



**UNIVERSIDADE DO SUL DE SANTA CATARINA
MAHARA CHAVES DE LIMA**

**O RECONHECIMENTO FACIAL E A COLETA DE DADOS PARA FINS DE
CONSUMO: UM ESTUDO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS
(LGPD)**

Florianópolis

2023

MAHARA CHAVES DE LIMA

**O RECONHECIMENTO FACIAL E A COLETA DE DADOS PARA FINS DE
CONSUMO: UM ESTUDO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS
(LGPD)**

Trabalho de Conclusão de Curso apresentado ao
Curso de Graduação em Direito, da
Universidade do Sul de Santa Catarina, como
requisito parcial para obtenção do título de
Bacharel em Direito.

Orientador: Prof. Demetrius Nichele Macei.

Florianópolis
2023

MAHARA CHAVES DE LIMA

**O RECONHECIMENTO FACIAL E A COLETA DE DADOS PARA FINS DE
CONSUMO: UM ESTUDO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS
(LGPD)**

Este Trabalho de Conclusão de Curso foi julgado adequado à obtenção do título de Bacharel em Direito e aprovado em sua forma final pelo Curso de Graduação em Direito, da Universidade do Sul de Santa Catarina.

Florianópolis, 26 de novembro de 2023.

Prof. Orientador Demetrius Nichele Macei
Universidade do Sul de Santa Catarina

Prof. Nome do Professor, titulação
Universidade do Sul de Santa Catarina

Prof. Nome do Professor, titulação
Universidade do Sul de Santa Catarina

TERMO DE ISENÇÃO DE RESPONSABILIDADE

O RECONHECIMENTO FACIAL E A COLETA DE DADOS PARA FINS DE CONSUMO: UM ESTUDO À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico e referencial conferido ao presente trabalho, isentando a Universidade do Sul de Santa Catarina, a Coordenação do Curso de Direito, a Banca Examinadora e o Orientador de todo e qualquer reflexo acerca deste Trabalho de Conclusão de Curso.

Estou ciente de que poderei responder administrativa, civil e criminalmente em caso de plágio comprovado do trabalho monográfico.

Florianópolis, 26 de novembro de 2023.

 Documento assinado digitalmente
MAHARA CHAVES DE LIMA
Data: 09/11/2023 09:35:45-0300
Verifique em <https://validar.iti.gov.br>

MAHARA CHAVES DE LIMA

Dedico o presente trabalho em especial a minha família, que sempre sonharam junto comigo esse sonho, sempre acreditaram, incentivaram e apoiaram a minha jornada acadêmica, também à DEUS por permitir que eu esteja vivendo esse momento único e que eu pudesse desenvolver com muito amor e dedicação a produção dessa monografia.

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão a todas as pessoas que contribuíram para a realização deste trabalho de conclusão de curso. Em primeiro lugar, agradeço aos meus amigos e familiares, que estiveram ao meu lado em todos os momentos, me apoiando, incentivando e compreendendo a importância deste projeto. Seu amor, compreensão e encorajamento foram essenciais para que eu pudesse superar os desafios e alcançar meus objetivos. Agradeço também ao meu orientador/professor Demetrius Nichele Macei, pelo apoio, orientação e paciência ao longo deste processo.

A ajuda e o apoio de cada um, este trabalho não seria possível. Que este seja apenas o começo de uma jornada contínua em busca de conhecimento e crescimento. Muito obrigada!

“Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível” (CHARLES CHAPLIN, 1920).

RESUMO

O reconhecimento facial e a coleta de dados para fins de consumo são temas de grande relevância no contexto atual, especialmente no que diz respeito à proteção de dados. O objetivo desta monografia é verificar se o reconhecimento facial para fins comerciais é compatível com os preceitos da LGPD. Pretende-se, também, analisar como esses direitos são aplicados no âmbito do direito digital, à luz da legislação nacional. A pesquisa adota uma abordagem dedutiva, utilizando um método monográfico qualitativo, baseado em referências bibliográficas e documentos relevantes. Busca-se compreender os principais tópicos relacionados aos elementos da relação de consumo, ao direito digital e ao reconhecimento facial, a fim de verificar se a proteção de dados pessoais por meio do reconhecimento facial em estabelecimentos comerciais durante transações de compra e venda pode ser considerada segura, ou seja, se ela respeita de fato a LGPD. Diante desses termos, o estudo concentra-se no direito digital e na aplicação do reconhecimento facial dentro da Lei Geral de Proteção de Dados (LGPD), que ainda é um assunto amplamente discutido e debatido no meio jurídico. No entanto, esta pesquisa conclui que, mesmo havendo debates em relação ao tema, a coleta de dados pessoais para fins de consumo é uma tendência em constante crescimento, embora seja um avanço que deve ser tratado com cautela.

Palavras-chave: Relação de Consumo, Reconhecimento Facial, Proteção de dados.

SUMÁRIO

1	INTRODUÇÃO.....	9
2	ASPECTOS DESTACADOS DA TUTELA DA RELAÇÃO DE CONSUMO NO ORDENAMENTO JURÍDICO BRASILEIRO.....	11
2.1	UM HISTÓRICO DO DIREITO DO CONSUMIDOR.....	11
2.2	OS ELEMENTOS DA RELAÇÃO DE CONSUMO.....	13
2.2.1	O Consumidor.....	14
2.2.1.1	O consumidor standard.....	15
2.2.1.2	O consumidor por equiparação.....	16
2.2.2	O fornecedor.....	18
2.2.3	O produto.....	19
2.2.4	O serviço.....	20
2.3	OS PRINCÍPIOS CONSUMERISTAS.....	21
2.3.1	O princípio da vulnerabilidade.....	21
2.3.2	Princípio da informação adequada.....	22
2.3.3	Princípio da boa fé.....	24
2.3.4	Princípio da transparência.....	25
2.3.5	O princípio da confiança.....	27
2.3.6	Princípio da equidade ou princípio do equilíbrio contratual absoluto.....	27
2.4	OS DIREITOS BÁSICOS DO CONSUMIDOR.....	28
3	O RECONHECIMENTO FACIAL E A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO.....	31
3.1	O DIREITO DIGITAL E O SURGIMENTO DO RECONHECIMENTO FACIAL.....	31
3.2	OS MÉTODOS DO RECONHECIMENTO FACIAL.....	36
3.3	O USO E AS APLICAÇÕES DO RECONHECIMENTO FACIAL.....	37
3.4	A TUTELA DO RECONHECIMENTO FACIAL NO BRASIL.....	38
3.5	O RECONHECIMENTO FACIAL PARA FINS DE CONSUMO.....	39
3.6	A PROTEÇÃO DOS DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO.....	40
3.6.1	Um histórico da proteção de dados no brasil.....	41
3.6.2	O surgimento da lei geral de proteção de dados (LGPD).....	43

3.6.3 Os princípios inerentes a lei geral de proteção de dados (LGPD).....	44
3.6.4 A estrutura da lei geral de proteção de dados (LGPD).....	46
3.6.4.1 Os dados pessoais.....	47
3.6.4.2 Os sujeitos e os órgãos na lei geral de proteção de dados.....	49
3.6.2.3 As ações.....	50
3.2.3.4 Os instrumentos.....	51
4. A UTILIZAÇÃO DO RECONHECIMENTO FACIAL PARA FINS DE CONSUMO E A QUESTÃO DO TRATAMENTO DA IMAGEM NA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).....	52
4.1 A IMPORTÂNCIA DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS.....	53
4.2 O RECONHECIMENTO FACIAL PARA COLETA DE DADOS PARA FINS COMERCIAIS.....	54
4.3 RECONHECIMENTO FACIAL PARA FINS COMERCIAIS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).....	57
4.4 O ENTENDIMENTO DOUTRINÁRIO ACERCA DA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PARA FINS COMERCIAIS.....	58
4.5 O ENTENDIMENTO JURISPRUDENCIAL ACERCA DA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PARA FINS COMERCIAIS.....	59
CONCLUSÃO.....	64
REFERÊNCIAS.....	66

1 INTRODUÇÃO

O presente trabalho, requisito para a conclusão e aprovação do curso de Direito na Universidade do Sul de Santa Catarina - UNISUL, tem como objetivo compreender se o reconhecimento facial para fins de consumo respeita de fato a Lei Geral de Proteção de Dados. A pesquisa foi conduzida por meio de uma abordagem bibliográfica, buscando compreender o direito dos dados coletados no Brasil.

A relevância deste estudo reside na abordagem de um tema atual e de consequências iminentes no contexto jurídico brasileiro. Com o aumento do patrimônio digital e a crescente demanda por coleta de dados para fins comerciais e de consumo, é inevitável que isso afete diversos campos do direito. A escolha do tema foi motivada pelo interesse pessoal da pesquisadora pelo Direito Digital e pelos impactos das coletas de dados no contexto jurídico.

O advento da digitalização nas últimas décadas trouxe profundas transformações e avanços em diversos modelos de consumo. O reconhecimento facial tornou-se uma realidade em nosso país, e as pesquisas sobre o assunto têm se tornado cada vez mais frequentes para compreender esse universo que envolve o direito digital, a coleta de dados e a LGPD, abordando diferentes perspectivas e áreas ainda pouco exploradas. Surge a problemática central desta pesquisa: será que o ordenamento jurídico brasileiro permite atualmente a coleta segura de dados para fins de consumo por meio do reconhecimento facial?

Essa pergunta aborda as peculiaridades dos ativos virtuais, principalmente em sua característica de descentralização e na forma como são mantidos pelos titulares. Diante da iminente chegada dessas demandas ao Poder Judiciário e da necessidade de nos prepararmos para lidar com elas, fica evidente a pertinência e atualidade do tema, cujo estudo busca a convergência entre o tradicional direito digital e a recente coleta de dados por meio do reconhecimento facial.

A estrutura da monografia é composta por cinco seções: introdução, três capítulos de desenvolvimento e conclusão. O primeiro capítulo visa compreender o histórico, os elementos e os princípios da relação de consumo, por meio da exposição dos principais conceitos e formas de coleta de dados.

O segundo capítulo tem como objetivo identificar e compreender o surgimento do direito digital e do reconhecimento facial, analisando seus métodos, aplicação e reflexos no

mundo jurídico, bem como sua conexão com a evolução da informação e sua introdução no direito digital. O terceiro capítulo abordará a utilização do reconhecimento facial para fins de consumo no ordenamento jurídico brasileiro, considerando o entendimento doutrinário e jurisprudencial e as leis relacionadas à relação de consumo.

2 ASPECTOS DESTACADOS DA TUTELA DA RELAÇÃO DE CONSUMO NO ORDENAMENTO JURÍDICO BRASILEIRO

Neste primeiro capítulo será apresentada uma breve análise acerca da história do direito do consumidor, seus direitos e garantias que são assegurados pela Lei nº 8.078/1990, um assunto que é de bastante importância e preocupação pelos legisladores em razão ao tema inovador na sociedade. Ainda ao tratar dessa questão, mesmo as pessoas sabendo que a Lei Geral de Proteção de Dados nº 13.709/2018 é atual no Brasil, a preocupação com a coleta dos dados pessoais já é antiga em outros países.

Cabe registrar que o Código de Defesa do Consumidor possui uma série de dispositivos legais que visam equilibrar a relação entre consumidores e fornecedores, garantindo a proteção dos direitos dos consumidores e promovendo a transparência e a boa-fé nas relações de consumo. Alguns aspectos importantes destacados no CDC, assim como de proteção contratual ao consumidor, introduzindo a teoria da imprevisão, a responsabilidade pelo fato do produto ou do serviço, as cláusulas abusivas dentre outros (MACIEL, 2019).

2.1 UM HISTÓRICO DO DIREITO DO CONSUMIDOR

Para dar início ao alusivo assunto, é importante destacar a história do homem que é marcada por esforços, conflitos, discrepâncias, na luta pela construção e desconstrução de processos com o objetivo de sobrevivência de forma pessoal para mais adiante ter o retorno ao meio social e coletivo. Por tais razões, para reduzir com as diferenças o direito contemporâneo tem apresentado soluções para equilibrar as relações econômicas por meio de normas jurídicas, no intuito de proteger a pessoa vulnerável na relação (MIRAGEM, 2016, p. 40).

Ainda na perspectiva de Miragem (2016, p. 40):

O paradigma individualista, sobretudo no direito privado, cede espaço a novos interesses igualmente reconhecidos pelo Estado, cuja intervenção em favor do sujeito reconhecido como vulnerável tem por objetivo a recomposição da igualdade jurídica, corrigindo os elementos fáticos de desigualdade.

Por tais aspectos, na era antiga as pessoas estavam sempre comprando ou vendendo algo para garantir seu sustento. Como se depreende, os primeiros movimentos dos consumeristas ocorreram nos EUA na década de 1960, surgindo a necessidade de regularizar

o mercado de consumo. Para isso o Presidente Kennedy enviou uma mensagem Especial ao Congresso dos Estados Unidos (SOUZA, 2018, p.06), conforme relata Souza (2018, p .06):

Coube a louvável iniciativa ao Presidente Kennedy, em sua inesquecível Mensagem Especial ao Congresso dos Estados Unidos sobre a Proteção dos Interesses dos Consumidores, de 15 de março de 1962, na qual afirmou que os consumidores constituíam o mais importante grupo econômico e o único não efetivamente organizado, enunciando, a seguir, e de maneira sintética, os seus direitos básicos, que dizem respeito à saúde, à segurança, à informação, à escolha e a serem ouvidos.

Por essa razão a data de 15 de março se consagrou como o Dia Nacional dos Direitos dos Consumidores (SOUZA, 2018, p. 06).

Sobre a proteção dos interesses dos consumidores pelo então Presidente John Fitzgerald Kennedy, Cavalieri (2011, p. 05), traz:

Consumidores, por definição, somos todos nós. Os consumidores são o maior grupo econômico na economia, afetando e sendo afetado por quase todas as decisões econômicas, públicas e privadas [...]. Mas são o único grupo importante da economia não eficazmente organizado e cujos posicionamentos quase nunca são ouvidos.

Cabe registrar que a Comissão de Direitos Humanos das Nações Unidas, em 1973 reconheceu os direitos básicos, como à dignidade humana, à integridade física, à honra e tantos outros direitos. No mesmo ano foi criada a Carta de Proteção do Consumidor, por meio da Assembleia Consultativa do Conselho da Europa, utilizada como suporte para a Resolução do Conselho da Comunidade Europeia (CAVALIERI FILHO, 2011,p.06).

Nesse passo, as primeiras leis de proteção do consumidor surgiram na França, sendo elas a Lei 22/12/1972 que concede período de 7 dias para pensar sobre a compra, a Lei 27/12/1973 da proteção do consumidor sobre a propaganda enganosa e as Leis 7.822 e 23 10/01/1978 de proteção aos consumidores contra crédito e cláusulas excessivas (CAVALIERI FILHO, 2011, p. 07).

No entanto, em 1988, com o rompimento do movimento absolutista de governo e o renascimento da democracia, surgiu no ordenamento jurídico o dever do Estado de garantir a defesa do consumidor, prevista no rol de direitos e garantias fundamentais do artigo 5º, inciso XXXII da Constituição Federal de 1988 (NUNES, 2021; SOUZA, 2018).

Assim, pela primeira vez desde o início da industrialização no Brasil (1960) houve o reconhecimento do direito do consumidor e com ele a precisão de desenvolver uma

legislação própria, para solucionar conflitos das relações de consumo de forma correta e transparente entre as partes (CAVALIERI FILHO, 2022; KHOURI, 2020).

2.2 OS ELEMENTOS DA RELAÇÃO DE CONSUMO

Cabe destacar que os elementos da relação de consumo se classificam em elementos subjetivos, que são os sujeitos dessa relação jurídica e objetivos, relacionados ao objeto das prestações ali sugeridas, estes elementos estão relacionados entre consumidor e fornecedor de um produto/serviço (CAVALIERI FILHO, 2018, p. 94).

Leciona Cavalieri (2018, p. 94), “Impõe-se observar que o legislador preferiu definir os elementos da relação de consumo, na esperança de, assim, contribuir para a melhor compreensão da lei e de seu campo de incidência, o que é de ser louvado”.

Complementa ainda Cavalieri (2018) “Nada obstante o seu esforço, doutrina e jurisprudência durante longo tempo não se harmonizaram sobre a questão, mormente no que se refere ao conceito jurídico de consumidor, ora por se pretender alargar, ora por se pretender restringir, o campo de incidência da Lei nº 8.078/90 que, por certo, está relacionado com a exata identificação do destinatário da proteção jurídica”.

À vista desse panorama, Marques (2012, P.67-107) explica sobre a relação de consumo e como é composta por quatro elementos básicos sendo eles fornecedor, consumidor, produto e serviço. A presença simultânea dentre esses quatro elementos é fundamental para a configuração da relação de consumo e também para a aplicação do CDC.

Como observa Khouri (2020), a relação de consumo é constituída por um elemento subjetivo ligado ao consumidor e fornecedor e também um teleológico junto à finalidade do serviço objeto da relação ou do bem.

Por oportuno saliente-se que o entendimento do autor é que no fim da relação consumerista o importante é que o objeto, tendo em vista a destinação dada pelo adquirente é quem definirá se a relação de consumo está ou não protegida pelo CDC (KHOURI, 2020).

2.2.1 O Consumidor

Nota-se, portanto, que o Código de Defesa do Consumidor de 1990 em seu art. 2º define o consumidor (BRASIL, 1990), como: “Consumidor é toda a pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final”.

Diante desse pressuposto, Cavalieri (2011 *apud* ALMEIDA, 2006, p.61) esclarece sobre a definição do consumidor de acordo com o CDC:

Pela definição legal de consumidor, basta que ele seja o ‘destinatário final’ dos produtos ou serviços (CDC art. 2º), incluindo aí não apenas aquilo que é adquirido ou utilizado para o uso pessoal, familiar ou doméstico, mas também o que é adquirido para o desempenho de atividade ou profissão, bastando, para tanto, que não haja a finalidade de revenda. O advogado que adquire livros jurídicos para bem desempenhar sua profissão é, sem dúvida, destinatário final dessa aquisição, e, como tal, consumidor segundo a definição legal. Não há razão plausível para que se distinga o uso privado do profissional; mais importante, no caso, é a ausência de finalidade de intermediação ou revenda.

