capítulo. Suas funções são as de:

- I - zelar pela proteção dos dados pessoais, nos termos da legislação;
- II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
- III - **elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;**
- IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- V - apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
- VI - **promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;**

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;

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;

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos;

XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;

XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento;

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (LGPD, grifo nosso)

Após, citadas as competências da ANPD, percebe-se que o seu conjunto exige a elaboração de uma Política Pública Preventiva de Proteção de Dados Pessoais e da Privacidade do Consumidor, principalmente devido às exigências dos incisos III e VI em negrito, e, ainda, pela defesa do consumidor ser um dos princípios constitucionais da ordem econômica..

Destaca-se, ainda, o Conselho de Proteção de Dados Pessoais e da Privacidade – CNPDPP. Ele está incumbido de:

- I - propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD;
- II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- III - sugerir ações a serem realizadas pela ANPD;
- IV - elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade; e
- V - disseminar o conhecimento sobre a proteção de dados pessoais e da privacidade à população.

Note-se que são muitos os órgãos existentes para contribuírem com a política pública que aqui se propõe.

3.3 A NECESSIDADE DE UMA POLÍTICA PÚBLICA PREVENTIVA DE PROTEÇÃO DE DADOS DOS CONSUMIDORES, NA ESFERA DIGITAL, PARA A GARANTIA DA PRIVACIDADE E DO PRINCÍPIO CONSTITUCIONAL DA ORDEM ECONÔMICA CONSTITUCIONAL DA DEFESA DO CONSUMIDOR

Políticas públicas podem ser definidas como o conjunto de diretrizes e intervenções emanadas do Estado, feitas por pessoas físicas e jurídicas, públicas e/ou privadas, com o objetivo de tratar problemas públicos e que requerem, utilizam ou afetam recursos públicos (TCU, 2021). O vazamento de dados pessoais de consumidores tem de fato se tornado um problema do consumidor, de direito fundamental, constitucional e de segurança pública cibernética.

Dias e Matos (2012, p. 37) explicam que políticas públicas:

são ações e programas que são desenvolvidos pelo Estado para garantir e colocar em prática direitos que são previstos na Constituição Federal e em outras leis. São medidas e programas criados pelos governos dedicados a garantir o bem estar da população. Além desses direitos, outros que não

estejam na lei podem vir a ser garantidos através de uma política pública. Isso pode acontecer com direitos que, com o passar do tempo, sejam identificados como uma necessidade da sociedade. O planejamento, a criação e a execução dessas políticas é feito em um trabalho em conjunto dos três Poderes que formam o Estado: Legislativo, Executivo e Judiciário. O Poder Legislativo ou o Executivo podem propor políticas públicas. O Legislativo cria as leis referentes a uma determinada política pública e o Executivo é o responsável pelo planejamento de ação e pela aplicação da medida. Já o Judiciário faz o controle da lei criada e confirma se ela é adequada para cumprir o objetivo.

As políticas públicas existem para viabilizar o pleno desenvolvimento social e econômico do País. No caso em tela, percebe-se uma necessidade urgente de uma política pública para a proteção de dados pessoais dos consumidores e a sua consequente garantia da privacidade. Isso porque esse direito fundamental está sendo violado pelas empresas de tecnologia, especialmente as de IA (inteligência artificial) que vem se desenvolvendo atualmente.

Diante do cenário de limitação de recursos destinados ao financiamento de ações públicas, faz-se necessária a adoção de práticas transparentes e mais racionais sobre escolha, formulação e execução de políticas que, de fato, entreguem valor para a sociedade. O mundo todo está diante dessa premente necessidade.

O processo de avaliação, antes, durante e após a implementação da política, fornecerá informações relevantes e fundamentadas sobre o sucesso ou a falha das intervenções efetivadas. Essas informações são essenciais para subsidiar o processo decisório acerca da continuidade do curso de ação, da revisão da concepção, de mudanças no curso de implementação ou, até mesmo, da indicação sobre a necessidade de extinção da política escolhida. Até o momento, as informações sobre o vazamento de dados pessoais dos consumidores demonstram uma necessidade verdadeira para a existência de uma política pública nessa área.

O diagnóstico do problema relativo à proteção de dados pessoais, em especial na esfera digital, e necessidade de privacidade ao consumidor é clarividente. É preciso agora, com o intuito de se elaborar uma política pública, apenas formar uma agenda, analisar as alternativas possíveis, tomar a decisão, apresentar como será desenvolvida a política, estruturar a governança e gestão, e alocar e gerir os recursos orçamentários e financeiros, operação, monitoramento e avaliação. O principal, que é a detecção da problemática, já existe de há muito.