Neste sentido Cavalieri Filho explica que “O conceito de consumidor, na esteira do finalismo, portanto, restringe-se, em princípio às pessoas físicas ou jurídicas, não profissionais, que não visam lucro em suas atividades e que contratam com profissionais. Prossegue o autor: “Entende-se que não se há falar em consumo final, mas intermediário, quando um profissional adquire produto ou usufrui de serviço com o fim de direta ou indiretamente, dinamizar ou instrumentalizar seu próprio negócio lucrativo” (CAVALIERI FILHO, 2011, p. 62).

Na mesma linha, relata Souza (2018) “Será muito fácil perceber que o núcleo central da definição é a referência restritiva a destinatário final”. Complementa ainda que “Como frequentemente acontece, no mundo jurídico, as definições nem sempre espancam as dúvidas, e podem até mesmo transformá-las em perplexidades, já que dependem das convicções filosóficas, políticas ou doutrinárias de cada definidor” (SOUZA, 2018, p. 23).

Deste modo, aponta o autor a origem de duas correntes distintas, conhecidas como teorias maximalista ou objetiva e finalista ou subjetiva (SOUZA, 2018, p. 23).

Na perspectiva de Cavalieri Filho (2011, p. 60):

A corrente maximalista ou objetiva entende que o CDC, ao definir o consumidor, apenas exige, para sua caracterização, a realização de um ato de consumo. A expressão destinatário final, pois, deve ser interpretada de forma ampla, bastando à configuração do consumidor que a pessoa, física ou jurídica, se apresente como destinatário fático do bem ou serviço, isto é, que o retire do mercado, encerrando objetivamente a cadeia produtiva em que inseridos o fornecimento do bem ou a prestação do serviço.

Nesse contexto, cita Filomeno (2018), “Já para o conceito objetivo ou maximalista, basta o ato de consumo, com a destinação final fática do produto ou serviço para alguém, que será considerado consumidor destes, pouco importando se a necessidade a ser suprida é de natureza pessoal ou profissional”. Procede ainda José Geraldo B. Filomeno, “Sob tal perspectiva, o caminhão comprado com o intuito de auxiliar no transporte de mercadorias de uma empresa atinge, nessa atividade, sua destinação final, uma vez que não será objeto de transformação ou beneficiamento” (FILOMENO, 2018, p. 19).

Importante destacar que a teoria finalista ou subjetivista para Cavalieri Filho (2022):

A corrente finalista ou subjetivista, por seu turno, interpreta de maneira restritiva a expressão destinatário final [...] Só merece a tutela do CDC aquele que é vulnerável. Entende ser imprescindível à conceituação de consumidor que a destinação final seja entendida como econômica, isto é, que a aquisição de um bem ou a utilização de um serviço satisfaça uma necessidade pessoal do adquirente ou utente, pessoa física ou jurídica, e não objetive o desenvolvimento de outra atividade negocial (CAVALIERI FILHO, 2022, p. 95).

Dessa feita, conclui Souza (2018, p. 24), “Já a corrente finalista ou subjetivista só considera destinatário final aquele que é vulnerável, não objetivando o exercício de outra atividade profissional lucrativa”.

2.2.1.1 O consumidor *standard*

Consoante o que fora visto no tópico sobre consumidor (art. 2º do CDC), o consumidor *standard* é o destinatário final, via de regra se considera consumidor o que recebe como leigo, aquele que não é profissional e recebe produto ou serviço de um profissional, dessa forma sendo caracterizado como consumidor vulnerável (MIRAGEM, 2016, p. 156).

Nessa linha, Tartuce (2021, p. 96), diz que:

São, pois, equiparados ao consumidor *standard*: a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo (parágrafo único do art. 2º), todas as vítimas do evento (art. 17) e todas as pessoas, determináveis ou não, expostas às práticas nele previstas (art. 29).

Muito antes da Lei n.º 8.078, de 11 de setembro de 1990, que instituiu o Código de Defesa do Consumidor, existem debates que exploram o consumidor como sujeito vulnerável e hipossuficiente na relação de consumo. Isso porque o consumidor não dispõe de controle sobre os bens de produção e em consequência disto submete-se ao poder de quem os possui. (BORGES, 2010).

Além disso, acerca do chamado destinatário final, é que surgem muitas teorias, mas duas apenas mostram-se originais estão discutidas no âmbito jurídico, essas teorias são chamadas de maximalista e finalista (SCHWARTZ, 2018 p. 28).

Em relação a teoria finalista, o consumidor é sobretudo vulnerável, tal qual se faz necessária uma interpretação do termo “destinatário final” com o interesse na finalidade do produto ou serviço (MARQUES, 2019).

Além disso, para os finalistas, o consumidor é quem retira o produto de circulação, assim como atribui uma finalidade não profissional seja de forma direta ou indireta sem visar obter lucros (MARQUES, 2019).

A teoria maximalista ou objetiva, sustenta que o CDC entende e define o consumidor apenas pela realização da prática na relação de consumo (CAVALIERI FILHO, 2011, p. 60).

No entendimento de Marques (2019), para a teoria maximalista o destinatário final é o fático, assim o consumidor pode ser pessoa física ou jurídica que vise ou não lucro.

A teoria finalista ou subjetiva é restritiva no que se diz destinatário final, considerando ser somente o vulnerável merecedor da tutela aplicável do Código de Defesa do Consumidor.

2.2.1.2 O consumidor por equiparação

Importante destacar que o consumidor é vulnerável no mercado de consumo, ele adquire ou utiliza produtos ou serviços como destinatário fático e econômico a fim de suprir as suas necessidades ou de sua família (CAVALIERI FILHO, 2011, p. 69).

E, nesse ponto, a legislação consumerista se aplica aos terceiros, ou seja, aqueles que não são consumidores, mas que assim são considerados para efeitos da tutela dentro do dispositivo do parágrafo único do art. 2º e arts. 17 e 29, todos do CDC (CAVALIERI FILHO, 2011, p. 69).

A primeira hipótese de consumidor por equiparação prevista no art. 2º, parágrafo único do CDC, que prevê “equipara-se a consumidor a coletividade de pessoas ainda que indetermináveis, haja intervindo nas relações de consumo” (BRASIL, 1990).

O dispositivo legal, traz a característica marcante da vulnerabilidade, aspecto que equipara o consumidor. Nesse passo a doutrina de Cavalieri faz a seguinte análise:

- I. A coletividade de pessoas**, ainda que indetermináveis, que haja intervindo nas relações de consumo (art. 2º, parágrafo único - *terceiros-in-tervenientes*);
- II. Todas as vítimas** do fato do produto ou serviço (art. 17- *terceiros-vítimas*);
- III. Todas as pessoas, determináveis ou não, expostas às práticas comerciais e à disciplina contratual** – neste último caso, em posição de vulnerabilidade (art. 29 – *terceiros-expostos*); (CAVALIERI FILHO, 2011, p. 70, grifo autor).

Cavaliere Filho (2011), ensina de forma inteligível:

O parágrafo único do art. 2º do Código do Consumidor estende a proteção da legislação à coletividade de pessoas, ainda que indetermináveis, que, de alguma forma, haja intervindo nas relações de consumo absorvendo bens ou serviços ou se apresentando para tais absorções. Este dispositivo afirma o caráter difuso do direito do consumidor. Tem finalidade instrumental por excelência, pois destina-se a dar eficácia, como veremos, à tutela coletiva dos direitos e interesses difusos, coletivos e individuais homogêneos estabelecidos nos arts. 81 e seguintes do CDC.

Saliente-se ainda que o art. 17 do CDC estabelece a segunda hipótese de consumidor por equiparação, onde é equiparado aos consumidores todas as vítimas do dano. A partir de então, entende-se que as vítimas do acidente do consumo são consideradas consumidoras (SILVA, 2020, p. 37).

O artigo 17 do Código de Defesa do Consumidor (CDC) estabelece que qualquer indivíduo que seja vítima de um incidente envolvendo um serviço ou produto é considerado um consumidor, conforme definido pela legislação brasileira de 1990. Esta disposição legal equipara todas as vítimas a consumidores, independentemente de sua participação direta ou indireta na transação comercial. (BRASIL, 1990).

O Código de Defesa do Consumidor em seu art. 17, dispõe sobre o consumidor por equiparação (bystander), são todos aqueles que de certa forma não tem participação direta com a relação de consumo e que venham a ser vítimas de alguma eventualidade danosa, mesmo que inexistindo relação com o contrato consumerista (THEODORO JÚNIOR, 2017, p. 30).

Essa proteção ao consumidor é chamada como proteção de terceiro ou bystander, ou seja, um terceiro alheio a relação contratual, poderá ser vítima de algum dano em relação ao produto ou serviço (MARQUES, 2019; NUNES, 2021).

Por conseguinte Nunes (2018, p. 107, 118) aborda em sua obra a importância do conceito de vulnerabilidade na definição do consumidor por equiparação. E acrescenta o art. 29 do CDC, como terceira hipótese de que todos se equiparam a consumidores, aqueles expostos a publicidades, práticas abusivas, mesmo que não tenham adquirido o produto ou o serviço. Aliás, ainda que nenhum consumidor tenha reagido contra a prática ilegal mesmo de modo a natureza de direito difuso legítima (NUNES, 2021).

2.2.2 O fornecedor

Partindo dessa premissa, o segundo elemento da relação jurídica de consumo é o fornecedor, previsto no art. 3º, *caput*, do Código de Defesa do Consumidor, que dispõe:

Art. 3º Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços (BRASIL, 1990).

Corroborando ainda, Cavalieri (2011, p.111):

Note-se que, diferentemente do que ocorre com o conceito jurídico de consumidor, o de fornecedor, constante do art. 3º, *caput*, é bastante amplo. Fornecedor é gênero – quer no que respeita ao sujeito em si (pessoa física ou jurídica; pública ou privada; nacional ou estrangeira), quer no que se refere às atividades que desenvolve – e não por acaso.

A estratégia do legislador permite considerar fornecedores todos aqueles que, mesmo sem personalidade jurídica (“entes despersonalizados”), atuam nas diversas etapas do processo produtivo (produção-transformação-distribuição-comercialização--prestação), antes da chegada do produto ou serviço ao seu destinatário final.

No entanto, Souza (2018) reporta, “ainda, o art. 3º aos entes despersonalizados, também denominados pessoas formais, e que não ostentam personalidade jurídica, embora sejam dotadas de legitimidade *ad causam* e *ad processum*, como são os exemplos da família, da massa falida, do condomínio, do espólio ou dos grupos de consórcio”. Complementa ainda que, no passado não havia título legal para responsabilizar os entes despersonalizados, o que agora se superou com a oportuna inclusão no art. 3º (SOUZA, 2018, p. 26).

Sobre as chamadas “relações de consumo”, Explica ainda Filomeno (2018):

Em vez de consignar como tal o “industrial”, ou então o “vendedor”, “prestador de serviços” ou com qualquer outro termo restritivo, cada qual dentro de uma dada concepção ligada à natureza da operação praticada, temos para nós que o termo fornecedor, tanto de bens como de serviços, seja o vocábulo mais apropriado.

A citação em questão ressalta a importância da escolha de palavras ao definir as partes envolvidas em uma transação comercial. O termo “fornecedor”, conforme sugerido, é um termo abrangente que engloba vários papéis, como “industrial”, “vendedor” ou “prestador de serviços”. Isso sugere que a escolha do termo “fornecedor” é intencional para abranger todas as possíveis entidades que fornecem bens ou serviços ao consumidor, independentemente da natureza da operação.

Sobre a definição de fornecedor, Theodoro Junior (2017), [...] afirma que, para caracterização deste é necessário “desenvolver atividades tipicamente profissionais, como a comercialização, a produção, a importação, indicando também a necessidade de uma certa habitualidade, como a transformação, a distribuição de produtos”.

Sobretudo a condição de fornecedor está diretamente ligada à atividade desenvolvida, como ipso facto, responsabilidade sobre os danos causados aos consumidores (GRINOVER et al., 2022).

Como se pode notar, a defesa do consumidor em razão da vulnerabilidade deste, frente ao fornecedor, ou seja, o consumidor sempre será o lado mais sensível da relação (CAVALIERI FILHO, 2011).

2.2.3 O produto

Um dos elementos da relação de consumo é o produto, que pode ser um determinado bem móvel, imóvel ou material que esteja no mercado de consumo (TARTUCE, 2021, p. 98).

O Código de Defesa do Consumidor, dispõe:

Art. 3º Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.

§ 1º Produto é qualquer bem, móvel ou imóvel, material ou imaterial (BRASIL, 1990).

Entretanto, Cavaliere Filho (2011), aduz que:

Em princípio, qualquer bem pode ser considerado produto, desde que resulte de atividade empresarial em série de transformação econômica. Quanto aos bens do setor primário, tal como são os de natureza agrícola, entende-se que serão incluídos sob a esfera do Código de Defesa do Consumido, desde que tenham sofrido transformação por intervenção do trabalho humano ou mecânico.

Ainda, Souza (2018) ensina que, produto é tudo o que se produz, direta ou indiretamente, resultado de um processo de fabricação, incluindo os bens de natureza agrícola, ainda que haja processo de transformação e de beneficiamento. Enfatiza, ainda o autor, “tudo o que interessa ou necessita o ser humano é para ele produto, sendo irrelevante a sua origem ou processo de produção”.

De acordo com o art. 82 do Código Civil, “são móveis os bens suscetíveis de movimento próprio, ou de remoção por força alheia, sem alteração da substância ou da destinação econômico-social”. De outra parte, “são bens imóveis o solo e tudo quanto se lhe incorporar natural ou artificialmente como estabelece o artigo 79 do referido diploma legal (BRASIL, 2022).

Considerando que os produtos mesmo que gratuitos são designados como amostra grátis. Desta forma, Nunes (2021), aduz que “estes produtos também estão submetidos às exigências de qualidade, garantia, durabilidade, proteção contra vício, defeitos”.

2.2.4 O serviço

O Código de Defesa do Consumidor em seu art. 3º § 2º, traz uma conceituação sobre tal legislação sustenta que “§ 2º Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista (BRASIL, 1990)”.

Neste contexto afirma Filomeno (2018, p. 19), [...] “são exemplos de serviços: os prestados por um electricista, encanador, pintor, coletivos de transporte, e outros tipos de transporte terrestre, aéreo, marítimo, lacustre, ferroviário, de dedetização, de turismo etc”.

Além do Código de Defesa do Consumidor estabelecer em seu art. 3º que toda a pessoa jurídica também é fornecedora sem qualquer distinção, também traz em seu art. 22 que “os órgãos públicos, por si ou suas empresas, concessionárias, permissionárias ou sob qualquer outra forma de empreendimento, são obrigados a fornecer serviços adequados, eficientes, seguros e, quanto aos essenciais, contínuos” (BRASIL, 1990).

Convém destacar por oportuno, que constitui serviço toda aquela atividade que é prestada mediante custeio por impostos, mas também são reconhecidos e se consideram como objeto da relação de consumo, as apostas e jogos de azar a fim de exploração comercial que são oferecidos no mercado (MIRAGEM, 2016,p. 188).

Mais adiante, Filomeno sustenta que (2018, p. 19), “Apesar das opiniões em sentido contrário, evidentemente externadas pelos interessados em deixar tal atividade fora do Código de Defesa do Consumidor, a verdade é que ela é, eminentemente, relação de consumo”.

O Código de Defesa do Consumidor, em sua essência, é orientado para a regulação de atividades, ao invés de se concentrar em negócios jurídicos específicos. Esta perspectiva é destacada por Souza (2018, p. 30), que sugere que o Código tem um escopo mais amplo, abrangendo uma variedade de interações comerciais e econômicas. Isso significa que o Código não se limita a regular apenas transações contratuais específicas, mas estende sua proteção a todas as atividades que possam afetar os consumidores.

De outro vértice Souza (2018, p.30), fala sobre “o objetivo perseguido pelo legislador decorre da enorme densidade social e econômica destas atividades que frequentam o dia a dia

de grande parcela da população brasileira, que delas necessita, e das quais participa, quase sempre, em situação de vulnerabilidade”.

Enfatiza ainda, Cavalieri Filho (2022, p. 114):

Para o mercado de consumo não se restringe ao fornecimento de produtos. A expansão do setor terciário na economia contemporânea é fenômeno inviolável, mormente diante da constante evolução tecnológica e das crescentes e contínuas robotização e informatização do processo produtivo. A mão de obra humana, cada vez mais, vai sendo substituída por máquinas, e, assim, migrando para o setor de serviços e para a chamada “economia informal”.

Por fim, essas atividades acima mencionadas podem ser tanto de natureza material ou financeira e podem receber remuneração direta ou indireta, ser prestadas por entidades públicas ou privadas (CAVARELI FILHO, 2022, p. 114).

2.3 OS PRINCÍPIOS CONSUMERISTAS

A propósito do tema, o CDC trouxe uma nova visão nas relações entre consumidores e fornecedores a partir de uma série de princípios consumeristas, conquanto, os que mais se destacam é o princípio da vulnerabilidade e a boa-fé objetiva (MARQUES, 2010, p. 54- 67).

2.3.1 O princípio da vulnerabilidade

Empregado, de acordo com o art. 4º, inc. I do Código de Defesa do Consumidor é visto com transparência pelo legislador em favorecer em todas as situações de vulnerabilidade na relação de consumo o consumidor (TARTUCE, 2021, p. 48).

Na visão de Souza (2018, p. 14):

Tanto isto é verdade que no artigo 4º, que trata da Política Nacional de Relações de Consumo, afirma-se que ela tem por objetivo o atendimento das necessidades dos consumidores, *atendidos os seguintes princípios: I –reconhecimento da vulnerabilidade do consumidor no mercado de consumo.*

Dentro desta perspectiva o consumidor é a parte fraca da relação de consumo, decorrendo de dois aspectos que são de ordem técnica e cunho econômico. (NUNES, 2018, p. 122). Do ponto de vista técnico, o consumidor geralmente não possui o conhecimento especializado necessário para entender completamente o produto ou serviço que está adquirindo. Isso pode incluir a falta de entendimento sobre a composição do produto, seu funcionamento, os termos do serviço, entre outros.

Nessa mesma linha, Nunes aduz (2018, p. 122):

O primeiro está ligado aos meios de produção, cujo conhecimento é monopólio do fornecedor. E quando se fala em meios de produção não se está apenas referindo aos aspectos técnicos e administrativos para a fabricação e distribuição de produtos e prestação de serviços que o fornecedor detém, mas também ao elemento fundamental da decisão: é o fornecedor que escolhe o que, quando e de que maneira produzir, de sorte que o consumidor está à mercê daquilo que é produzido.

Ainda, Nunes (2018, p. 122), complementa que:

O segundo aspecto, o econômico, diz respeito à maior capacidade econômica que, por via de regra, o fornecedor tem em relação ao consumidor. É fato que haverá consumidores individuais com boa capacidade econômica e às vezes até superior à de pequenos fornecedores.

Nesse viés, Souza (2018, p. 14) relata que “A vulnerabilidade é inerente a todos os consumidores, como se fosse uma marca registrada, que se opõe a todos eles, independentemente de sua condição social ou econômica. É ela que justifica a adoção das regras protetivas que o Código elenca”.

A respeito Filomeno (2018, p. 14) aduz que:

Por vulnerabilidade, há de se entender a fragilidade dos consumidores, em face dos fornecedores, quer no que diz respeito ao aspecto econômico e de poder aquisitivo, quer no que diz respeito às chamadas informações disponibilizadas pelo próprio fornecedor ou ainda técnica. Ora, referidas informações, que podem ser, por exemplo, verdadeiras ou falsas, ou então desatenderem às expectativas dos consumidores, mediante oferta, publicidade ou apresentação (embalagens, bulas de remédios, manuais de uso, cartazes e outros meios visuais), apresentando-se, por conseguinte, na fase chamada pré-contratual. Essa vulnerabilidade ainda está presente na fase de contratação na aquisição de um produto ou da prestação de um serviço.

Por conseguinte, o que se constata no conceito de vulnerabilidade é dessemelhante ao de hipossuficiência, desse modo, todo o consumidor é sempre vulnerável, o que se trata de uma característica inerente à própria condição daquele que é o destinatário final do produto/serviço, porém nem todo o consumidor é hipossuficiente (TARTUCE, 2021, p. 49).

2.3.2 Princípio da informação adequada

Importante observar o inciso III do art. 6º do Código de Defesa do Consumidor sobre o direito à informação:

Art. 6º São direitos básicos do consumidor:

[...]

III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; (BRASIL, 1990).

Interessa observar que o parágrafo único do art. 6º, estabelece que: “A informação de que trata o inciso III do caput deste artigo deve ser acessível à pessoa com deficiência, observado o disposto em regulamento” (BRASIL, 1990). Nesse caso, o fornecedor deverá adaptar meios de comunicação acessíveis, para poder oferecer informações às pessoas com deficiência, tanto auditiva quanto visual.

O direito de ser informado tem início na fase pré-contratual e vai estender até depois do exaurimento da relação jurídica de consumo, como por exemplo as garantias legais que impõem o fornecedor as obrigações na fase pós-contratual, assim tendo o fornecedor a obrigação de disponibilizar todas as informações e assistência precisas ao consumidor, mesmo que ele já tenha adquirido o produto ou o serviço (SOUZA, 2018, p. 44).

O direito à informação é um reflexo do princípio da transparência e está junto ao princípio da vulnerabilidade, esse direito é o primeiro aparato de igualdade e reequilíbrio na relação de consumo (CAVALIERI FILHO, 2022, p. 133).

Complementa Cavalieri (2022, p. 133) que, “com efeito, o consumidor não tem conhecimento algum sobre o produto ou serviço de que necessita; detentor desse conhecimento é o fornecedor, que tem o domínio do processo produtivo. Este sim sabe o que produziu, como produziu, por que e para quem produziu, aspectos em que o consumidor é absolutamente vulnerável”.

A respeito do direito à informação Cavalieri Filho (2022, p. 133) esclarece:

Outra característica do direito à informação é que ele não é um fim em si, não se exaure em si mesmo. Na verdade, tem por finalidade garantir ao consumidor o exercício de outro direito ainda mais importante, que é o de escolher conscientemente. Essa escolha consciente propicia ao consumidor diminuir os seus riscos e alcançar suas legítimas expectativas. Mas sem informação adequada e precisa o consumidor não pode fazer boas escolhas, ou, pelo menos, a mais correta. É o que se tem chamado de consentimento informado, vontade qualificada ou, ainda, consentimento esclarecido.

A informação é fundamental para colocar o consumidor em lugar de igualdade, assim terá liberdade de vontade somente quando ver a segurança da informação recebida de forma clara e transparente podendo então tomar sua decisão dentro da relação (CAVALIERI FILHO, 2023, p. 133).

Por sua vez, comenta, Theodoro Júnior (2017, p.65) que o “dever de informação clara quanto ao conteúdo do contrato a ser celebrado, às obrigações que estarão sendo assumidas pelo

consumidor, evitando que seja surpreendido por cláusulas abusivas ou que não consiga cumprir”.

Ainda sobre o princípio da informação Souza (2018, p. 18), esclarece:

Aliás, convém lembrar que a informação inadequada ou incompleta se equipara à vício do produto ou do serviço, gerando responsabilidade civil do fornecedor. Outra regra decorrente do princípio da informação e que muitos não perceberam é a obrigação de constar de todos os produtos a informação de seus prazos de validade, e de maneira visível e indelével. Consideramos, assim, que ficou suficientemente demonstrada a relevância e a constante presença do princípio da informação no corpo do Código do Consumidor.

Isto posto, deverá o fornecedor especialista informar, aconselhar e orientar o consumidor não especialista sobre o produto ou serviço, ou seja, dar ao consumidor informações indispensáveis para que ele possa escolher entre as várias opções que são oferecidas (CAVALIERI FILHO, 2022, p. 135).

2.3.3 Princípio da boa fé

Dentro dos princípios consumeristas, existe um chamado princípio da boa-fé, elencado no CDC. Denota-se que não se trata de uma tutela absoluta e incondicional que o CDC põe a serviços dos consumidores e sim a que rodeia a vulnerabilidade dos consumidores, sem comprometer o avanço econômico do país, sendo necessário para o melhor desenvolvimento social e seu bem-estar (THEODORO JÚNIOR, 2017, p. 216).

Nesse viés, resta esculpido no disposto do art. 4º, III do Código de Defesa do Consumidor, que diz:

“Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores; (BRASIL, 1990).

No entanto, Souza (2018, p. 16), explica que “Após o advento do Código do Consumidor e do Código Civil de 2002, objetivou-se a boa-fé, que se transformou em dever jurídico, regra obrigatória de conduta, e não apenas uma exortação ética”.

Esse direito decorre da boa-fé, sendo um princípio de que tem a obrigação de conduzir todas as relações, sejam elas jurídicas ou não (SOUZA, 2018, p. 44).

Nesse passo, em relação ao primeiro item, considera que a boa-fé se impõe para estabelecer o conteúdo e obtenção das cláusulas contratuais, a fim de interpretá-las de maneira que torne melhor ao interesse e confiança gerada entre as partes (SOUZA, 2018, p. 44).

Já em uma situação formal que seria a celebração de um contrato, cada parte acredita e confia que a outra agirá com boa-fé e que os regulamentos do contrato têm a finalidade de satisfazer os interesses das partes (SOUZA, 2018, p. 44).

Na explicação de Souza (2018, p. 45), “Por fim, a boa-fé impõe, sobre os contratos, diversos limites, impedindo-se abusos e, de outro modo, determinando que as relações negociais estejam sempre materialmente equilibradas, vedando-se o enriquecimento ilícito das partes”.

À luz desse contexto, Filomeno (2018, p. 118), tanto no que diz respeito ao novo Código Civil, como no Código de Defesa do Consumidor, portanto, o chamado princípio da boa-fé (presente no inciso III do art. 4º, como já visto linhas atrás, e no inciso IV do art. 5142 do Código de Defesa do Consumidor, bem como nos arts. 113 e 422 do novo Código Civil), demanda, primeiramente, se partir do princípio de que o contrato tem uma função social, e não mais simplesmente individual ou individualista.

2.3.4 Princípio da transparência

O artigo 4º do Código de Defesa do Consumidor estabelece a necessidade de “transparência e harmonia nas relações de consumo”. Isso indica que os princípios da transparência e da boa-fé estão intrinsecamente ligados nas relações de consumo, conforme destacado por Cavalieri Filho (2022, p. 72). Em outras palavras, a transparência nas relações de consumo é fundamental para garantir a boa-fé entre as partes envolvidas. Isso implica que tanto os consumidores quanto os fornecedores devem agir com honestidade, clareza e consideração mútua para garantir uma relação de consumo justa e equilibrada.

Há que se notar, que a transparência nas relações de consumo é importante ao trazer informações, corretas e precisas sobre aquele produto ou serviço que foi oferecido ou prestado, assim como os contratos firmados mediante direitos e obrigações (CAVALIERI FILHO, 2022, p. 72).

Em razão disso Cavalieri (2022, p.72) esclarece, “A principal consequência do princípio da transparência é, por um lado, o dever de informar do fornecedor e, por outro, o direito à informação do consumidor”.

Dentro dessa perspectiva, Cavalieri Filho (2022, p. 72) retrata:

Transparência não importa apenas em dever negativo do fornecedor. Importa também um conjunto diversificado de deveres procedimentais que recaem sobre aqueles que fornecem produtos e serviços no mercado de consumo. Nesta dimensão, a transparência tem a ver com a qualidade e a quantidade da informação que o fornecedor tem que prestar ao consumidor, consoante arts. 8º, parágrafo único, 9º, 10, 30, 31, 36, 46, 52, 54, § 4º, todos do CDC.

Já Souza (2018), aduz: “Considerando que o princípio da transparência está intimamente ligado ao da boa-fé, constituindo uma consequência lógica deste.”

Importante entender que na transparência está o dever de informar de forma clara e certamente recai sobre os fornecedores no momento de oferecer e o consumidor poder escolher e decidir com segurança o que lhe foi oferecido e ter total conhecimento, ao que tem interesse, assim como, celebrar contrato a saber quais os riscos que está à mercê de sofrer (SOUZA, 2018, p. 17).

Nesse sentido, Souza (2018, p.17) esclarece: “A transparência que agora se exige, desde a oferta, a publicidade e na redação das cláusulas do contrato, representa uma das mais eficazes proteções que o Código confere aos consumidores”. Complementa ainda Souza (2018, p. 17), “E diante da possibilidade de o fornecedor malicioso violar o dever de transparência, redigindo cláusulas nebulosas, reticentes, sibilinas, o melhor antídoto fornecido pelo Código está em seu art. 47, segundo o qual as cláusulas contratuais serão interpretadas de maneira mais favorável ao consumidor”.

Dispõe, conforme o parágrafo único do art. 36 do Código de Defesa do Consumidor assevera que:

Art. 36. A publicidade deve ser veiculada de tal forma que o consumidor, fácil e imediatamente, a identifique como tal.
Parágrafo único. O fornecedor, na publicidade de seus produtos ou serviços, manterá, em seu poder, para informação dos legítimos interessados, os dados fáticos, técnicos e científicos que dão sustentação à mensagem (BRASIL, 1990).

Sobre o dever tanto da informação quanto da transparência, o Código de Defesa do Consumidor decidiu por alterar regra chamada de *caveat emptor*, que era papel do consumidor de ir atrás das informações referentes ao produto ou serviços de seu interesse, e passou a ser chamado então de *caveat venditor*, ou seja, que deve caber ao fornecedor levar as devidas informações ao consumidor (SILVA, 2022. p. 24).

2.3.5 O princípio da confiança

Este princípio é pertencente ao princípio da boa-fé e está junto ao princípio da transparência. O princípio da confiança é a segurança e a credibilidade que o consumidor entrega ao produto ou serviço mediante contrato como uma ferramenta cabível para determinado fim de aquisição que lhes é de interesse (CAVALIERI FILHO, 2022.p. 73).

Em outras palavras, este princípio nas relações de consumo é o que apresenta uma grande importância (SOUZA, 2018, p. 19).

Nesse caso o consumidor acredita e confia que o produto ou serviço que lhe são oferecidos são de total confiança e apresentam todas as características descritas pelo fornecedor, assim confiando que são verdadeiras as informações prestadas e que se porventura vier sofrer algum dano, este terá reparo integralmente daquilo que adquiriu (SOUZA, 2018, p. 19).

Por fim, explica Souza (2018, p. 19), “É a confiança que confere credibilidade ao mercado de consumo, incentivando e aquecendo a demanda. Ninguém se disporia a adquirir um produto, ou contratar um serviço, se suspeitasse não serem verdadeiras as informações do fornecedor, ou que tivesse ele algum defeito”.

2.3.6 Princípio da equidade ou princípio do equilíbrio contratual absoluto

Com relação ao princípio da equidade encontra-se previsto no Código do Consumidor nos artigos 7º que, dispõe:

Art. 7º Os direitos previstos neste código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e equidade (BRASIL, 1990).

Outro ponto que deve ser analisado também é o art. 51, IV, que considerando despótico e em desacorde com a boa-fé ou também com a equidade.

Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: IV - estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade; (BRASIL, 1990).

Sob este enfoque, o princípio da equidade tem a finalidade de firmeza na relação contratual, tendo em vista que não se trata somente de prerrogativas, assim como nas aplicações

de partes que estejam envolvidas no decurso do consumo e no fornecimento, trazendo mais segurança a fim de terminar com a prática abusiva dentro da relação de consumo (SILVIA, 2003, p. 73).

Com tal delineamento, o princípio da equidade concede ao juiz o poder de dirimir o conflito diante de suas persuasões (SOUZA, 2018, p. 20).

Por essa razão, Souza (2018, p. 20), aponta que “Como se vê, no sistema do direito do consumidor, a equidade é uma utilíssima ferramenta, que o Código o autoriza a manejar, diante de um caso específico, em que o texto da lei não se mostra suficiente para se alcançar o justo”.

2.4 OS DIREITOS BÁSICOS DO CONSUMIDOR

Os direitos e garantias do consumidor desempenham um papel fundamental na proteção dos indivíduos em suas relações de consumo. Ao longo das últimas décadas, diversos países ao redor do mundo têm implementado legislações específicas para assegurar que os consumidores tenham seus direitos respeitados e estejam protegidos contra práticas abusivas por parte das empresas. No Brasil, por exemplo, o Código de Defesa do Consumidor (CDC), promulgado em 1990, estabeleceu um conjunto abrangente de direitos e garantias para os consumidores, nos previstos em seu art. 6º (BRASIL, 1990).

No propósito de seguir a ordem constitucional em garantir a defesa do consumidor, foi estabelecido uma lista de direitos básicos pelo legislador, tais como, “os interesses mínimos, materiais ou instrumentais, relacionados a direitos fundamentais universalmente consagrados com relevância social e econômica” (CAVALIERI FILHO, 2022).

Estabelece o art. 1º, III, CF e 6º, I, CDC, os direitos em espécie, a proteção à segurança, à saúde e a vida podendo ser entendida como um desdobre do princípio constitucional da dignidade da pessoa humana (BRASIL, 1988; BRASIL, 1990).

Desta forma, cabe ao fornecedor a obrigação e o dever de garantir a proteção aos consumidores, através de propagandas, nas embalagens de produtos cientificando sobre qualquer eventualidade de risco que estão sujeitos (CAVALIERI FILHO, 2022).

No que se refere ainda ao art. 6º do CDC, outro direito importante é o da educação do consumidor, tendo como finalidade o cuidado com a igualdade de contratação e liberdade de escolha. Já Grinover et al (2022), ressalta que este direito pode ser dividido como formal e informal, podendo o primeiro ser aplicado em disciplinas escolares e o segundo aplicado por meio de ações de marketing patrocinadas pelos fornecedores que oferecem os produtos.

Nesse passo, outro direito importante é o dever de informar, no entendimento de Neves (2022), “existe desde a fase pré-contratual e se estende até depois do exaurimento da relação jurídica de consumo [...], cabendo ao fornecedor prestar todas as informações e assistência ao consumidor mesmo após a aquisição do produto ou serviço”.

No mesmo sentido Neves (2022), traz a proteção da contra a publicidade e propaganda enganosa e abusiva, com o propósito de resguardar a liberdade de escolha e não a sujeição do consumidor a condições desfavorável.

Já Garcia (2019, p. 346), traz também:

O direito à privacidade é uma garantia fundamental do consumidor, que deve ter seus dados pessoais protegidos contra o uso indevido ou abusivo por parte dos fornecedores. A Lei Geral de Proteção de Dados Pessoais estabelece regras claras para o tratamento de dados pessoais, garantindo que os consumidores tenham controle sobre seus dados e que estes sejam utilizados de forma transparente e segura.

No entanto é fundamental que os consumidores conheçam e exerçam seus direitos e garantias, a fim de contribuir para a construção de uma relação de consumo mais equilibrada e justa. Vale destacar o art. 37 da Carta Magna, protegido nos princípios constitucionais, o legislador presumiu como direito do consumidor a adequação dos serviços públicos prestados. (BRASIL, 1988; BRASIL, 1990).

Para um conhecimento mais amplo, o estudo dos direitos do consumidor é de grande importância para a compreensão das bases da norma consumerista, perante as quais estão protegidas as relações da sociedade nova de consumo, pelo crédito, impessoalidade e marketing (GRINOVER et al., 2022).

No entanto esse método tem sido amplamente utilizado no campo do marketing personalizado, o qual visa oferecer produtos e serviços de acordo com o perfil individual do consumidor, resultando em uma maior probabilidade de concretização do negócio (MIRAGEM, 2018).

Por fim, no próximo capítulo será abordado a questão do reconhecimento facial frente a proteção de dados pessoais.

3 O RECONHECIMENTO FACIAL E A PROTEÇÃO DE DADOS PESSOAIS NO DIREITO BRASILEIRO

No âmbito do direito brasileiro, o reconhecimento facial e a proteção de dados pessoais são questões regulamentadas e protegidas por leis específicas, especialmente pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n. 13.709, de 14 de agosto de 2018, que entrou em vigor no ano de 2020, constando também rol de direitos e garantias fundamentais previsto no art. 5º, LXXIX, a partir da Emenda Constitucional n. 115/2022 (BRASIL, 2018; BRASIL, 2022).