As práticas voltadas para a identificação do problema são conhecidas por

todos e estão sendo divulgadas e acompanhadas pelos telejornais no mundo. A delimitação e caracterização do problema já está feita, além de já se saber o público alvo e as possíveis causas, efeitos e formas de resolução:

Formação da agenda pública envolve a escolha do conjunto de problemas ou temas considerados merecedores de intervenção pública. Desenho da política pública contempla a caracterização da política com base em modelo lógico que explicita, entre outras coisas, seus objetivos, produtos, atividades, resultados e impactos. Análise de alternativas se desenvolve por meio de escrutínios formais ou informais das consequências do problema e confronta aspectos como custos-benefícios e custo-efetividade de cada alternativa disponível para apoiar o processo de tomada de decisão. Tomada de decisão representa o momento em que os interesses dos atores são equacionados e as intenções (objetivos e métodos) de enfrentamento de um problema são explicitadas. Estruturação da governança e gestão envolve a definição das estruturas de governança, de gestão de riscos e controles internos, de monitoramento e de avaliação da política pública, bem como do plano de implementação da política, dos processos e operações necessários ao seu funcionamento. Alocação e gestão de recursos orçamentários e financeiros compreende, entre outras coisas, a identificação das fontes de financiamento e a disponibilização tempestiva de créditos orçamentários e recursos financeiros necessários à implementação da política pública. Operação e monitoramento é o momento em que regras, rotinas e processos são convertidos de intenções em ações e no qual se produzem os resultados concretos da política pública. Avaliação diz respeito ao processo de julgamento deliberado sobre a validade de propostas para a ação pública ou inação, bem como sobre o sucesso ou falha de intervenções executadas. O resultado da avaliação pode subsidiar a continuidade do curso de ação, a revisão da concepção, mudanças no curso de implementação ou, até mesmo, a indicação de necessidade de extinção da política pública (TCU, 2021, p. 10, 11)

O caso do robô do ChatGPT demonstrou a vulnerabilidade dos dados pessoais dos consumidores, pois a inteligência artificial manuseia com todos esses dados. O vazamento dessas informações dos consumidores é algo que vem se tornando frequente na sociedade. A necessidade de uma política pública preventiva que proteja esses dados é notória.

Hodiernamente, não existe uma política pública voltada para a proteção dos dados pessoais dos consumidores, no que diz respeito a prevenir infrações cometidas pelas AIs a privacidade e a proteção das informações dos consumidores. Registram-se apenas ações dispersas dos órgãos de proteção neste sentido, não se observa uma política que trate essa questão de maneira objetiva.

O TCU apresenta, inclusive, essas etapas citadas acima, para orientar o processo de elaboração da política pública. Os benefícios da criação dessa política pública serão inestimáveis, uma vez que se gastam milhões em indenizações para

quitar os dados aos consumidores quando do vazamento de dados pessoais. O ponto central a se corrigir seria o de se implementar o encaixe de uma base legal que traga segurança ao detentor de dados, afirmando o compromisso com o direito fundamental à proteção de dados pessoais, mas que também se delimite o entendimento legal, a fim de se proporcionar ao titular de dados pessoais uma experiência enriquecedora e útil no dia a dia, buscando um desenvolvimento consciente e justo para ambas as partes.

Fundamental citar o Projeto de Lei n. 2338 de 2023 que atualmente tramita no Senado Federal, de autoria do Senador Rodrigo Pacheco sobre IA. Discute-se um marco legal para a IA, uma vez que se trata de um problema de direitos e garantias fundamentais. É do conhecimento de todos que os impactos dessas tecnologias serão amplos e segmentados, demandando uma proteção legal para a sociedade. Não é sem razão que o Senado Nacional está com a proposta ora apresentada.

A regulamentação da inteligência artificial (IA) é necessária e emergencial, em especial diante dos riscos reais e iminentes. Ela apresenta princípios éticos na utilização da tecnologia; definição da necessidade de que os algoritmos tenham transparência e que sejam explicáveis; asseguramento de direitos e garantias dos afetados pela IA e implementação de medidas para o combate à discriminação. O Projeto propõe definir alguns riscos, classificá-los e com base neles impor deveres de conduta. Os principais pontos a serem discutidos são os erros, discriminações e ampliação de desinformação. Afirma-se, inclusive, que não só o direito fundamental à privacidade pode ser burlado com a IA, mas também os princípios da igualdade, liberdade e devido processo legal (SENADO, 2023).

Deve-se lembrar que a criação dessa política pública e de todas essas discussões que ora ocorrem sobre o marco legal da IA são exemplos da boa governança acontecendo. De acordo com o art. 50 da LGPD:

Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

As primeiras normas de proteção à privacidade foram promulgadas visando a defesa dos direitos de primeira geração, a liberdade em sentido amplo. Num segundo momento, a preocupação externada, principalmente pelo ONU e pela União Europeia, se prendeu ao grande armazenamento de dados por parte das nações com avançado potencial tecnológico, bem como com a segurança na manipulação dessas informações. Já na terceira fase desse processo, momento atual, busca-se meios normativos de estabelecer limites e controle ao armazenamento, fluxo e comercialização desse produto hipervalorizado no mercado digital global, denominado dados pessoais.

Sobre a trajetória das principais leis que abarcam a proteção de dados no universo digital, o caso alemão é paradigmático pois a adoção da Lei no Estado de Hesse precede a discussão e formulação de casos legais acerca da proteção de dados e, posteriormente, a adoção de uma lei federal na Alemanha. (LAVITS, 2023)

Seguiram-se, a partir de então várias iniciativas na Europa, a Suécia promulgou a Datalegen, Lei 289 de 11 de maio de 1973; A Dinamarca regulamentou a questão da proteção de dados pelas Leis 243 e 244, em julho de 1978; A França aprova a Lei 78-77, em janeiro de 1978; A Espanha inseriu em norma constitucional a proteção à privacidade; e em Portugal, 1977, a Constituição, no artigo 35, trouxe a previsão do direito ao cidadão de controlar a utilização de seus dados. Dentro desse período, os Estados Unidos aprovaram leis para regulação dos relatórios de crédito dos consumidores (*Fair Credit Reporting Act* -1970), e ainda, em 1974 a *Privacy Act* (Lei de privacidade), aplicável à administração pública (TAVARES, ALVAREZ, 2016)

Importante destacar, que no final da década de 70, havia no âmbito internacional o debate, iniciado pela ONU, que tratava sobre a transmissão de dados entre os computadores e sobre a comunicação social entre as nações. A preocupação com a conectividade crescente entre os países muda o foco do direito à privacidade, atribuindo-se a ele, não somente a defesa quanto à vida privada do cidadão, mas agrega-se a esse direito, a defesa dos dados pessoais no universo digital, diante das possibilidades de cruzamento e comercialização dessas informações no mercado global.

A partir de então, simultaneamente com o desenvolvimento da tecnologia, cresce a preocupação com o controle dos conteúdos armazenados em formato

digital. Os países que detinham 90% dos bancos de dados, adotaram um posicionamento firmado no fluxo livre das informações armazenadas, como uma extensão ao liberalismo comercial. Já os países em desenvolvimento, eram contrários a esse posicionamento, defendiam um maior controle dos dados que entravam e saíam de seus territórios nacionais. (CARVALHO, 2006, p.78, citando DANTAS, 1988, p. 235).

As legislações nacionais seguiram importantes instrumentos internacionais e transnacionais que contribuíram para a consolidação de um conceito de privacidade ligado à proteção de dados pessoais. Em 1980, as diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais dá início as ações internacionais sobre o tema. Destaca-se aqui, porém, a convenção 108, do Conselho da Europa, em 1981, que ajudou a unificar e desenvolver melhor as normas para o tratamento automatizado de dados pessoais.

No Brasil, em 1988, nossa Constituição Federal, no artigo 5º, trata da privacidade sob a seguinte ordem: “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”. A lei 9.296 de 1996 acrescentou no art. 5º que é “inviolável o sigilo da correspondência e das comunicações telefônicas, salvo as previsões da lei. Importantíssimo passo a defesa das informações pessoais dos brasileiros foi a promulgação do Código de Defesa do Consumidor em 1993, onde consta uma seção específica sobre cadastros e banco de dados.

Mais uma vez a União Europeia, em 1995, através da Diretiva 95/46/CE, contribui significativamente para a estruturação normativa, de maneira uniforme servindo de inspiração para diversos países, no que tange a defesa dos direitos à privacidade e a proteção de dados pessoais, criando um regulamento que estabelece regras a serem respeitadas por todos os membros do grupo.