3.1 O DIREITO DIGITAL E O SURGIMENTO DO RECONHECIMENTO FACIAL

O direito digital é um ramo do direito que trata das questões jurídicas relacionadas ao uso da tecnologia da informação e das comunicações, ocorre que a tecnologia e a internet andam juntas e sempre em constante evolução, segundo Farias, Rosenvald e Braga (2015), “serviços bancários, turismos, modos de deslocamento na cidade, compras em geral, música, cultura, educação, quase todas as áreas das relações sociais parecem ter sofrido fortes mudanças com o efetivo ingresso da internet em nossas vidas”.

Pode-se afirmar que o Direito Digital engloba o conjunto de normas e princípios que regem o comportamento e as interações dos indivíduos cujas ações e evidências de suas manifestações de vontade ocorrem no ambiente digital, resultando em dados eletrônicos que validam e representam as obrigações assumidas, bem como a autoria correspondente (PINHEIRO, 2021).

A consolidação da era da informação ocorreu com o advento da tecnologia digital e a criação da Internet, cuja origem remonta às décadas de 1960 e 1970, quando os Estados Unidos estabeleceram a Rede de Agência de Pesquisas em Projetos Avançados - ARPANET (Advanced Research Projects Agency Network). Inicialmente concebida para fins militares, a ARPANET tinha como propósito principal a transmissão de dados entre instituições militares (LINS, 2013).

A internet – que surgiu como uma forma de interligação, de modo descentralizado, dos computadores militares americanos – passou a ser utilizado comercialmente nos Estados Unidos em 1987. Foi então que ganhou essa denominação, internet. No Brasil, a internet chegou em meados da década de noventa (em 1995, especificamente, é publicada uma norma do Ministério das Comunicações que marca esse início). A

internet, sob o prisma técnico, é a conexão entre protocolos, conhecidos como IPs (*internet protocols*). Esse IP, uma espécie de endereço digital, permite que as investigações descubram (ou tentem descobrir) de onde partiram certas postagens na rede. Há, ainda, os nomes de domínio (*domain name system*), que são endereços que digitamos para chegarmos aos *sites*, complementados pelas respectivas terminações (*top level domains*), que são os finais dos endereços, após o ponto (ou o último ponto, se houver mais de um: *.com, .gov, .jus*). Nós nos deslocamos pela internet usando navegadores (*browsers*). Não por acaso, usamos o verbo *navegar* (FARIAS; ROSENVALD; BRAGA, 2015).

Depois do surgimento da internet e o atual momento em que vivemos é que o Direito Digital surge com o intuito de normalizar as novas relações que a internet vem trazendo a cada dia. A evolução do Direito Digital acompanha a rápida transformação da sociedade impulsionada pelas novas tecnologias. Ele abrange os princípios e institutos fundamentais do Direito existentes, adaptando-os ao contexto digital em constante evolução. Além disso, o Direito Digital introduz novos institutos e elementos para o pensamento jurídico, permeando todas as áreas do Direito (PINHEIRO, 2021).

Nesse sentido Pinheiro (2013) afirma, que “o Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje [...]”. Apesar disso, o Direito Digital objetiva incluir novos elementos para o pensamento jurídico no intuito de que o Direito venha a se adaptar a realidade da era digital buscando remédio jurídico para todas as áreas do Direito.

Nesse aspecto, Pinheiro (2013), enfatiza que:

A proposta é que o Direito siga sua vocação de refletir as grandes mudanças culturais e comportamentais vividas pela sociedade. No Direito Digital prevalecem os princípios em relação às regras, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa. Por isso, a disciplina jurídica tende à autorregulamentação, pela qual o conjunto de regras é criado pelos próprios participantes diretos do assunto em questão com soluções práticas que atendem ao dinamismo que as relações de Direito Digital exigem.

Em suma, o Direito Digital é presente em todas as áreas do Direito, no entanto essa etapa do Direito os princípios jurídicos desempenham um papel muito significativo, a tecnologia evolui exponencialmente todos os dias criando um desafio constante para os legisladores acompanharem essas mudanças, como vemos pela análise de Patrícia Pack (2016):

A velocidade das transformações é uma barreira à legislação sobre o assunto. Por isso qualquer lei que venha a tratar dos novos institutos jurídicos deve ser genérica o suficiente para sobreviver ao tempo e flexível para atender aos diversos formatos que podem surgir de um único assunto. Essa problemática legislativa, no entanto, não tem nada de novo para nós, uma vez que a obsolescência das leis sempre foi um fator de discussão em nosso meio.

Conforme a autora destaca, as mudanças sociais exercem uma influência significativa na legislação, o que demanda uma constante evolução das leis para se adequarem às novas realidades presentes na sociedade. Essa necessidade de adaptação torna-se ainda mais evidente diante do impacto que tais transformações exercem sobre o tecido social.

O constante aumento no volume de dados tem gerado uma demanda crescente por processamentos cada vez mais rápidos. Nesse contexto, a realização manual desse processamento por um ser humano torna-se cada vez mais desafiadora. Como resultado, a utilização de ferramentas computacionais se tornou imprescindível para aprimorar o processamento de dados, permitindo uma resolução mais ágil de problemas (FACELI et al., 2015).

Nas atividades diárias, são constantes os desafios para executar diversas tarefas que demandam inúmeros processamentos por parte do nosso cérebro, o qual é responsável por gerenciar nossos pensamentos e emoções. Inspirado no desempenho notável do nosso sistema nervoso, foram desenvolvidas as redes neurais artificiais, que buscam simular o funcionamento do cérebro humano. Essas redes têm a capacidade de processar informações e aprender com os dados obtidos (FACELI et al., 2015).

O reconhecimento facial é apenas uma das muitas possibilidades criadas pela inteligência artificial. Antes de explorar essa tecnologia em detalhes, é importante ressaltar o conceito mais amplo de inteligência artificial em si, “uma subárea da ciência da computação e busca fazer simulações de processos específicos da inteligência humana por intermédio de recursos computacionais” (PEIXOTO; SILVA, 2019).

Já Coppin (2010), corrobora que, “envolve utilizar métodos baseados no comportamento inteligente de humanos e outros animais para solucionar problemas complexos”.

Como se pode perceber a respeito do projeto de lei citado, Silva (2019) explica:

[...] os estabelecimentos comerciais que utilizarem programas de reconhecimento facial com o intuito de identificar os consumidores devem alertá-los na entrada do estabelecimento com placas e/ou adesivos da análise de características sendo utilizada [...] além de identificarem pessoas, os sistemas podem detectar emoções e reações por meio de expressões monitoradas, o que fere os direitos humanos fundamentais como privacidade e liberdade de expressão [...] outra preocupação com os sistemas de reconhecimento e detecção facial envolve as falhas na identificação de pessoas, especialmente na precisão diferente para distintos grupos étnicos e raciais.

No entanto o reconhecimento facial, é uma tarefa cada vez mais exigente, utiliza técnicas de aprendizado de máquina, como o *machine learning*, em conjunto com redes neurais artificiais. Essa combinação apresenta desafios significativos, especialmente quando se trata de sistemas de segurança que requerem uma maior assertividade. Diversos fatores, como o ponto de vista da câmera, a iluminação e a expressão facial, podem dificultar o processo de reconhecimento facial (LI; JAIN, 2004).

O *deep learning*, uma subárea do aprendizado de máquina, revolucionou a capacidade dos computadores em lidar com grandes conjuntos de dados de forma rápida e eficiente. Através de algoritmos sofisticados e técnicas avançadas, os computadores são capazes de realizar tarefas que anteriormente eram exclusivas dos seres humanos, como o reconhecimento de voz e imagens (DEEP, 2019).

Com o avanço das ferramentas de inteligência artificial e *deep learning*, os sistemas de reconhecimento facial surgiram e se popularizaram rapidamente. Essa tecnologia revolucionária permite identificar pessoas por meio da análise detalhada dos traços geométricos e logarítmicos de suas imagens faciais, com base na premissa de que cada indivíduo possui um padrão facial único e característico. Essa abordagem tem sido amplamente adotada em diversas áreas, impulsionando a segurança, autenticação e personalização de experiências. O reconhecimento facial representa um marco importante na evolução da inteligência artificial, proporcionando uma poderosa forma de identificar e distinguir pessoas com base em suas características faciais distintivas (GUARIENTO; MARTINS, 2022).

Dentro desse enfoque, em contraste com o sistema de impressão digital, desenvolvido pelo francês Francis Galton em 1892, o reconhecimento facial é uma tecnologia relativamente mais recente, tendo suas origens a partir da década de 1960. Foi nessa época que o governo dos Estados Unidos deu início à pesquisa e ao desenvolvimento de um sistema semiautomático de reconhecimento facial, semelhante ao que conhecemos atualmente. Desde então, o reconhecimento facial passou por avanços significativos, impulsionados pelos avanços nas ferramentas de inteligência artificial e *deep learning*, permitindo uma difusão cada vez maior dessa tecnologia em diversas aplicações (GUARIENTO; MARTINS, 2022).

De fato, como visto, o sistema de reconhecimento facial utiliza padrões biométricos como base, estes são considerados dados pessoais sensíveis, de acordo com o art. 5º, II, da Lei Geral de Proteção de Dados (LGPD). O tratamento desses dados biométricos requer requisitos

específicos, mais rigorosos do que aqueles aplicados ao tratamento de dados pessoais em geral. Assim, o tratamento dos dados biométricos no contexto do reconhecimento facial deve ser realizado com cuidado e em conformidade com as disposições legais estabelecidas (GUARIENTO; MARTINS, 2022).

Segundo especialistas da IBM (2018), o conceito de *deep learning* vai além do *machine learning* convencional. O *deep learning* enfatiza a capacidade de aprendizado contínuo, onde o sistema busca aprender com o mundo real e adaptar o modelo de aprendizado à medida que novas informações são recebidas e novas ideias são geradas. Essa abordagem permite uma maior flexibilidade e capacidade de lidar com cenários complexos, permitindo que o sistema se aperfeiçoe ao longo do tempo. Com essa capacidade de aprendizado contínuo, o *deep learning* demonstra seu potencial em fornecer soluções mais sofisticadas e adaptáveis aos desafios do mundo real.

Por tais aspectos, com dados não estruturados, como imagens, texto, voz e vídeos, a abordagem tradicional de engenharia manual de recursos se torna demorada, frágil e não escalonável na prática. É por isso que as redes neurais estão se tornando cada vez mais populares, devido à sua capacidade de descobrir automaticamente as representações necessárias para a detecção ou classificação de recursos a partir de dados brutos. Isso elimina a necessidade de engenharia manual de recursos e permite que a máquina aprenda os próprios recursos, utilizando-os para realizar tarefas específicas. A base do *deep learning* reside nas redes neurais, especialmente as redes neurais convolucionais (CNNs), que se destacam no reconhecimento de padrões e são a principal tecnologia por trás de aplicações como carros autônomos, reconhecimento facial, transcrição de fala e muitas outras. As CNNs têm a capacidade de extrair características complexas e hierárquicas dos dados, tornando-as uma ferramenta poderosa no processamento de informações não estruturadas (MIT 6.S191, 2020).

Com tal delineamento, apesar de o reconhecimento facial ser uma ferramenta importante para monitoramento e segurança em espaços públicos, a sua utilização ainda suscita questões sobre a legitimidade do ponto de vista da privacidade e da proteção de dados. Isso ocorre devido à preocupação em preservar os direitos e liberdades individuais dos titulares dos dados, especialmente porque ainda não existe uma orientação específica da Autoridade Nacional de Proteção de Dados e a jurisprudência relacionada ao assunto ainda é limitada. Diante desse

cenário, torna-se necessário um debate amplo e aprofundado para encontrar um equilíbrio entre a segurança proporcionada pelo reconhecimento facial e a necessidade de proteção dos direitos fundamentais dos indivíduos, a fim de garantir que seu uso seja realizado de maneira ética e legalmente adequada (GUARIENTO; MARTINS, 2022).

Considerando o tratamento em grande escala de dados pessoais sensíveis, inclusive de indivíduos vulneráveis, é recomendável a elaboração de um Relatório de Impacto à Proteção de Dados. Esse relatório tem como objetivo identificar a necessidade de adoção de medidas específicas para mitigar os impactos e riscos em situações concretas. Assim, é possível avaliar de maneira abrangente os possíveis efeitos do tratamento de dados pessoais sensíveis, especialmente no contexto do reconhecimento facial, e adotar medidas adequadas para proteger a privacidade e os direitos dos titulares desses dados (GUARIENTO; MARTINS, 2022).

3.2 OS MÉTODOS DO RECONHECIMENTO FACIAL

Os métodos utilizados para detecção facial variam de acordo com a finalidade da aplicação e os requisitos específicos do sistema.

Para Li e Jain (2004), o desempenho de diversos métodos de reconhecimento facial é frequentemente afetado por mudanças na iluminação e expressões faciais. Além disso, a ocorrência de falsos positivos levou à necessidade de um estudo mais aprofundado sobre o reconhecimento de padrões, com um enfoque específico no reconhecimento facial, a fim de avaliar a eficácia de cada técnica empregada nesse campo.

Os métodos de reconhecimento facial também podem ser classificados em duas categorias principais que são: baseados em características e baseados em aprendizado de máquina. O primeiro que são os métodos baseados em características específicas da face, como contornos, proporções e texturas, essas características são usadas para identificar um determinado indivíduo através de técnicas de correspondência ou classificação (JIE ZHOU, 2018).

E o outro, que são os métodos baseados em aprendizados de máquina aproveitam algoritmos de aprendizados para treinar modelos que podem reconhecer rostos com base em padrões aprendidos a partir de um conjunto de dados. Tais métodos têm demonstrado um desempenho, especialmente com o advento de técnicas avançadas, como redes neurais

convolucionais (CNNs), que têm a capacidade de extrair automaticamente características discriminativas das imagens faciais (JIE ZHOU, 2018).

Assim a análise é a escolha do método de reconhecimento facial que dependerá do contexto de aplicação, das restrições e das necessidades específicas do sistema.

3.3 O USO E AS APLICAÇÕES DO RECONHECIMENTO FACIAL

O reconhecimento facial é um método avançado que envolve a aplicação de técnicas de análise de características biométricas com o objetivo de identificar e verificar a identidade de indivíduos com base em suas características faciais exclusivas, as características biométricas são um campo de estudo e pesquisa altamente relevante nos dias atuais, especialmente no contexto do reconhecimento facial para fins de autenticação (JAFRI, 2009).

Entretanto as tecnologias baseadas em características biométricas abrangem uma ampla gama de métodos de identificação, que envolvem tanto características fisiológicas quanto traços comportamentais. No que diz respeito às características fisiológicas, os sistemas biométricos podem utilizar dados como o rosto, as impressões digitais, a geometria dos dedos, a geometria das mãos, as veias das mãos, a palma da mão, a íris, a retina e até mesmo a orelha para autenticar e identificar indivíduos (JAIN, 2006).

Na mesma senda, essas etapas são essenciais para avaliar e processar a imagem obtida, eliminando informações desnecessárias e focalizando nas áreas relevantes. Por exemplo, quando um algoritmo de reconhecimento facial é aplicado a uma imagem, ele realiza uma análise para identificar uma ou mais faces presentes (GUIMARÃES, 2022).

Dessa forma, para obter resultados satisfatórios, muitos algoritmos de detecção facial requerem treinamento extensivo. Esse treinamento envolve a detecção de uma ampla variedade de imagens contendo faces e objetos diversos. Uma abordagem comum para abordar o problema de detecção facial é aplicar técnicas de reconhecimento de padrões de duas classes, onde uma classe representa todas as instâncias de faces e a outra classe engloba tudo o que não é uma face. Durante o treinamento, o algoritmo aprende a distinguir características e padrões que são comuns em faces e a diferenciá-las de objetos não relacionados (GUIMARÃES, 2022).

De acordo com Guimarães (2022 *apud* Brunelli, 1993), um dos primeiros sistemas de reconhecimento facial foi desenvolvido com base em um modelo de técnicas aplicadas a um

conjunto de características faciais, resultando em uma representação facial comprimida correspondente.

3.4 A TUTELA DO RECONHECIMENTO FACIAL NO BRASIL

É oportuno registrar que o Projeto de Lei nº 3.069/22 estabelece diretrizes para o uso do reconhecimento facial automatizado pelas forças de segurança pública em investigações criminais ou procedimentos administrativos. O objetivo é proporcionar uma regulamentação clara e transparente para garantir que o uso dessa tecnologia seja feito de forma adequada, respeitando os direitos individuais, a privacidade e a segurança dos cidadãos (GONZAGA, 2022).

Entretanto, o projeto de lei estabelece salvaguardas, como o estabelecimento de critérios claros para a coleta, armazenamento e compartilhamento de dados faciais, bem como a necessidade de autorização judicial prévia em determinados casos. Além disso, serão adotadas medidas de segurança para proteger os dados pessoais e prevenir o uso indevido do reconhecimento facial.

Diante disso, o Projeto de Lei 3069/22 define o reconhecimento facial como o procedimento biométrico automatizado utilizado para identificação humana, baseado na captura e análise de uma imagem facial (GONZAGA, 2022).

Conforme explicado por Gonzaga (2022). O reconhecimento facial é uma tecnologia emergente que tem o potencial de transformar muitos aspectos de nossas vidas, desde a segurança até a interação social. A tecnologia de reconhecimento facial funciona através da análise de características faciais únicas para identificar um indivíduo. Isso pode incluir a distância entre os olhos, o tamanho do nariz, a forma do queixo, entre outros.

Ademais, deve-se destacar que, até o momento, no Brasil não existem regulamentações específicas detalhadas para o uso do reconhecimento facial. No entanto, há projetos em andamento que visam implementar o uso dessa tecnologia na segurança pública e nas relações de consumo, levando em consideração os limites legais e as boas práticas aplicáveis. É necessário estabelecer diretrizes claras e normas específicas para garantir que o uso do reconhecimento facial seja realizado de forma ética, respeitando a privacidade dos indivíduos e protegendo seus direitos (ESCOVAR, 2020).

3.5 O RECONHECIMENTO FACIAL PARA FINS DE CONSUMO

O reconhecimento facial para fins de consumo é uma tecnologia em ascensão que tem o potencial de transformar a maneira como interagimos em atividades relacionadas ao consumo (SILVA, 2019).

De acordo com Silva (2019), as tecnologias relacionadas ao conhecimento facial são poderosas ferramentas de identificação, mas ao mesmo tempo levantam questões éticas distintas, pois podem ser utilizadas sem o conhecimento ou consentimento das pessoas que estão sendo submetidas a elas.