Uma política de fato, com a formulação, planejamento e avaliação de resultados não existe sobre a questão de proteção de dados dos consumidores quanto aos riscos do mundo cibernético. As políticas públicas preventivas devem ser executadas em todas as esferas de governo do país, com ações em níveis federal, estadual e municipal. Por serem programas relacionados com direitos que são garantidos aos cidadãos, existem políticas públicas preventivas nas áreas de

educação, saúde, trabalho, assistência social, meio ambiente, e moradia, dentre outras. Todavia, ainda não existe para a proteção dos dados pessoais dos consumidores, em específico na esfera digital, notadamente quanto a protegê-lo nas relações de consumo onde a inteligência artificial está integrada, universo de grande vulnerabilidade para este que é um ator de fundamental importância na economia global, o Consumidor.

CONSIDERAÇÕES FINAIS

A importância da segurança cibernética caracteriza-se cada vez mais como condição *sine qua non* de desenvolvimento, requerendo para tanto, dentre outras ações, a promoção de diálogos e de intercâmbios de ideias, de iniciativas, de dados e informações, de melhores práticas, para a cooperação no tema, no país e entre países. Entender, portanto, tais movimentos e as respectivas oportunidades e desafios são questões estratégicas que o Estado Brasileiro vem se aprimorando e se organizando para melhorar seu posicionamento tanto no nível nacional quanto, consequentemente, no que se refere à sua inserção internacional, no tema.

Chama a atenção que o denominado espaço cibernético não tem suas fronteiras ainda claramente definidas, impactando o dia a dia de todos os dirigentes governamentais, de empreendimentos privados e dos próprios cidadãos. Isso vem deixando uma grande lacuna no que se refere aos dados pessoais dos cidadãos, e principalmente na dimensão dos consumidores, que estão armazenados no mundo virtual hodiernamente.

A evolução da sociedade faz com que novos modos de vida se definam, fazendo com que adaptações sejam imprescindíveis para a perpetuação e manutenção dos seres humanos. Os tempos atuais são outros. O advento da pandemia trouxe mudanças radicais para nossa sociedade, sobretudo no que diz respeito às novas tecnologias.

A nova Era Digital da sociedade trouxe a inteligência artificial. Junto a isso, inúmeros avanços e dúvidas também vieram a esse novo desconhecido. Ao mesmo tempo em que a inteligência artificial trouxe facilidades para a economia mundial, riscos quanto aos dados pessoais das pessoas, por exemplo, também se mostram presentes nesse universo. Os dados pessoais dos consumidores, sobretudo, estão cada vez mais vulneráveis, fato este que desafia o princípio constitucional da ordem econômica da defesa do consumidor.

Trata-se de um princípio fundamental e humano, que interfere na própria dignidade da pessoa humana do consumidor. Isso porque seus dados podem ser manipulados e difundidos nas redes da internet sem o menor zelo, como preceitua a LGPD.

Uma medida para sanar essa vulnerabilidade precisa ser tomada, a fim de se garantir a proteção da privacidade dos dados dos cidadãos.

Atualmente, urge uma política comum de regras preventivas de privacidade voltada para a proteção dos dados digitais dos consumidores. Essa política pública precisa ser elaborada em prol do cumprimento do princípio da ordem econômica de defesa do consumidor. A Constituição do Brasil de 1988 precisa ser respeitada. O caso do ChatGPT ilustra a necessidade de criação dessa política preventiva na medida em que se observou a vulnerabilidade dos dados dos consumidores na criação e utilização da referida inteligência artificial.

O presente trabalho mostra, então, a necessidade de criação desse tipo de política pública voltada para a proteção de dados dos consumidores. Espera-se que a criação de regras preventivas de proteção à privacidade desses dados venha a proteger de fato os consumidores, e não seja apenas mais um conjunto de leis sem a devida execução.

Trata-se de regras, que se colocadas em prática, têm grandes chances de se tornar eficaz para a proteção dos dados digitais dos consumidores, mas que carecerá, certamente, de aperfeiçoamento constante em virtude dos avanços tecnológicos da sociedade.

Existindo uma política pública de regras preventivas de proteção dos dados pessoais digitais do cidadão, na dimensão dos consumidores, para a garantia do princípio constitucional econômico da defesa do consumidor, haverá o devido acompanhamento a proteção que se clama aqui neste estudo.

REFERÊNCIAS

ALMEIDA, Eduardo Costa; TORREÃO, Renan Palhares. **ANPD, em estruturação**, Disponível em <<https://torreaobraz.com.br/anpd-em-estruturacao-ja-recebeu-indicacoes-para-composicao-doconselho-diretor-e-do-conselho-nacional-de-protecao-de-dados-pessoais-e-da-privacidade/>>. Acesso em: 26 mar. 2022.

ANPD. **Vazamento de Dados**. 2020. Disponível em: <[www. https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf](https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf)>. Acesso em: Jun. 2023.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo**. 8. ed. São Paulo: Saraiva Educação, 2019.

BAUMAN, Zygmunt. **Vida para o Consumo**. São Paulo: Zahar, 2007.

_____, Zygmunt. **Modernidade Líquida**. São Paulo: Zahar, 2021.

BENTES, Anna. **Privacidade, Proteção de Dados e Capitalismo de Vigilância** <https://lavits.org/privacidade-protecao-de-dados-e-capitalismo-de-vigilancia-anna-bentes-ao-etc-ufma/> - Entrevista a Lavits em 04/11/2022. Anna Bentes Professora da FGV ECMI | Doutora em Comunicação e Cultura UFRJ | PhD in Communication and Culture.

_____, Anna. **Quase um tique. Economia da Atenção Vigilância, e Espetáculo em uma Rede Social**, https://pantheon.ufrj.br/bitstream/11422/16510/1/quase-um-tique_2020.pdf - @editoraufRJ, acessado em 22/04/2023.

BERCOVICI, G. **Constituição Econômica e Desenvolvimento**. São Paulo: Malheiros, 2005.

BIONI, Bruno Ricardo. **Regulação e Proteção de Dados Pessoais: o princípio da accountability**. São Paulo: Forense, 2022.

BRASIL. Planalto. **Constituição Federativa do Brasil (1988). Código do Consumidor. Lei de Acesso à Informação. Marco Civil da Internet. Lei Geral de Proteção de Dados**. Emenda Constitucional nº 115. Disponível em: <[www. https://planalto.org.br](https://planalto.org.br)>. Acesso em: maio. 2023.

_____. Lei Nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**.

https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm#:~:text=LEI%20N%C2%BA%208.078%2C%20DE%2011%20DE%20SETEMBRO%20DE%201990.&text=Disp%C3%B5e%20sobre%20a%20prote%C3%A7%C3%A3o%20do%20consumidor%20e%20d%C3%A1%20outras%20provid%C3%AAs. Acesso em: 26.06.2023

_____. Lei 10.406, de 10 de janeiro de 2002. Institui o **Código Civil**. Diário Oficial da República Federativa do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/2002/110406.htm>. Acesso em: 26.06.2023

_____. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais** e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> . Acesso em: 26.06.2023

_____. **Legislação Informatizada - Decreto nº 70.370, de 5 de Abril de 1972** - Publicação Original, <https://www2.camara.leg.br/legin/fed/decret/1970-1979/decreto-70370-5-abril1972-418827-publicacaooriginal-1-pe.html>, acessado em 24/maio/2023

BRASILEIRO, Eduardo T. Quarta Revolução Industrial e Direito do Trabalho. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2022. E-book. ISBN 9786556276113. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786556276113/>. Acesso em: 25 jul. 2023.

BURCH, Sally. **Sociedade da Informação/Sociedade do Conhecimento**. In: AMBROSI, Alain; PEUGEOT, Valérie; PIMIENTA, Daniel. Desafios das Palavras: enfoques multiculturais das sociedades da informação. 2005. Disponível em: <<https://www.cin.ufpe.br/~cjgf/SOCIETY/Sociedade%20da%20informacao%20e%20o%20Conhecimento%20-%20Sally%20Burch.pdf>>. Acesso em: maio 2023.

CAPIBERIBE, Denise de Araújo. **O Princípio da Boa-Fé Objetiva e sua Evolução Doutrinária e Jurisprudencial ao Longo dos 10 Anos de Edição do Novo Código Civil**. Disponível em: https://www.emerj.tjrj.jus.br/serieaperfeicoamentodemagistrados/paginas/series/13/volumel/10anosdocodigocivil_117.pdf

CARVALHO, Diógenes Faria de; FERREIRA Vitor Hugo do Amaral. **Defesa do consumidor ganha com a nova lei de proteção de dados pessoais**, 2018, <https://www.conjur.com.br/2018-ago-15/garantias-consumo-defesa-consumidor-ganha-lei-protecao-dados>, maio 2023.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A Trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**, <https://www.cos.ufrj.br/uploadfile/1430748034.pdf> acessado em 22/04/2023.