Além disso, o reconhecimento facial pode ser empregado como uma forma de aprimorar o entendimento aos clientes. De acordo com Resende (2019), essa inovadora ferramenta desempenha um papel útil na personalização do entendimento para clientes que frequentam regularmente determinadas lojas, auxiliando na identificação das preferências dos compradores e nas características dos produtos que provavelmente serão de seu interesse.

Ainda no que diz respeito às tecnologias de reconhecimento e a sua aplicação em relação aos consumidores, em particular no contexto das possíveis evoluções no campo do marketing, a Associação Brasileira de Marketing Direto (2020), destaca que:

[...] os profissionais de marketing estão começando a explorar o poder do reconhecimento facial para rastrear o comportamento do consumidor, avaliar as reações das campanhas dos consumidores, personalizar a experiência de compra e oferecer experiências em atritos, mas devem agir com cuidado pois os legisladores ainda discutem o assunto. Mas o fato é que a tecnologia está se espalhando [...] Alguns restaurantes e hotéis [...] estão testando o software para oferecer experiências personalizadas, rápidas e sem atritos para os consumidores angustiados. Os profissionais de tecnologia também estão usando a tecnologia para avaliar as reações dos consumidores às campanhas [...] Mas essa tecnologia pode ameaçar o equilíbrio entre a necessidade de informações e o direito à privacidade de um indivíduo, e os consumidores – e os legisladores – estão percebendo isso.

Observa-se, por conseguinte, que a versatilidade de funções do reconhecimento facial na relação com o consumidor possa ser vista como altamente proveitosa, é importante ressaltar que essa perspectiva não é amplamente consensual. De acordo com Resende (2019), essa prática, mesmo em sua forma aparente, está longe de ser considerada danosa:

[...] No Brasil, essa realidade não está longe e algumas redes começam a testar sistemas de reconhecimento facial que permitem verificar as reações dos clientes de

forma que a loja ajuste a disposição de seus produtos ou vitrines para se tornarem mais atrativas e aumentarem as vendas. Restaurantes e outros estabelecimentos também têm usado a tecnologia como um atrativo a mais para atender às expectativas do consumidor 4.0 [...] Nada de cartões fidelidade nem logins demorados para ser atendido – o pagamento também é feito pelo reconhecimento facial.

Nesse contexto, considerando as facetas mencionadas acima, que abrangem o direito consumerista e o reconhecimento facial, é imprescindível ressaltar o impacto dessa inovação na legislação nacional, especialmente no que se refere à Lei Geral de Proteção de Dados (LGPD), bem como nas perspectivas doutrinárias e jurisprudenciais. Embora seja um assunto recente, com sua implementação ocorrendo gradualmente no território nacional, os debates em torno da aplicabilidade, consequências e benefícios do uso do reconhecimento facial têm ganhado cada vez mais relevância (RESENDE 2019).

No entanto a relação entre os consumidores e o uso do reconhecimento facial é frequentemente abordada por especialistas no campo. Segundo Silva (2019), as lojas podem ser obrigadas, por meio do Projeto de Lei n. 2.537/19, a informar os consumidores sobre a implementação de sistemas de reconhecimento facial em suas instalações. Essa exigência reflete a importância de garantir a transparência e a consciência dos consumidores em relação ao uso dessa tecnologia, permitindo que tomem decisões informadas sobre sua participação e o compartilhamento de seus dados biométricos.

Ademais a reconhecimento facial para fins de consumo tem ligação com o próximo tópico que são a proteção dos dados pessoais no ordenamento jurídico brasileiro que é relacionada à necessidade de garantir o sigilo e a proteção dos dados coletados.

3.6 A PROTEÇÃO DOS DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

O crescente debate em torno da proteção da esfera privada tem se intensificado, especialmente devido às inovações tecnológicas que cada vez mais exigem a utilização de dados pessoais para aprimorar a experiência do usuário, impulsionadas pelos modelos de negócios na Internet. Essas discussões revelam um cenário contraditório, pois observa-se uma maior preocupação político-institucional com a proteção de dados e informações pessoais, ao mesmo

tempo em que se torna cada vez mais desafiador garantir essa proteção efetiva dos dados pessoais (SANTOS; CHEVTCHUK, 2015).

3.6.1 Um histórico da proteção de dados no Brasil

A implementação de uma Lei Geral de Proteção de Dados no Brasil não é um assunto recente. Há aproximadamente oito anos, o Ministério da Justiça lançou o tema da proteção de dados pessoais para consulta pública por meio de uma plataforma online (culturadigital.org), possibilitando amplas contribuições de indivíduos, empresas, academia e organizações do terceiro setor (VIDOR, 2019).

Como mencionado repetidamente, independentemente da nomenclatura atribuída à sociedade contemporânea, todas elas compartilham um elemento comum: a informação. Isso também se aplica ao Brasil, que está imerso nesse contexto. Apoiada por uma economia cada vez mais globalizada, a informação se tornou um elemento essencial e vital para as interações sociais, abrangendo perspectivas como o comércio eletrônico, a circulação de obras digitais, os direitos autorais e muito mais (BASAN, 2021).

Em 1990 no Brasil, começaram a surgir os diplomas legais chegando à proteção de dados pessoais a um outro nível jurídico. Desde então o CDC (Lei nº 8.078/90), fez a regularização do banco de dados dos consumidores e com isso foi estabelecido o direito do consumidor de ter acesso às informações contidas em cadastros, fichas, registros e dados pessoais e de consumo que se refiram a ele, permitindo-lhe verificar a existência de tais registros e corrigir possíveis imprecisões, assim o direito do consumidor obter acesso às informações contidas em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre si mesmo, conferindo-lhe a possibilidade de retificar eventuais imprecisões (MACIEL, 2019)

No ano de 2011, no Brasil, foram promulgadas duas leis de grande importância: a Lei do Cadastro Positivo e a Lei de Acesso à Informação. Sendo a primeira Lei nº 12.414/11 (Cadastro Positivo), com a propósito de consulta e informação sobre adimplemento de pessoas naturais ou jurídicas visando constar no histórico de créditos de devedores (MACIEL, 2019).

E a segunda, Lei nº 12.527/11 que é a Lei de Acesso à Informação pessoal relacionada a pessoa identificada ou não roborando aos órgãos do poder público sobre a proteção da

informação secreta, sempre com o cuidado a sua “disponibilidade, autenticidade, integridade e eventual restrição de acesso” (MACIEL, 2019).

No decorrer dos anos foram criadas novas leis sobre a proteção de dados como a Lei Carolina Dieckman que é a Lei nº 12.737/12 que põe fim a invasão de dispositivos informáticos, criado no final de 2012. Depois em 2013 veio o Decreto nº 7.962/13 - Decreto do Comércio Eletrônico em comemoração ao Dia do Consumidor (MACIEL, 2019).

Com o Marco Civil da Internet que a palavra “privacidade” passou a existir no sistema jurídico no Brasil, assim no ano de 2014 que o MCI entrou em vigor que a internet no Brasil, começou a ser regrada e mantendo o cuidado com a proteção de privacidade dos dados pessoais, previstos nos artigos 3º e 7º da Lei 12.737/12 de 2014;

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

[...]

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - 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;

X - 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; (BRASIL, 2014).

Assim, em 2018, o Brasil deu um importante passo ao estabelecer uma legislação voltada para a proteção de dados pessoais, claramente inspirada no regulamento europeu. Inicialmente programada para entrar em vigor em 16 de fevereiro de 2020, houve uma prorrogação do prazo através da Medida Provisória nº 869/18, ampliando-o em seis meses, passando para agosto do mesmo ano (MACIEL, 2019).

Portanto estamos, sem dúvida, vivendo um "novo tempo" em relação à proteção de dados no Brasil, e é esperado que haja um significativo amadurecimento tanto por parte das empresas quanto das pessoas naturais no que diz respeito à coleta e tratamento de dados

peçoais. A aprovação da Lei Geral de Proteção de Dados (LGPD) desempenha um papel fundamental nesse cenário, sendo de extrema relevância (ZAIDAN, 2019).

3.6.2 O surgimento da lei geral de proteção de dados (LGPD)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), conhecida pelo seu acrônimo "LGPD", foi promulgada pelo então presidente Michel Temer em 14 de agosto de 2018. Seu propósito principal é regular e proteger os dados pessoais de indivíduos, tendo como principal inspiração o Regulamento Geral de Proteção de Dados (GDPR) europeu que dispõe.

“Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.” (BRASIL, 2018).

A adoção da Lei Geral de Proteção de Dados (LGPD) no Brasil, inspirada nos princípios da General Data Protection Regulation (GDPR) europeia, ressalta a importância da proteção de dados pessoais. Além disso, a incorporação da proteção de dados como um direito fundamental na Constituição Federal, por meio de emendas constitucionais, evidencia a necessidade de salvaguardar informações sensíveis, evitando assim possíveis prejuízos e assegurando os direitos dos indivíduos (BLUM, 2020).

A LGPD introduz uma centralização na regulamentação do tratamento, proteção e privacidade de dados pessoais no Brasil, simplificando um cenário anteriormente fragmentado, caracterizado por diversas leis e normas aplicáveis. Antes da LGPD, questões relacionadas à proteção de dados eram abordadas por leis como o Código do Consumidor, o Marco Civil da Internet e a Lei de Acesso à Informação, resultando em uma estrutura legal complexa e dispersa (KOHLS, 2021).

No seu Artigo 2º, a LGPD estabelece os fundamentos que refletem os principais objetivos da lei, evidenciando o seu foco e determinação na proteção das informações pessoais das pessoas físicas, em consonância com o desenvolvimento tecnológico e a inovação. Esses fundamentos são:

- 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 (BRASIL, 2018).

A lei de proteção de dados se aplica a todas as entidades, sejam elas pessoas físicas ou jurídicas, independentemente do local onde os dados são armazenados ou do país de origem ou sede da pessoa envolvida. No entanto, é importante destacar que a aplicação da lei ocorre quando o tratamento dos dados ocorre no Brasil. Isso inclui situações em que os dados foram coletados no território nacional, pertencem a um indivíduo localizado no Brasil e o propósito da manipulação das informações é oferecer um bem ou serviço no território nacional. Essas condições delimitam o âmbito de aplicação da lei e garantem a proteção dos direitos dos indivíduos no contexto brasileiro (DE LUCCA, 2019).

Além de estabelecer as circunstâncias em que a lei se aplica, a legislação também define conceitos fundamentais relacionados aos tipos de dados tratados e às regras que regem sua utilização. Entre esses conceitos estão os de "Dados Pessoais" e "Dados Pessoais Sensíveis" (DONEDA, 2020).

3.6.3 Os princípios inerentes a lei geral de proteção de dados (LGPD)

A Lei Geral de Proteção de Dados (LGPD) estabelece uma série de princípios que devem ser observados no tratamento de dados pessoais. Esses princípios são fundamentais para garantir a proteção e o uso responsável das informações pessoais. Os principais princípios da LGPD são: I. finalidade II. adequação III. necessidade IV. livre acesso V. qualidade dos dados VI. transparência VII. segurança VIII. prevenção IX. não discriminação X. responsabilização e prestação de contas (MACIEL, 2019).

Os princípios da LGPD desempenham um papel fundamental na compreensão e na definição da legalidade do uso de dados pessoais (MACIEL, 2019)

A garantia da proteção dos direitos dos titulares dos dados pessoais é baseada na definição de princípios que regem o tratamento dessas informações, levando em consideração os limites dos direitos fundamentais. Da mesma forma, o Regulamento Geral de Proteção de Dados (GDPR) estabelece princípios orientadores para o tratamento de dados pessoais no artigo 5º. Esses princípios têm como objetivo fundamental assegurar a privacidade, a segurança e o controle dos indivíduos sobre seus dados pessoais. Ao adotar e seguir esses princípios, as

organizações podem estabelecer uma base sólida para a proteção dos direitos dos titulares e promover uma cultura de respeito à privacidade e à segurança dos dados pessoais (PINHEIRO, 2018).

Como se pode notar, Maciel (2019), traz em sua obra a explicação de cada um dos princípios inerentes a LGPD que são:

Princípio da finalidade, é um dos princípios fundamentais da Lei Geral de Proteção de Dados. Esse princípio estabelece que o tratamento de dados pessoais deve limitado ao mínimo necessário para alcançar as finalidades pretendidas.

Princípio da adequação, estabelece que o tratamento de dados pessoais deve ser realizado de forma compatível com as finalidades informada os titulares de dado,

Sobre o princípio da necessidade, a finalidade e adequação e a necessidade são elementos interligados no tratamento de dados pessoais, assim o princípio da necessidade estabelece que apenas os dados necessários para alcançar a finalidade informada devem ser tratados.

O princípio do livre acesso, da qualidade dos dados e da transparência assegura ao titular dos dados o direito de realizar consultas de forma fácil e gratuita, obtendo informações sobre como e por quanto tempo seus dados pessoais estão sendo tratados, tal princípio busca garantir a transparência no processo de tratamento de dados, permitindo que os titulares tenham conhecimento e controle sobre suas informações pessoais (MACIEL, 2019).

Os princípios da segurança e da prevenção destacam que a proteção de dados pessoais vai além da responsabilidade exclusiva da área de tecnologia da informação.

O princípio da não discriminação estabelece que nenhum dado coletado, independentemente da sua base legal ou finalidade explicitada com consentimento válido, pode ser utilizado para fins discriminatórios ilegais ou abusivos.

E por último os princípios da responsabilização e da prestação de contas estabelecem que o responsável pelo tratamento de dados não apenas deve cumprir as normas de proteção de dados, mas também ter a capacidade de demonstrar sua conformidade (MACIEL, 2019).

Ao analisar os princípios que regem a proteção de dados, pode-se identificar um núcleo comum que evidencia a importância desse tema. Esses princípios estabelecem diretrizes fundamentais para o tratamento adequado das informações pessoais, visando garantir a privacidade, a transparência e a segurança dos dados (BASAN, 2021).

3.6.4 A estrutura da lei geral de proteção de dados (LGPD)

A estrutura da LGPD é composta por diversos artigos que abrangem diferentes aspectos, como os princípios fundamentais da proteção de dados, os direitos dos titulares dos dados, as obrigações das empresas e órgãos públicos que realizam o tratamento de dados, as sanções em caso de descumprimento da lei, entre outros temas relevantes (OLIVEIRA, 2020).

Essa legislação visa garantir que os dados pessoais sejam tratados de forma transparente, segura e com respeito à privacidade das pessoas. Além disso, a LGPD estabelece a necessidade de obtenção do consentimento do titular dos dados para o seu uso, bem como o direito de acesso, retificação e exclusão dessas informações (SOUZA, 2020).

Na explicação de Maciel (2019), a respeito da estrutura da LGPD;

Definições: A lei inicia fornecendo uma série de definições importantes, como o que é considerado dado pessoal, dado sensível, tratamento de dados, controlador, operador, entre outros termos relevantes para a compreensão da legislação.

Princípios: A LGPD estabelece uma série de princípios que devem ser observados no tratamento de dados pessoais. Esses princípios incluem a finalidade, necessidade, adequação, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

Direitos dos titulares dos dados: A lei assegura aos indivíduos uma série de direitos em relação aos seus dados pessoais. Esses direitos incluem o acesso aos dados, a correção de informações incorretas, a eliminação dos dados, a portabilidade dos dados, a revogação do consentimento, a informação sobre o tratamento realizado, a oposição a determinadas atividades de processamento, entre outros.

Consentimento: A LGPD estabelece que o tratamento de dados pessoais somente poderá ser realizado mediante o consentimento do titular, de forma livre, informada e inequívoca. Além disso, a lei traz requisitos específicos para o consentimento válido, como a possibilidade de revogação a qualquer momento.

Bases legais para o tratamento: Além do consentimento, a LGPD apresenta outras bases legais que permitem o tratamento de dados pessoais, como o cumprimento de obrigação legal ou regulatória, o exercício regular de direitos em processos judiciais, a proteção da vida, a tutela da saúde, o legítimo interesse, entre outras.

Responsabilidade das empresas: A lei atribui responsabilidades às empresas que realizam o tratamento de dados pessoais. Elas devem adotar medidas de segurança para proteger as informações, estabelecer políticas de privacidade claras e transparentes, nomear um Encarregado de Proteção de Dados (DPO), comunicar incidentes de segurança, entre outras obrigações.

Transferência internacional de dados: A LGPD também trata da transferência de dados pessoais para países que não possuam níveis adequados de proteção de dados. Nesses casos, são estabelecidos requisitos específicos para a realização dessa transferência, como a obtenção de autorização prévia ou a adoção de cláusulas contratuais específicas.

Autoridade Nacional de Proteção de Dados (ANPD): A LGPD

Em suma, para Pinheiro (2018) a estrutura da LGPD representa um avanço significativo no Brasil para garantir a privacidade e os direitos dos indivíduos em um contexto cada vez mais digital e conectado. Ao estabelecer regras claras e responsabilidades, a lei busca equilibrar a inovação e o uso de dados pessoais com o respeito à privacidade, promovendo a confiança dos usuários e a proteção de suas informações no ambiente digital.

3.6.4.1 Os dados pessoais

De uma perspectiva simplificada, dados pessoais são todas as informações relacionadas a uma pessoa que possam identificá-la diretamente ou indiretamente, conforme definido no artigo 5º, I, da LGPD. Essas informações podem incluir nome, endereço, número de telefone, endereço de e-mail, CPF, entre outros dados que permitam a identificação do titular. A ampla definição de dados pessoais estabelecida pela LGPD visa garantir a proteção adequada das informações que possam estar ligadas à identidade de um indivíduo (BRASIL, 1988).

Ainda, o tratamento de dados pessoais está sujeito a uma série de regras e princípios, além da necessidade de agir de boa-fé. A Lei Geral de Proteção de Dados (LGPD) estabelece, em seu artigo 7º, um rol exaustivo com dez bases legais que autorizam o tratamento de dados pessoais. É importante ressaltar que o tratamento de dados pode se basear em mais de uma dessas bases legais (COTS; OLIVEIRA, 2019).

Uma das hipóteses primárias para o tratamento de dados pessoais é a obtenção do consentimento do titular, conforme explicitado na LGPD. Esse consentimento deve ser uma manifestação voluntária, baseada em informações claras e suficientes, na qual o titular concorda expressamente com o tratamento dos seus dados para uma finalidade determinada (BRASIL, 2018).