CARVALHOSA, Modesto. **Direito Econômico**. São Paulo: RT, 2013.

CASA Civil da Presidência da República. **Guia da Política de Governança Pública**. 2018. Brasília. Disponível em: < <https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/downloads/guia-da-politica-de-governanca-publica#:~:text=Assim%2C%20de%20forma%20mais%20objetiva,alinhados%20aos>

%20interesses%20da%20sociedade.>. Acesso em: jun. 2023.

CLARK, Giovani. Política Econômica e Estado. **Dossiê Nação/Nacionalismo**. 2008. Disponível em: <

DIAS, Reinaldo; MATOS, Fernanda. **Políticas Públicas: princípios, propósitos e processo**. São Paulo: Atlas, 2012.

DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. 3.ed. São Paulo: Revista dos Tribunais, 2021.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. Revista Espaço Jurídico, Joaçaba, v. 12, n. 2, jul./dez. 2001. Disponível em: <https://www.researchgate.net/publication/277241112_A_protecao_dos_dados_pessoais_como_um_direito_fundamental>. Acesso em: Jun. 2023.

DRUCKER, P. **Desafios gerenciais para o Século XXI**. São Paulo: Pioneira, 1999

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Curso de direito civil: parte geral e LINDB**. 13. ed. São Paulo: Atlas, 2015. v. 1.

FERREIRA, Daniela Assis Alves; PINHEIRO, Marta Macedo Kerr; MARQUES, Rodrigo Moreno. **Privacidade e Proteção de Dados Pessoais: perspectiva histórica**. Revistas USP. 2022. Disponível em: <www.revistas.usp.br>. Acesso em: maio 2023.

FERREIRA FILHO, Manoel Gonçalves. **Manual de Direito Constitucional**. 2.ed. São Paulo: Juspodvim, 2022

GATINFOSEC. **Vazamento de Dados**. Disponível em: <<https://www.gatinfosec.com/blog/vazamento-de-dados/>>. Acesso em: jun. 2023.

GÓIS, Veruska Sayonara de. **A Lei de Compliance e sua Configuração Enquanto Política Pública Regulatória** para o Setor Privado Brasileiro. Tribunal de Contas do Ceará. **Revista Controle**. v. 12, n. 2, p. 98–117, jul./dez., 2014. Disponível em: <unirioja.es>. Acesso em: Maio 2023.

GONÇALVES Iria. **Defesa do Consumidor na Cidade Medieval os Produtos Alimentares (Lisboa séculos XIV e XV)**, 1995, Universidade dos Açores, Repositório da Universidade dos Açores, Comunidades & Coleções, ARQUIPÉLAGO - Revista da Universidade dos Açores, ARQ - História, 2ª série, ARQ - Hist2s - Vol 01 - N 1 - Estudos Gerais (1995).

GRAU, Eros Roberto. **A ordem econômica na Constituição de 1988:** (Interpretação e crítica. 19. Ed. Atual. – São Paulo: Malheiros, 2018.

GRINOVER, Ada Pellegrini; OLIVEIRA FILHO, Vicente Gomes de; BRAGA, João Ferreira. **Código Brasileiro de Defesa do Consumidor.** 13.ed. São Paulo: Forense, 2022.

INÁCIO, Hillary Christine Piedade. **Novas tecnologias e o trabalho 4.0: a face cruel e precária da nova era digital.** Revista eletrônica do Tribunal Regional do Trabalho da Bahia, Salvador, v. 9, n. 13, p. 25-39, mai.2021. Disponível em: <www.juslaboris.tst.jus.br>. Acesso em: maio 2023.

LAVITS, pelo mundo. <http://dadospessoais.lavits.org/historico-pelo-mundo/#:~:text=A%20Lei%20de%20Hesse%20tem,consentimento%20do%20titular%20dos%20dados>. Acessado em 22/04/2023

LINS, Bernardo Felipe Estellita, **A evolução da Internet: uma perspectiva histórica,** Artigos & Ensaios, Cadernos ASLEGIS | 48 • janeiro/abril • 2013

LOCKE, John. **Segundo tratado sobre o governo civil:** ensaio sobre a origem, os limites e os fins verdadeiros do governo. Petrópolis: Vozes, 1999.