O consentimento para o tratamento de dados pessoais pode ser expresso por escrito, com destaque em relação às demais cláusulas contratuais. Contudo, é válido destacar que a legislação permite que o consentimento seja demonstrado de outras formas estabelecidas em lei. Diante do progresso tecnológico, novas alternativas têm emergido, tais como o uso de tokens, SMS, autenticações por e-mail e login, entre outros meios, que também podem ser utilizados para manifestar o consentimento de forma válida (COTS; OLIVEIRA, 2019).

Complementam os autores sobre:

[...] (i) preservada e inequívoca; (ii) seja inteligível, ou seja, deve ser compreensível caso precise ser comprovada, especialmente perante as esferas judiciais; e (iii) esteja adequadamente atrelada aos termos do tratamento de dados, isto é, é necessário comprovar que determinado consentimento se deu sobre determinado tratamento [...]. (COTS; OLIVEIRA, 2019, p. 92).

Consequentemente, é responsabilidade do controlador do tratamento de dados pessoais o ônus de comprovar que o consentimento foi devidamente fornecido, em conformidade com as disposições legais aplicáveis (BRASIL, 2018).

Conforme previsto nos parágrafos 4º e 6º do artigo 8º nota-se, “[...] se em relação ao consentimento original houver alteração posterior quanto à finalidade específica do tratamento, forma, duração ou compartilhamento, a informação deve ser fornecida ao titular que, caso não concorde, poderá revogar o consentimento”. (COTS; OLIVEIRA, 2019).

O titular dos dados tem o direito de revogar o consentimento a qualquer momento, mediante um procedimento gratuito e de fácil acesso. É importante ressaltar que o processamento dos dados pessoais deve permanecer inalterado até que o titular solicite expressamente a exclusão das informações, conforme estabelecido no artigo 18 da LGPD (BRASIL, 2018).

Adicionalmente, de acordo com o parágrafo 5º do artigo 7º da LGPD, é exigido um consentimento específico do titular para a comunicação ou compartilhamento de dados entre diferentes controladores. No entanto, a legislação não fornece uma orientação precisa sobre como essa especificação deve ser realizada. Dessa forma, presume-se que essa especificação deva ser incluída no contrato, juntamente com a identificação do controlador com quem pretende-se compartilhar os dados pessoais do titular (COTS; OLIVEIRA, 2019).

É válido destacar que dados pessoais de acesso público podem ser objeto de tratamento sem a necessidade de consentimento do titular, desde que o controlador possua outras bases legais elencadas na LGPD que justifiquem esse tratamento (BRASIL, 2018).

É fundamental destacar que a dispensa de consentimento para o tratamento de dados pessoais se aplica somente aos casos em que os dados são tornados públicos por vontade explícita do titular. Dessa forma, dados divulgados por terceiros, como aqueles encontrados em diários oficiais, não se enquadram nessa hipótese de dispensa. Além disso, mesmo nos casos em que os dados são públicos, o tratamento deve ser realizado de acordo com a finalidade legítima e com base na boa-fé do interesse público (COTS; OLIVEIRA, 2019).

A regulamentação estabelecida pela LGPD no que diz respeito ao crédito desempenha um papel fundamental na proteção dos direitos do titular de dados pessoais que estão armazenados em bancos de dados e utilizados em fórmulas estatísticas para a atribuição de rankings de crédito (OLIVA; VIÉGAS, 2020).

Fica evidente que o legislador teve a preocupação de envolver ativamente o titular no processo de suas informações pessoais, estimulando um comportamento proativo por parte do indivíduo e estabelecendo a responsabilidade dos agentes no tratamento dessas informações (TEPEDINO; TEFFÉ, 2020).

3.6.4.2 Os sujeitos e os órgãos na lei geral de proteção de dados

A Lei Geral de Proteção de Dados (LGPD) estabelece a participação de diferentes sujeitos e órgãos para garantir a proteção adequada dos dados pessoais. Alguns dos principais sujeitos e órgãos mencionados na LGPD são:

O titular dos dados é a pessoa a quem os dados se referem e que está sendo alvo da coleta. Conforme mencionado por diversos especialistas na área de proteção de dados, como Antônio Henrique Albani Siqueira (s/p, 2019), “[...] titular dos dados pessoais é a pessoa natural que detém os direitos de livremente dispor dos dados pessoais”.

Entretanto, Siqueira (s/p, 2019, apud DINIZ, 2010);

[...] os direitos da personalidade são absolutos (possuem efeito erga omnes e implicam um dever geral de abstenção), intransmissíveis (são inseparáveis de seu titular), indisponíveis (inalienáveis), ilimitados, imprescritíveis e inexpropriáveis (inatos, adquiridos no instante da concepção e protegidos mesmo após o falecimento).

Conforme estabelecido pela Lei Geral de Proteção de Dados (LGPD), o Controlador será a pessoa física ou jurídica responsável por todas as decisões relacionadas ao tratamento dos dados pessoais dos titulares. É o que a LGPD nos apresenta a pessoa do Controlador (BLUM, 2020).

É necessário analisar, também o Controlador, Operador e Encarregado, a respeito do Controlador terá a responsabilidade de elaborar, quando solicitado pela autoridade competente, um relatório de impacto à proteção de dados referente às operações de tratamento de dados, corrobora a explicação de Siqueira (s/p, 2019):

A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados. Tais relatórios deverão conter, no mínimo, a

descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), surge o papel do Operador, que é responsável por realizar a coleta e o tratamento dos dados em conformidade com as instruções do Controlador. Conforme mencionado por Siqueira (s/p, 2019), a LGPD classifica tanto o Controlador quanto o Operador como 'agentes de tratamento'. Ambos possuem a responsabilidade de manter registros detalhados de todas as operações relacionadas ao tratamento de dados.

Por fim o Encarregado, conforme mencionado por especialistas no assunto, como Maria Carolina Cardoso (s/p, 2021), desempenha o papel de intermediário entre o Controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Ele pode ser tanto uma pessoa física quanto uma pessoa jurídica, ficando a critério do Controlador fazer essa escolha.

3.6.2.3 As ações

Conforme mencionado por Daniel Donda (2020), uma abordagem eficaz para estar em conformidade com a LGPD envolve a implementação de várias ações, tais como:

- Estabelecer um comitê responsável pela análise e tomada de decisões relacionadas à proteção de dados;
- Designar um Oficial de Proteção de Dados (DPO) para supervisionar e garantir a conformidade com a LGPD;
- Mapear e compreender o ciclo de vida dos dados, desde a coleta até a exclusão;
- Adotar regulamentos e padrões de segurança da informação para garantir a proteção adequada dos dados;
- Realizar auditorias e monitorar regularmente o ambiente de tratamento de dados;
- Elaborar um relatório de impacto à proteção de dados pessoais, avaliando os riscos associados às operações de tratamento de dados;
- Desenvolver um plano de ação para lidar com situações de emergência relacionadas à proteção de dados.

Ademais, a adoção de ações adequadas é fundamental para garantir a conformidade com a legislação de proteção de dados, como a LGPD. As organizações devem implementar medidas de segurança da informação, políticas internas, treinamentos e controles para proteger os dados pessoais de seus titulares (BRASIL, 2018).

3.2.3.4 Os instrumentos

Cabe salientar que a Lei Geral de Proteção de Dados (LGPD) prevê diversos instrumentos que visam garantir a proteção dos dados pessoais. Alguns desses instrumentos incluem estão previstos no artigo 7º e seguintes, que dispõe:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

(BRASIL, 2018)

É importante ressaltar que cada organização deve adaptar esses instrumentos de acordo com suas necessidades específicas e as exigências da legislação. Além disso, a implementação efetiva da LGPD requer um comprometimento contínuo com a atualização e aprimoramento desses instrumentos, em consonância com os avanços tecnológicos e as mudanças nas práticas de tratamento de dados (MACIEL, 2019).

4. A UTILIZAÇÃO DO RECONHECIMENTO FACIAL PARA FINS DE CONSUMO E A QUESTÃO DO TRATAMENTO DA IMAGEM NA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A utilização do reconhecimento facial para fins de consumo envolve tecnologia para identificar e autenticar clientes, personalizar experiências de compra, melhorar a segurança nas transações e oferecer serviços mais eficientes (DONEDA, 2021).

A utilização do reconhecimento facial para fins de consumo pode oferecer benefícios significativos para empresas e consumidores, mas é importante garantir que seja realizada de forma ética, transparente e em conformidade com as regulamentações de proteção de dados (BARROS, 2018).

A utilização do reconhecimento facial para fins do consumidor está sujeita às disposições da Lei Geral de Proteção de Dados (LGPD) no Brasil em relação ao tratamento de imagem. É essencial obter o consentimento do titular dos dados, adotar medidas de segurança adequadas e respeitar os direitos dos indivíduos em relação ao tratamento de sua imagem (BARRETTO, 2020).

A utilização do reconhecimento facial para fins de consumo tem despertado crescente interesse e levantado importantes questões no âmbito da proteção de dados pessoais. Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD) no Brasil, a abordagem desse tema tornou-se ainda mais relevante, exigindo uma análise aprofundada das implicações legais e éticas do tratamento da imagem nesse contexto.

Nessa perspectiva, o jurista Danilo Doneda tem contribuído no campo da privacidade e proteção de dados, sobre a relação entre o uso do reconhecimento facial para fins de consumo e as disposições da LGPD. Esta pesquisa pretende explorar as considerações trazidas por Doneda (2021), destacando a importância de uma abordagem responsável e ética na utilização dessa tecnologia, em consonância com os princípios e diretrizes estabelecidos pela LGPD.

No que diz respeito ao tratamento da imagem, Doneda (2021), destaca que a captura e o uso de imagens faciais se enquadram como dados pessoais sensíveis, uma vez que podem revelar informações biométricas e traços identificáveis dos indivíduos. Nesse sentido, a LGPD estabelece que o tratamento de dados pessoais sensíveis requer um nível maior de proteção e que deve ser respaldado por bases legais específicas.

Como Barros (2018) destaca, é essencial que haja medidas adequadas para proteger esses dados contra acesso não autorizado, divulgação ou uso indevido. Isso implica que as organizações que coletam e armazenam dados de reconhecimento facial devem implementar medidas técnicas e organizacionais robustas.

O jurista também salienta a importância de os indivíduos terem o direito de acessar, retificar e, se necessário, excluir seus dados pessoais, incluindo as imagens faciais coletadas. Isso está em consonância com os direitos previstos na LGPD, que visam garantir a autonomia e o controle dos titulares sobre suas informações pessoais (DONEDA, 2021).

Ainda a necessidade de segurança adequada para proteger os dados de reconhecimento facial contra acesso não autorizado, divulgação ou uso indevido. Ressaltando que as organizações devem implementar medidas técnicas e organizacionais robustas para garantir a integridade e confidencialidade desses dados (BARROS, 2018).

Com isso, Barros (2018), também aborda a importância do direito dos indivíduos à transparência e ao acesso aos seus dados pessoais, incluindo as informações capturadas por meio do reconhecimento facial. As pessoas devem, dessa forma, ter a possibilidade de retificar ou excluir esses dados, caso necessário, de acordo com as disposições da LGPD.

4.1 A IMPORTÂNCIA DO CONSENTIMENTO NA PROTEÇÃO DE DADOS PESSOAIS

A importância do consentimento na proteção de dados pessoais é fundamental para garantir a privacidade e a autonomia dos indivíduos. O consentimento é uma das bases legais para o tratamento de dados, conforme previsto na Lei Geral de Proteção de Dados (LGPD) e em outras legislações de proteção de dados em diversos países (BIONI, 2018).

Dessa forma, o consentimento é uma manifestação livre, informada e inequívoca do titular dos dados, em que ele concorda com o tratamento de suas informações pessoais para uma finalidade específica. Ele deve ser obtido de forma clara e transparente, por meio de uma linguagem acessível e de fácil compreensão (MACIEL, 2018).

No entanto, ao fornecer seu consentimento, o titular dos dados tem o controle sobre suas informações pessoais, podendo decidir quais dados deseja compartilhar, para qual finalidade e com quem. Isso permite que as pessoas exerçam seu direito à autodeterminação informativa e tenham maior participação no processo de tratamento de seus dados (MACIEL, 2018).

Maciel (2018), explica ainda, “Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;”.

A importância do consentimento na proteção de dados pessoais é fundamental para garantir a privacidade e a autonomia dos indivíduos. De acordo com a Lei Geral de Proteção de Dados (LGPD), o consentimento é uma manifestação livre, informada e inequívoca do titular dos dados, em que ele concorda com o tratamento de suas informações pessoais para uma finalidade específica (ACCIOLY, 2018).

A Lei Geral de Proteção de Dados (LGPD) trouxe uma série de mudanças significativas na forma como as empresas lidam com os dados pessoais de seus clientes e funcionários. Uma dessas mudanças diz respeito ao consentimento do titular dos dados, que é um dos pilares da LGPD. No entanto, a questão do consentimento se torna mais complexa quando se trata de relações de trabalho, Santos (2020), aborda essa questão:

Embora o consentimento seja dispensado nas hipóteses de “execução de contrato ou de procedimentos relacionados a contrato do qual seja parte o titular dos dados do empregado” o seu tratamento merece ainda mais cautela, para não ferir a privacidade do trabalhador, ocasionando danos à imagem, danos de natureza moral, além de prejuízos de ordem material ao empregador. As violações previstas poderão ser objeto de reclamação trabalhista e denúncias ao MPT (Ministério Público do Trabalho), bem como sujeitas à fiscalização da ANPD (Autoridade Nacional de Proteção de Dados) com sanções disciplinares previstas o art. 52 da Lei Treinamento e conscientização do uso devido dos dados pessoais, aliados ao departamento de Recursos Humanos (RH), tem papel primordial na adequação à LGPD e compliance.

No contexto das transações bancárias, o consentimento desempenha um papel crucial. As instituições financeiras, ao coletar e tratar dados pessoais, devem obter o consentimento do titular dos dados. Isso se torna ainda mais relevante na era digital, onde as transações bancárias são cada vez mais realizadas por meios digitais (SANTOS, 2020).

Quando se trata de dados sensíveis, como dados biométricos ou de saúde, a necessidade de consentimento é ainda mais crítica. A LGPD estabelece regras específicas para o tratamento desses tipos de dados, exigindo não apenas o consentimento do titular dos dados, mas também garantindo que esses dados sejam tratados de maneira segura e confidencial (ALMEIDA, 2022).

A revogação do consentimento é um direito fundamental do titular dos dados, podendo ser exercido a qualquer momento, por meio de uma manifestação expressa. Esse processo deve ser gratuito e facilitado, garantindo ao titular o controle sobre suas informações pessoais (ACCIOLY, 2018).

O cenário digital não dispõe de outro caminho a não ser estar preparado para interagir e atender as regulamentações. No entanto, é importante que as empresas, instituições e organizações, estejam alinhadas com o armazenamento e tratamento das informações de titulares, e apostos para atender às solicitações, na mesma velocidade da era digital. Além disso, a ambiente pesquisa e educacional, deve servir

de exemplo ao tratar dos direitos humanos e ao estar em conformidade com as Leis. Caso contrário, arcarão com sanções, multas pesadas e advertências severas. (ALMEIDA, 2022)

Além disso, o consentimento é uma forma de promover a confiança entre os indivíduos e as organizações responsáveis pelo tratamento dos dados. Ao obter o consentimento de forma adequada, as empresas demonstram seu compromisso com a proteção da privacidade e mostram respeito pelos direitos e interesses dos titulares dos dados.

Assim, o consentimento desempenha um papel essencial na proteção de dados pessoais, assegurando que o tratamento seja realizado de forma ética, transparente e em conformidade com a legislação (SANTOS, 2020). No entanto, o consentimento por si só não é suficiente. É igualmente importante que as organizações tratem os dados de maneira ética e transparente. Isso significa que as organizações devem ser claras sobre como e por que estão usando os dados, e devem tomar medidas para proteger os dados contra acesso não autorizado ou uso indevido.

Além disso, o consentimento é uma forma de promover a confiança entre os indivíduos e as organizações responsáveis pelo tratamento dos dados. Ao obter o consentimento de forma adequada, as empresas demonstram seu compromisso com a proteção da privacidade e mostram respeito pelos direitos e interesses dos titulares dos dados (KOHLS, 2021).

Assim, o consentimento desempenha um papel essencial na proteção de dados pessoais, assegurando que o tratamento seja realizado de forma ética, transparente e em conformidade com a legislação. Ao valorizar e respeitar o consentimento dos titulares dos dados, é possível construir relações de confiança e fortalecer a proteção da privacidade no ambiente digital (KOHLS, 2021).

Nota-se, que a questão do consentimento é um aspecto crucial destacado pelo artigo 8º da legislação, especialmente no contexto da coleta de dados. Ao longo dos anos, com o avanço da tecnologia e o crescente valor das informações pessoais, a necessidade de obter o consentimento do indivíduo para a coleta de seus dados tem ganhado cada vez mais importância. Isso ocorre devido à crescente sensibilidade e vulnerabilidade associadas às informações pessoais no ambiente virtual (PINHEIRO, 2018).

Ademais, a revogação do consentimento é um direito fundamental do titular dos dados, podendo ser exercido a qualquer momento, por meio de uma manifestação expressa. Esse processo deve ser gratuito e facilitado, garantindo ao titular o controle sobre suas informações pessoais. É importante ressaltar que os tratamentos realizados com base no consentimento anteriormente concedido permanecem válidos, desde que não haja um pedido de eliminação dos dados. Além disso, é importante destacar que o consentimento não é exigido para dados que tenham sido tornados manifestamente públicos pelo próprio titular (GROSSI, 2020).

4.2 O RECONHECIMENTO FACIAL PARA COLETA DE DADOS PARA FINS COMERCIAIS.

A utilização do reconhecimento facial para a coleta de dados para fins comerciais tem se tornado cada vez mais comum em diversos setores, como varejo, publicidade e marketing, essa tecnologia permite identificar e rastrear indivíduos com base em suas características faciais, o que pode fornecer informações valiosas para empresas sobre seus clientes e consumidores em potencial (SIMÃO, 2020).