MACHADO, Joana de Moraes Souza. **A Expansão do Conceito de Privacidade e a Evolução na Tecnologia de Informação com o Surgimento dos Bancos de Dados.** 2014. **Revista da Ajuris.** Disponível em: <<http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/viewFile/206/142>>. Acesso em: Maio 2023.

MANDARINO JR., Raphael; CANONGIA, Raphael. Livro **Verde: segurança cibernética no Brasil.** Brasília: GSIPR/SE/DSIC, 2010. Disponível em: <https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf>. Acesso em: jun. 2023.

MANZI, Vanessa Alessi. **Compliance no Brasil:** consolidação e perspectivas. São Paulo: Ed. Saint Paul, 2008.

MARQUES, Claudia Lima; BENJAMIN, Antonio Herman V.; MIRAGEM, Bruno. **Comentários ao Código de Defesa do Consumidor.** 7. ed. (4. ed. do e-book) São Paulo: Revista dos Tribunais, Thomson Reuters Brasil, 2021.

MARQUES, Mariana. **Sociedade de Consumo na Era da Informação.** 2022. Disponível em: <[www. https://ufop.br/noticias/em-discussao/sociedade-do-consumo-na-era-da-informacao](https://ufop.br/noticias/em-discussao/sociedade-do-consumo-na-era-da-informacao)>. Acesso em: maio 2023.

MATOS, Tiago Farina, 2005, **Comércio de dados pessoais, privacidade e Internet,** BDJUR, Revista de Doutrina da 4ª Região, TRF4.

MENDES, Laura S. Série IDP - **Linha de pesquisa acadêmica - Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**, 1ª Edição. Editora Saraiva, 2014. E-book. ISBN 9788502218987. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9788502218987/>. Acesso em: 07 mai. 2023.

MILLS, Jon L. **Privacy: the lost right**. New York: Oxford University Press. Kindle Editions, Ebook, 2008.

MILTON SANTOS. *A Natureza do Espaço: técnica e tempo*. São Paulo: Hucitec, 2008

MORAES, Alexandre de. **Direito Constitucional**. 36. ed. São Paulo: Atlas, 2020.

NEVES, Júlia. **Indústria 5.0: o que é, características e impactos**, 28 de junho de 2023, <https://www.oitchau.com.br/blog/industria-5-0/#:~:text=O%20principal%20prop%C3%B3sito%20da%20quinta,voltados%20para%20as%20suas%20necessidades>. Acessado em 25 de julho de 2023.

NOVELINO, Marcelo. **Curso de Direito Constitucional**. 11. ed. Salvador: Ed. JusPodivm, 2016

OLIVEIRA, Fabiane Araújo de. **Perfil dos dados pessoais na Constituição da República de 1988 e suas repercussões nas atividades econômicas**. 2021. Disponível em: <<https://repositorio.ufrn.br/handle/123456789/46518>>. Acesso em: Maio 2023.

ONU. **Declaração Universal de Direitos do Humanos**. 1948. Disponível em: <<https://onu.org.br>>. Acesso em: Maio 2023.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais: comentários à Lei 13.709/2018 LGPD**. 4.ed. São Paulo: Saraiva, 2023.

PINTO, Alexandre Guimarães Gavião. Os Princípios mais Relevantes do Direito Administrativo. **Revista da EMERJ**, v. 11, nº 42, 2008. Disponível em: <www.https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista42/Revista42_130.pdf>. Acesso em: Jun. 2023.

RAMALHO, Francisco Rodolfo Xavier; RIGO, Ariádne Scalfoni; GRANGEIRO, Rebeca da Rocha. Gig economy e on-demand economy: **flexibilização das relações de trabalho na economia do compartilhamento**. Revista Interface UFRN, v. 17, n. 1, p. 21-40, jan/jul. 2020. Disponível em: <www.ojs.ccsa.ufrn.br>. Acesso em: maio 2023.

ROBL FILHO, Iton Norberto, **Direito Intimidade e Vida Privada: Uma perspectiva histórico-política para uma delimitação contemporânea**, Biblioteca Digital de Periódico, da Universidade Federal do Paraná, REC Revista Eletrônica do Cejur, 2006, p. 185-186, <https://revistas.ufpr.br/cejur/article/view/14841/9962>, acessado em

16/05/2023.