No entanto, essa prática também levanta preocupações significativas em relação à privacidade e proteção de dados pessoais. O reconhecimento facial pode envolver o processamento de dados biométricos sensíveis, que são considerados informações pessoais especialmente protegidas. Por tanto é essencial que as empresas que utilizam essa tecnologia estejam em conformidade como a Lei Geral de Proteção de Dados (LGPD) no Brasil (SIMÃO, 2020).

Conforme demonstrado por Zaidan (2019), sendo o Projeto de Lei n. 2.537/2019, poderá ser estabelecida a obrigatoriedade de utilização de placas ou adesivos fixados nas entradas dos estabelecimentos comerciais, com o intuito de informar aos consumidores sobre a utilização de programas de reconhecimento facial. Essa medida tem como objetivo promover a transparência e garantir que os indivíduos estejam cientes de que suas imagens estão sendo capturadas e processadas para fins de identificação. Essa iniciativa busca também fomentar a conscientização dos consumidores em relação à proteção de seus dados pessoais no contexto do reconhecimento facial.

Por tais razões, a tecnologia de reconhecimento facial está se tornando cada vez mais presente no debate público. É comum que seja apresentada como uma solução “conveniente” ou “eficiente” para as pessoas em geral (PASQUALE, 2015).

Nessa linha, dispõe o Código Civil de 2002 sobre o cuidado ao direito à imagem em seu art. 20:

Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes (BRASIL, 2002).

O debate em curso sobre a utilização de um dos atributos mais distintivos, o rosto, não

consegue acompanhar o ritmo da imaginação daqueles que desenvolvem e comercializam essa tecnologia para o mercado e para as autoridades. Avanços na tecnologia de reconhecimento facial continuam a ocorrer de forma acelerada, e com isso levanta preocupações sobre a falta de regulamentação adequada e o potencial abuso de poder que essas tecnologias podem conferir (KUTTERER *et. al*, 2020).

Do ponto de vista ético, é imperativo considerar o impacto potencial do reconhecimento facial na discriminação e no viés algorítmico. O uso inadequado dessa tecnologia pode acarretar resultados injustos e violações dos direitos humanos, como a discriminação com base em raça, gênero ou outras características protegidas. Assim, é crucial garantir a equidade e imparcialidade no desenvolvimento e aplicação dos algoritmos de reconhecimento facial (KUTTERER *et. al*, 2020).

Um dos principais desafios reside na garantia de obter o consentimento adequado por parte dos indivíduos para a coleta e o uso de suas informações faciais. É fundamental que as empresas forneçam informações claras e transparentes sobre as finalidades e os métodos de tratamento dos dados, permitindo que os consumidores tomem decisões devidamente informadas acerca da divulgação de suas informações pessoais (BIONI, 2021).

O art. 2º da LGPD também dispõe como fundamento a inviolabilidade da intimidade, honra e da imagem:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

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. (BRASIL, 2018)

Ademais, a segurança dos dados constitui uma preocupação crítica. O armazenamento e processamento de informações faciais exigem a implementação de medidas de segurança robustas com o intuito de prevenir o acesso não autorizado e assegurar a confidencialidade e

integridade dos dados coletados. Nesse sentido, as organizações devem adotar salvaguardas técnicas e organizacionais apropriadas para mitigar os riscos de violação e vazamento de informações.

A utilização do reconhecimento facial para fins comerciais abre um amplo leque de possibilidades em termos de como essa tecnologia pode ser empregada. Os fins comerciais referem-se à aplicação do reconhecimento facial no contexto das atividades comerciais, visando melhorar a experiência do consumidor, aumentar a eficiência operacional e personalizar os serviços oferecidos (RESENDE, 2019).

Uma das principais maneiras como o reconhecimento facial pode ser utilizado para fins comerciais é na autenticação e segurança do acesso a locais físicos ou digitais. Por exemplo, empresas podem adotar essa tecnologia para permitir o acesso seguro a prédios, escritórios ou até mesmo a dispositivos eletrônicos, substituindo senhas ou cartões de acesso por reconhecimento facial. Isso proporciona conveniência e segurança, além de eliminar a necessidade de lembrar e gerenciar múltiplas senhas (RECONHECIMENTO..., 2019).

Segundo Bárbara Simão, o reconhecimento facial também pode ser aplicado em setores como segurança, transporte, hospedagem e entretenimento. Em aeroportos, por exemplo, a tecnologia pode ser utilizada para o controle de fronteiras, facilitando o processo de embarque e desembarque. Na indústria hoteleira, hotéis podem empregar o reconhecimento facial para agilizar o check-in e garantir maior segurança aos hóspedes (SIMÃO, 2020).

No entanto, é importante ressaltar que o uso do reconhecimento facial para fins comerciais deve ser realizado de maneira responsável e ética. As empresas devem estar em conformidade com as leis de proteção de dados e garantir a segurança e a privacidade das informações coletadas. O consentimento informado dos indivíduos deve ser obtido de forma transparente, e medidas adequadas devem ser adotadas para evitar discriminação e garantir a justiça e a imparcialidade no tratamento dos dados faciais (PASQUALE, 2015).

Por tais razões, a tecnologia de reconhecimento facial está se tornando cada vez mais presente no debate público. É comum que seja apresentada como uma solução “conveniente” ou “eficiente” para as pessoas em geral (PASQUALE, 2015).

4.3 RECONHECIMENTO FACIAL PARA FINS COMERCIAIS À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

O reconhecimento facial para fins comerciais refere-se à utilização de tecnologia de

reconhecimento facial por empresas e organizações para diversos propósitos relacionados aos seus negócios. Essa tecnologia permite identificar e verificar a identidade de indivíduos com base em características faciais únicas (TEIXEIRA; ARMELIN, 2020).

A legislação aprovada em 2018 é aplicável à utilização de reconhecimento facial para fins comerciais, com exceção de sua utilização para fins de segurança. A lei proíbe a inclusão de dados biométricos em bancos de dados comerciais, a menos que sejam observadas três opções: fornecer um aviso aos indivíduos afetados, que deve ser facilmente acessível; obter consentimento expresso, que deve ser renovado a cada novo uso comercial; ou oferecer um mecanismo para evitar o uso posterior de identificadores biométricos para fins comerciais (BIONI, 2021).

O Artigo 11 da Lei Geral de Proteção de Dados (LGPD) do Brasil estabelece as condições sob as quais o tratamento de dados pessoais sensíveis pode ocorrer. Dados pessoais sensíveis são categorias especiais de dados que são particularmente sensíveis e, portanto, requerem maior proteção. Isso inclui informações sobre a origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos, dados relativos à saúde ou à vida sexual ou orientação sexual de uma pessoa natural.

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2019)

O consentimento do titular dos dados é geralmente necessário para o tratamento de dados pessoais sensíveis. No entanto, existem algumas exceções a essa regra. Por exemplo, o tratamento de dados pessoais sensíveis pode ser necessário para o cumprimento de uma obrigação legal ou regulatória pelo controlador, para a realização de estudos por um órgão de pesquisa, para a proteção da vida ou da incolumidade física do titular ou de terceiro, entre outros.

Além disso, é importante notar que mesmo quando o tratamento de dados pessoais sensíveis é permitido, ele deve ser realizado de acordo com os princípios e requisitos estabelecidos pela LGPD. Isso inclui a necessidade de garantir a segurança dos dados, respeitar os direitos dos titulares dos dados e, sempre que possível, anonimizar os dados pessoais sensíveis.

A exceção para a utilização de reconhecimento facial para fins de segurança é uma medida importante que equilibra a necessidade de proteger a privacidade individual com a necessidade de garantir a segurança pública. Em contextos de segurança, o uso de tecnologias de reconhecimento facial pode ser crucial para identificar suspeitos, encontrar pessoas desaparecidas ou prevenir atividades criminosas (ARAÚJO, 2021).

No entanto, mesmo nesses casos, é essencial que haja salvaguardas adequadas para prevenir abusos. Por exemplo, o acesso aos dados biométricos coletados deve ser estritamente limitado ao pessoal autorizado e deve haver políticas claras sobre quando e como esses dados podem ser usados. Além disso, deve haver mecanismos de responsabilização para garantir que qualquer uso indevido dos dados seja adequadamente punido (ARAÚJO, 2021).

Em última análise, a exceção para fins de segurança na legislação brasileira reflete um compromisso entre proteger a privacidade individual e garantir a segurança pública. É um exemplo de como as leis podem evoluir para lidar com as complexidades apresentadas pelas novas tecnologias (GUEDES, 2021).

A lei estabelece que é necessário informar previamente os indivíduos sobre a coleta de dados biométricos para fins comerciais e obter o seu consentimento. É proibida a venda, locação ou divulgação dos dados biométricos coletados para fins comerciais, a menos que haja autorização por lei federal, cumprimento de obrigações legais, realização de transações

financeiras autorizadas pelo titular dos dados, ou autorização do titular para a divulgação em caso de investigação de desaparecimento ou morte (BIONI,2021).

Várias cidades e estados têm implementado sistemas para comparar fotos de suspeitos com registros de bancos de dados. Por exemplo, o estado de São Paulo adotou um dos principais sistemas de reconhecimento facial para segurança pública no Brasil. Este sistema, utilizado pela Polícia Civil, compara imagens de câmeras com uma base de dados com mais de 30 milhões de RGs emitidos no estado (SILVA, 2020).

A utilização de algoritmos e tecnologias de reconhecimento facial tem se tornado cada vez mais comum em diversas áreas da sociedade. No entanto, a falta de transparência e a possibilidade de viés nos algoritmos têm levantado preocupações significativas. Araujo (2021), aborda essas questões em detalhes, destacando as implicações do racismo estrutural no desenvolvimento e aplicação dessas tecnologias:

Outra preocupação que cabe relevo é o fato de que a empresa não expunha ao certo como era o funcionamento do algoritmo do COMPAS, de forma que o réu submetido ao software não conseguia questionar o resultado, visto que não se sabia sequer como foi calculado o seu risco. Fato é que os únicos com acesso total aos algoritmos são os próprios programadores. A reflexão disso no contexto em que o racismo estrutural é a regra é, naturalmente, que os modelos desenvolvidos sejam enviesados a partir das concepções racistas de seus criadores. Não é novidade que no Brasil o racismo permeia a sua história desde o descobrimento, e mesmo sendo maioria dentre a população, os negros são os menos favorecidos na educação, são mais pobres, são minoria no mercado de trabalho e com salários menores, tem menos saneamento básico, são mais dependentes do sistema único de saúde - SUS, e não ocupam, ou se ocupam é de forma irrisória os altos cargos do país, tem baixíssima representatividade política, e são maioria no sistema carcerário, sendo relevante que, pelo que se verifica, o risco destes dados serem transpostos para os softwares de reconhecimento facial é extremamente elevado.

No entanto, a expansão dessas tecnologias em uma sociedade permeada pelo racismo estrutural levanta questões sobre a precisão dos novos instrumentos de monitoramento e vigilância pública. Especialistas em direito digital alertam para os riscos que essas ferramentas podem trazer à população, incluindo o tratamento inadequado dos dados dos cidadãos e a possibilidade de erros nos sistemas (ARAUJO, 2021)..

O reconhecimento facial é uma tecnologia emergente que tem o potencial de revolucionar a maneira como interagimos com o mundo ao nosso redor. No entanto, também levanta questões significativas sobre privacidade e consentimento. A Lei nº 2537/2019 aborda essas preocupações ao exigir que os estabelecimentos comerciais informem claramente aos clientes quando o reconhecimento facial está sendo usado (BRASIL, 2019).

A lei é um passo importante para garantir que os direitos dos consumidores sejam protegidos na era digital. Ao exigir que os estabelecimentos comerciais divulguem o uso do reconhecimento facial, a lei dá aos consumidores a oportunidade de tomar decisões informadas sobre onde fazer compras e quais empresas apoiar (ALVES, 2022).

Como exemplo de prática ilícita de exposição de dados pessoais sensíveis de empregados, temos a decisão de Julho de 2020 dos julgadores da Segunda Turma do TRT3-MG, que, sem divergência, manteve sentença proferida pela 24ª Vara do Trabalho de Belo Horizonte. A juíza convocada MM. Maria Cristi na Diniz Caixeta entendeu que, pelas provas colhidas, ficaram claros os danos morais em virtude da exposição indevida da intimidade do trabalhador. A Justiça do Trabalho determinou que a empresa pague indenização por danos morais a um ex-empregado do setor administrativo que teve seus dados sigilosos expostos no sistema interno de informação da empresa. Um trabalhador da companhia confirmou, no processo que, ao fazer pesquisa no sistema, deparou-se com o relatório médico do autor da ação, com a indicação de que ele tinha pensamentos suicidas e era usuário de cocaína. Para a juíza convocada Maria Cristi na Diniz Caixeta, a conduta da empresa revelou o dano sofrido, já que a exposição de dados de cunho pessoal certamente causou dano moral ao autor. E, diante das provas, a magistrada reforçou que não via elementos capazes de afastar o direito do reclamante à reparação por dano moral. A julgadora manteve o valor fixado para a indenização, de três salários do trabalhador, por entender que o montante atende à finalidade de atenuar as consequências da lesão jurídica e reveste-se de razoabilidade. (TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO, 2020). Neste sentido, no caso de tratamento de dados pessoais sensíveis, com risco elevado no tratamento incluindo dados. (SANTOS, 2020)

No entanto, a lei também pode enfrentar desafios. Por exemplo, pode ser difícil para os estabelecimentos comerciais implementar efetivamente avisos de reconhecimento facial. Além disso, alguns podem argumentar que a lei não vai longe o suficiente para proteger a privacidade do consumidor (ALVES, 2022).

Por fim, é importante ressaltar que a falta de legislação específica no âmbito federal que proteja os dados tratados pela segurança pública, combinada com o uso de algoritmos sujeitos a erros, pode potencializar o desrespeito à igualdade e colocar em risco as garantias e direitos fundamentais constitucionalmente previstos. Portanto, é crucial que haja um debate contínuo sobre como equilibrar a necessidade de segurança pública com a proteção da privacidade individual (SILVA, 2020).

No contexto, além das discussões acadêmicas e doutrinárias sobre o uso do reconhecimento facial para fins comerciais, é importante mencionar o Projeto de Lei nº 2537/2019, em tramitação na Câmara dos Deputados. Este projeto propõe que estabelecimentos comerciais sejam obrigados a informar os titulares dos dados sobre o uso do reconhecimento facial para identificação. Uma das principais medidas previstas no projeto é a obrigatoriedade de colocar avisos visíveis aos consumidores na entrada dos estabelecimentos, informando sobre a utilização dos dados e como os consumidores podem exercer seus direitos em relação

à proteção de dados pessoais (TEIXEIRA JUNIOR, 2019).

A intenção não é proibir ou inviabilizar o uso do reconhecimento facial, mas sim estabelecer um ambiente propício para a sua utilização responsável e ética. É essencial estabelecer regulamentações adequadas, garantir transparência no uso da tecnologia e promover a conscientização dos usuários e das empresas sobre os impactos e responsabilidades envolvidos (TEIXEIRA JUNIOR, 2019).

4.4 O ENTENDIMENTO DOUTRINÁRIO ACERCA DA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PARA FINS COMERCIAIS

Observa-se, de maneira semelhante, que a discussão sobre o reconhecimento facial no âmbito doutrinário ainda é limitada. Bioni (2021), explica que a atual legislação proíbe a inclusão de dados comerciais, a menos que sejam observadas as três opções que são o consentimento; finalidade específica e proteção adequada.

No entanto Simão (2020), fala sobre a utilização do reconhecimento facial para a coleta de dados para fins comerciais que tem se tornado cada vez mais comum e crescido de forma rápida em diversos fatores.

Desta forma sobre o avanço rápido do reconhecimento facial e coleta de dados para fins comerciais, é importante analisar que os riscos à privacidade e à intimidade não se limitam mais às relações de consumo em si, Misugi, Freitas, Efig (2016), ressalta que isso ocorre porque qualquer indivíduo que esteja em um espaço público, e até mesmo em um ambiente privado, pode se tornar alvo de investigações instantâneas e abrangentes por meio de tecnologias como o reconhecimento facial.

O reconhecimento facial é uma tecnologia emergente que tem o potencial de revolucionar a maneira como interagimos com o mundo ao nosso redor. No entanto, também levanta questões significativas sobre privacidade e consentimento. A Lei nº 2537/2019 aborda essas preocupações ao exigir que os estabelecimentos comerciais informem claramente aos clientes quando o reconhecimento facial está sendo usado (BRASIL, 2019).

A LGPD é expressa no que se refere ao tratamento de dados pessoais. É mandatória a obtenção de consentimento do titular dos dados para sua utilização. Sendo necessário, ainda, que as informações obtidas sejam processadas estritamente às finalidades informadas pelo controlador, sem desvio de finalidade de qualquer natureza. Vale ressaltar, que há hipóteses de flexibilização dessas situações, as quais são taxativas e expressas na LGPD. A regra geral, basicamente, é a de que o controlador seja capaz de justificar e comprovar a obtenção de consentimento, a finalidade para a qual tratou os dados, a duração desse procedimento e a forma como ocorreu.

Desse modo, um recurso tão individual e privativo dos indivíduos como o reconhecimento facial, tem sua proteção englobada na LGPD e assim como para o tratamento de dados pessoais sensíveis somente poderá ocorrer mediante consentimento do titular ou de seu responsável legal. O que deve ocorrer de forma específica e para finalidades a que se for proposto. Sendo a ausência de consentimento apenas viável se a finalidade for uma das hipóteses expressas da LGPD, como por exemplo, para o exercício regular de direitos em processos judiciais.

Vale destacar que não basta a obtenção do consentimento para a utilização do reconhecimento facial. O controlador ou o operador deve, ainda, cumprir uma série de requisitos, como a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de incidentes de segurança e a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos. Estando sujeitos à fiscalização da Autoridade de Proteção de Dados (ANPD) competente, e das regulamentações por ela provisionadas. (SOLERE, 2021)

A lei é um passo importante para garantir que os direitos dos consumidores sejam protegidos na era digital. Ao exigir que os estabelecimentos comerciais divulguem o uso do reconhecimento facial, a lei dá aos consumidores a oportunidade de tomar decisões informadas sobre onde fazer compras e quais empresas apoiar (ALVES, 2022).