RUSSELL, Stuart; NORVIG, Peter. **Inteligência Artificial**. 3.ed. Recife: UFPE, 2013.

SANTOS, Vinícius Pereira dos. Código de Defesa do Consumidor: proteção do consumidor digital internacional. 2020. **Revistas FIBBauru**. Disponível em: <www.revistasfibbauru.br>. Acesso em: Jun. 2023.

SARLET, Ingo Wolfgang. **A Eficácia dos Direitos Fundamentais**. Porto Alegre: Livraria do Advogado, 1998.

SARLET, Ingo W.; SARLET, Gabrielle B S.; BITTAR, Eduardo C B. **Inteligência artificial, proteção de dados pessoais e responsabilidade na era digital**. [Digite o Local da Editora]: Editora Saraiva, 2022. *E-book*. ISBN 9786555599527. Disponível em: <https://app.minhabiblioteca.com.br/#/books/9786555599527/>. Acesso em: 24 jul. 2023.

SAYEG, Ricardo Hasson. **O Contexto Histórico da Defesa do Consumidor em face do Abuso de Poder Econômico e sua Importância**. 2004. Disponível em: <<https://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:2004;1000700709>>. Acesso em: Maio 2023.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016.

SERPRO. **Quem vai Regular e Fiscalizar a LGPD?** Disponível em: <<https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>>. Acesso em: Jun. 2023.

SILVA, Bruno. **229 bilhões de registros foram expostos em 2022 e Brasil lidera ranking de vazamentos**. Disponível em: <https://www.securityreport.com.br/229-bilhoes-de-registros-foram-expostos-em-2022-e-brasil-lidera-ranking-de-vazamentos/#:~:text=De%20acordo%20com%20levantamento%20da,prote%C3%A7%C3%A3o%20dos%20bancos%20de%20dados>>. Acesso em: Jun. 2023.

SOUZA, Washington Peluso Albino de. **Direito Econômico**. São Paulo: Saraiva, 1980

SPITZCOVSKY, Celso; LENZA, Pedro. **Direito Administrativo**. 5.ed. São Paulo: Saraiva, 2023

SZUPSZYNSKI, Vanessa Del Rio. **Direito à Ação Afirmativa**. São Paulo: LTR, 2014.

TAVARES, André Ramos; GAMA, Marina Faraco Lacerda. **O STF e a Constituição Econômica: casos e funções**. São Paulo: Intersaberes, 2022.

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. Disponível em:

<https://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ii%204.pdf?d=636680444556135606>. Acesso: Julho, 2023

TCU. Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública. 3.ed. 2020. Disponível em: <<https://portal.tcu.gov.br>>. Acesso em: jun. 2023.

TCU. **Política Pública em Dez Passos.** Disponível em: <https://portal.tcu.gov.br>

https://portal.tcu.gov.br/data/files/1E/D0/D4/DF/12F99710D5C6CE87F18818A8/Politica%20Publica%20em%20Dez%20Passos_web.pdf Acessado em: agosto, 2023.

THORNHILL, Chris. A sociology of constituent power: the political code of transnational societal constitutions". Indiana **Journal of Global Legal Studies**, 20: 551-603. 2013.

TOMASEVICIUS FILHO, Eduardo; FALEIROS JÚNIOR, José Luiz de Moura; DALESE, Pedro. **GDPR: Regulamento Geral sobre a Proteção de Dados da União Europeia.** São Paulo: Foco, 2023.

TOLEDO SILVEIRA, Cláudia Maria Toledo. **Direito Econômico e Cidadania.** 1997.

Disponível em: <

http://www.dhnet.org.br/direitos/sos/textos/silveira_dir_ec_cidadania.htm>. Acesso em: set. 2022.

ULEN, Thomas; COOTER, Robert. Direito e Economia. Porto Alegre: Bookman, 2010.

WENTZEL, Marina. **“Quarta revolução industrial”: Como o Brasil pode se**

preparar para a economia do futuro. 22 janeiro 2016, De Basileia(Suíça) para a BBC Brasil.

https://www.bbc.com/portuguese/noticias/2016/01/160122_quarta_revolucao_industrial_mw_ab. Acesso em: agosto, 2023

ZANON JR., Orlando Luiz. Moral, Ética e Direito. **REVISTA DA ESMESC**, v. 21, n. 27, 2014. Disponível em: <<https://revista.esmesc.org.br>>. Acesso em: jun. 2023.