No entanto, a lei também pode enfrentar desafios. Por exemplo, pode ser difícil para os estabelecimentos comerciais implementar efetivamente avisos de reconhecimento facial. Além disso, alguns podem argumentar que a lei não vai longe o suficiente para proteger a privacidade do consumidor (ALVES, 2022).

Embora as câmeras de vigilância sejam o exemplo mais óbvio, o uso do reconhecimento facial com o objetivo de identificar pessoas também possui diversas aplicações comerciais, sendo adotada por empresas em diferentes setores, como varejo, marketing e serviços financeiros (SIMÃO, 2020).

Com tal delineamento D’Urso (2020), traz que é importante destacar que a introdução de novas tecnologias, como o reconhecimento facial, pode trazer benefícios significativos na busca por uma sociedade mais segura. No entanto, é crucial não esquecer ou ignorar os potenciais efeitos prejudiciais do mau uso e da utilização inadequada desse sistema, o que certamente comprometeria o direito à privacidade das pessoas.

Desta forma, Resende (2019) destaca que, longe de ser uma prática prejudicial, pelo menos em sua forma aparente, a ampla gama de funcionalidades do reconhecimento facial na relação com o consumidor pode ser encarada como benéfica:

[...] No Brasil, essa realidade não está longe e algumas redes começam a testar sistemas de reconhecimento facial que permitem verificar as reações dos clientes de forma que a loja ajuste a disposição de seus produtos ou vitrines para se tornarem mais atrativas e aumentarem as vendas. Restaurantes e outros estabelecimentos também

têm usado a tecnologia como um atrativo a mais para atender às expectativas do consumidor 4.0 [...] Nada de cartões fidelidade nem logins demorados para ser atendido – o pagamento também é feito pelo reconhecimento facial.

Assim apesar de todo o esclarecimento trazido pela doutrina, especialmente diante das rápidas inovações tecnológicas características de uma sociedade da informação, é evidente uma mitigação na proteção da privacidade.

4.5 O ENTENDIMENTO JURISPRUDENCIAL ACERCA DA UTILIZAÇÃO DO RECONHECIMENTO FACIAL PARA FINS COMERCIAIS

A implementação plena da LGPD no Brasil ainda está em andamento, e a discussão sobre o uso do reconhecimento facial na perspectiva jurisprudencial brasileira tem potencial para crescer à medida que a lei entre em vigor e seja amplamente adotada nas práticas cotidianas. Como a LGPD ainda não entrou totalmente em vigor, é importante considerar que os julgamentos não podem se basear em uma lei que ainda não está em vigor. Conforme a implementação da LGPD avança, espera-se que haja uma maior análise jurisprudencial sobre questões relacionadas à utilização do reconhecimento facial e suas implicações legais no contexto brasileiro.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, foi sancionada em agosto de 2018 e entrou em vigor em setembro de 2020 no Brasil. Ela tem como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

A LGPD estabelece regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais, impondo um padrão mais elevado de proteção e penalidades significativas para o não cumprimento.

No contexto da Lei nº 2537/2019, que propõe a obrigatoriedade do aviso sobre o uso de tecnologias de reconhecimento facial em estabelecimentos comerciais, a LGPD é extremamente relevante. O uso de tecnologias de reconhecimento facial envolve a coleta e o processamento de dados biométricos, que são categorizados pela LGPD como dados pessoais sensíveis. Isso significa que as organizações que empregam essa tecnologia devem seguir os princípios e as obrigações estabelecidos pela LGPD (SERPRO, 2022).

A LGPD exige que as organizações obtenham o consentimento explícito para coletar e processar dados sensíveis. No entanto, a Lei nº 2537/2019 não aborda especificamente a questão do consentimento no uso de tecnologias de reconhecimento facial. Isso poderia ser

visto como uma lacuna na legislação que precisa ser abordada para garantir a conformidade total com a LGPD (OPICE, 2020).

É evidente que, considerando a recenticidade tanto do aspecto normativo quanto do aspecto prático, há escassez de casos de jurisprudência que discutam de maneira aprofundada a utilização do reconhecimento facial e a potencial violação dos direitos à imagem e privacidade, bem como a observância dos limites estabelecidos pelos princípios da finalidade previstos na Lei Geral de Proteção de Dados.

Nesse sentido, sobre violação do uso do reconhecimento facial:

APELAÇÃO CÍVEL. DIREITO DO CONSUMIDOR. CONTRATAÇÃO FRAUDULENTA. DESCONTOS INDEVIDOS EMBENEFÍCIO PREVIDENCIÁRIO.

Contratação não comprovada, ainda que por meio de assinatura digital.

"Selfie" que não comprova pactuação por meio de biometria (reconhecimento) facial. Falha na prestação do serviço evidenciada.

Ausência de validade/regularidade da contratação. Banco réu apelante que não se desincumbindo do ônus de provar a contratação do serviço que originou o débito, forçoso é o reconhecimento de sua inexistência. Inteligência do artigo 373, II do CPC. Falha na prestação de serviço demonstrada. Precedentes jurisprudenciais deste Tribunal de Justiça.

Cancelamento dos contratos com a restituição dos valores que se conserva.

Dano moral configurado. Descontos não autorizados realizados no benefício previdenciário da parte autora devem ser considerados abusivos e ilegais, restando o dano *in re ipsa*.

Cenário descrito pela parte autora não pode ser considerado mero dissabor ou aborrecimento, mormente em face da circunstância de que foi privada de valor de seu parco benefício.

Valor do dano extrapatrimonial arbitrado em R\$ 3.000,00 que se conserva, por bem atender aos princípios da proporcionalidade e razoabilidade. Súmula 343 deste Tribunal de Justiça.

Incidência de juros da condenação imposta a título de dano moral que se altera para que seja incidido a partir da data do evento danoso, na forma das Súmulas 54 do STJ e 129 do TJRJ, por se tratar de relação extracontratual.

Conhecimento e parcial provimento do recurso.

(RIO DE JANEIRO, 2023)

O tribunal concluiu que a contratação não foi comprovada, mesmo com o uso de assinatura digital. Uma "selfie" não foi considerada como prova suficiente de um acordo por meio de biometria facial. De acordo com a LGPD, o consentimento do titular dos dados é considerado elemento essencial para o tratamento. A decisão aponta uma falha na prestação do serviço pelo banco réu apelante. A LGPD estabelece que todas as organizações que processam informações sobre pessoas, brasileiras ou não, que estão no território nacional, devem observar a lei.

O tribunal concluiu que a contratação era inválida/irregular e o banco réu apelante não conseguiu provar a contratação do serviço que originou o débito. A LGPD exige que o

tratamento dos dados seja feito levando em conta alguns requisitos, como finalidade e necessidade.

O tribunal considerou que os descontos não autorizados realizados no benefício previdenciário da parte autora devem ser considerados abusivos e ilegais, resultando em dano moral. A LGPD oferece várias garantias ao cidadão, incluindo a possibilidade de solicitar a exclusão dos seus dados pessoais e revogar o consentimento.

Em suma, esta decisão judicial reflete vários princípios fundamentais da LGPD, incluindo a necessidade de consentimento informado para o tratamento de dados pessoais e a responsabilidade das organizações em garantir a proteção desses dados.

Logo, os sistemas de reconhecimento facial apresentam um potencial evidente de violação dos direitos constitucionais, como o direito à privacidade e à autodeterminação informativa. É inegável que a coleta e o processamento de dados biométricos sensíveis por meio desses sistemas podem representar uma ameaça à privacidade individual, bem como ao controle que cada pessoa tem sobre suas informações pessoais (SÃO PAULO, 2020).

Entretanto, existe divergência jurisprudencial sobre o assunto, como evidenciado pela recusa de acesso aos ativos virtuais, conforme decisão proferida pelo Tribunal de Justiça de Santa Catarina:

APELAÇÃO CÍVEL. EMPRÉSTIMO CONSIGNADO. SENTENÇA DE IMPROCEDÊNCIA. RECURSO DA AUTORA. CONTRATO DE EMPRÉSTIMO CONSIGNADO REALIZADO POR MEIO DIGITAL, COM RECONHECIMENTO DE BIOMETRIA FACIAL. REMESSA DE DOCUMENTO DE IDENTIFICAÇÃO IDÊNTICO AO QUE APARELHA A PETIÇÃO INICIAL. DOSSIÊ DA CONTRATAÇÃO NÃO IMPUGNADO PELA APELANTE. COMPROVAÇÃO DA LIBERAÇÃO DE CRÉDITO NA CONTA DA AUTORA. SUPOSTA FRAUDE NÃO COMPROVADA. VALIDADE DO CONTRATO.

PRINCÍPIO DA LIBERDADE DAS FORMAS, EXEGESE DO ART. 107 DO CÓDIGO CIVIL. DIREITO DE ARREPENDIMENTO. ART. 49 DO CÓDIGO DE DEFESA DO CONSUMIDOR. AUTORA QUE ENTROU EM CONTRATO COM O BANCO NO DIA SEGUINTE À CONTRATAÇÃO, MAS NÃO LHE FOI PERMITIDO O CANCELAMENTO DO NEGÓCIO. FALHA NA PRESTAÇÃO DOS SERVIÇOS. NECESSÁRIO CANCELAMENTO DO EMPRÉSTIMO E LIBERAÇÃO DE MARGEM CONSIGNÁVEL. REQUERENTE QUE DEVERÁ DEVOLVER O VALOR DEPOSITADO EM SUA CONTA. DANOS MORAIS.

NÃO ACOLHIMENTO. MERO DESCUMPRIMENTO CONTRATUAL. DESCONTOS QUE SEQUER INICIARAM. AUSÊNCIA DE VIOLAÇÃO À HONRA OU À DIGNIDADE DA AUTORA. SENTENÇA REFORMADA EM PARTE. SUCUMBÊNCIA RECÍPROCA. HONORÁRIOS RECURSAIS INCABÍVEIS. RECURSO CONHECIDO E PARCIALMENTE PROVIDO. (SANTA CATARINA, 2022)

Esta jurisprudência trata de uma apelação cível relacionada a um contrato de empréstimo consignado realizado por meio digital, com reconhecimento de biometria facial.

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Neste caso, a biometria facial é considerada um dado pessoal.

A LGPD estabelece que todas as organizações que processam informações sobre pessoas, brasileiras ou não, que estão no território nacional, devem observar a lei. No entanto, neste caso, a suposta fraude não foi comprovada. Ainda exige que o tratamento dos dados seja feito levando em conta alguns requisitos, como finalidade e necessidade. Neste caso, o tribunal concluiu que o contrato era válido.

Quanto a falha na prestação dos serviços a LGPD estabelece que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser observada. Neste caso, houve uma falha na prestação dos serviços.

Em resumo, esta decisão judicial reflete vários princípios fundamentais da LGPD, incluindo a necessidade de consentimento informado para o tratamento de dados pessoais e a responsabilidade das organizações em garantir a proteção desses dados.

Ainda, modo a ilustrar a inexistência de posicionamento jurisprudencial uníssono, colaciona-se outro julgado.

Conforme destacado por Rover (2020) em relação aos autos em questão, o foco principal das instituições reside na compreensão dos procedimentos de coleta e tratamento de dados. Devido à plena justificativa dos requisitos para a produção de provas, houve a concessão parcial desses pedidos pela competente magistrada, Dra. Renata Barros Souto Maior Baião. Cabe mostrar o posicionamento jurisprudencial uníssono, colaciona-se outro julgado:

APELAÇÃO CÍVEL. RESPONSABILIDADE CIVIL. AÇÃO ANULATÓRIA DE DÉBITO C/C DANOS MORAIS E RESTITUIÇÃO DE VALORES. FRAUDE NA CONTRATAÇÃO DE EMPRÉSTIMO BANCÁRIO CONSIGNADO EM FOLHA DE PAGAMENTO. REPETIÇÃO INDÉBITO. DANOS MORAIS CONFIGURADOS. DEVER DE INDENIZAR RECONHECIDO. QUANTUM MANTIDO. - A INSTITUIÇÃO FINANCEIRA É RESPONSÁVEL PELO BOM FUNCIONAMENTO DOS SERVIÇOS COLOCADOS À DISPOSIÇÃO DO CONSUMIDOR, BEM COMO POR RESGUARDAR A SEGURANÇA E EVITAR QUE OS MESMOS SEJAM VÍTIMAS DE FRAUDES. AQUI, INCIDE PLENAMENTE O ENUNCIADO Nº 479/STJ. TENDO SIDO COMPROVADA FRAUDE NO CASO DOS AUTOS, ACERTADA A DECLARAÇÃO DE NULIDADE DO CONTRATO. - ATUALMENTE SE VIVE EM UM MUNDO DIGITAL. O QUE ANTES ERA REALIZADO PRESENCIALMENTE, COM APRESENTAÇÃO DE DOCUMENTOS FÍSICOS E ASSINATURA GRIFADA NO PAPEL À CANETA, HOJE JÁ PODE SER FEITO POR MEIO DE LIGAÇÃO TELEFÔNICA, SMS, MENSAGENS VIA WHATSAPP, PREENCHIMENTOS DE DADOS EM APLICATIVOS, ENVIO DE DOCUMENTO EM PDF,

ASSINATURA DIGITAL E RECONHECIMENTO FACIAL. - A GAMA DE TECNOLOGIA QUE SE TEM A DISPOR, SEM DÚVIDAS NOS TROUXE DIVERSAS FACILIDADES E, A CONTRÁRIO SENSU, UMA ENORME VULNERABILIDADE QUANTO À SEGURANÇA FINANCEIRA. AS FRAUDES SE TORNARAM MAIS RECORRENTESE OS GOLPES IGUALMENTE, ESPECIALMENTE CONTRA IDOSOS E PESSOAS INDEFESAS. MUITO DISSO SE DÁ PELA FORMA POUCO SEGURA COMO ESTÃO SE DANDO AS TRANSAÇÕES BANCÁRIAS, ONDE AS INSTITUIÇÕES FINANCEIRAS ACABAM SE VALENDO DE SIGNIFICATIVA REDUÇÃO DOS CUSTOS FINANCEIROS COM A UTILIZAÇÃO, MUITAS VEZES, SEM A DEVIDA SEGURANÇA, DE CONTRATAÇÕES INFORMAIS, POR MEIOS DIGITAIS, PODENDO, A DEPENDER DAS CIRCUNSTÂNCIAS, CONFIGURAR FORTUITO INTERNO. - CONTRATAÇÃO FRAUDULENTA. CULPA EXCLUSIVA DE TERCEIRO QUE NÃO EXIME A RESPONSABILIDADE DA RÉ. A APLICAÇÃO DA TEORIA DO RISCO DO EMPREENDIMENTO. EVIDENCIADO O EXERCÍCIO DE ATIVIDADE LUCRATIVA NO MERCADO DE CONSUMO, ASSUME A DEMANDADA O RISCO DA OCORRÊNCIA DE FRAUDES, DEVENDO ARCAR COM OS PREJUÍZOS CAUSADOS. - EVIDENCIADA A ILICITUDE DOS DESCONTOS REALIZADOS NA FOLHA DE PAGAMENTO DO AUTOR, MOSTRA-SE CABÍVEL A DEVOLUÇÃO DO VALOR COBRADO INDEVIDAMENTE, NA FORMA SIMPLES, COMO RECONHECIDO EM SENTENÇA. - EMBORA A MERA COBRANÇA INDEVIDA NÃO GERE, A PRIORI, INDENIZAÇÃO DE CUNHO MORAL, OS TRANSTORNOS APONTADOS NOS AUTOS EXTRAPOLAM O MERO DISSABOR, ESPECIALMENTE CONSIDERANDO QUE O AUTOR TEVE PARCELAS DEBITADAS INDEVIDAMENTE NA FOLHA DE PAGAMENTO, VERBA DE NATUREZA ALIMENTAR. POSSIBILIDADE, NO CASO, DE ARBITRAMENTO DA INDENIZAÇÃO. - QUANTUM INDENIZATÓRIO. A INDENIZAÇÃO POR DANOS MORAIS DEVE SER QUANTIFICADA COM PONDERAÇÃO, DEVENDO ATENDER AOS FINS A QUE SE PRESTA – COMPENSAÇÃO DO ABALO E ATENUAÇÃO DO SOFRIMENTO – SEM REPRESENTAR, CONTUDO, ENRIQUECIMENTO SEM CAUSA DA PARTE OFENDIDA. CASOEM QUE O VALOR FIXADO NA ORIGEM (R\$ 5.000,00) NÃO MERECE MINORAÇÃO, PORQUANTO AQUÉM DO PARÂMETRO DA CÂMARA NO ENFRENTAMENTO DE SITUAÇÕES SEMELHANTES. APELAÇÃO DESPROVIDA.
(RIO GRANDE DO SUL, 2022)

Esta jurisprudência trata de uma apelação cível relacionada à responsabilidade civil, especificamente sobre uma fraude na contratação de empréstimo bancário consignado. A análise da decisão à luz da Lei Geral de Proteção de Dados (LGPD) pode ser feita da seguinte maneira. A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Neste caso, a contratação digital é considerada um tratamento de dados pessoais.

Ainda a legislação estabelece que todas as organizações que processam informações sobre pessoas, brasileiras ou não, que estão no território nacional, devem observar a lei. No entanto, neste caso, a fraude na contratação foi comprovada. E exige que o tratamento dos dados seja feito levando em conta alguns requisitos, como finalidade e necessidade. Neste

caso, o tribunal concluiu que a instituição financeira é responsável pelo bom funcionamento dos serviços colocados à disposição do consumidor (BRASIL, 2023).

A LGPD oferece várias garantias ao cidadão, incluindo a possibilidade de solicitar a exclusão dos seus dados pessoais e revogar o consentimento. No entanto, neste caso, o tribunal destacou a vulnerabilidade quanto à segurança financeira no mundo digital. Ainda estabelece que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser observada. Neste caso, houve uma contratação fraudulenta e a ré foi considerada responsável (CAPANEMA, 2020).

Em resumo, esta decisão judicial reflete vários princípios fundamentais da LGPD, incluindo a necessidade de consentimento informado para o tratamento de dados pessoais e a responsabilidade das organizações em garantir a proteção desses dados.

No que diz respeito ao uso do reconhecimento facial na perspectiva jurisprudencial brasileira, ainda não há uma jurisprudência consolidada devido à relativa novidade e complexidade do assunto. A utilização do reconhecimento facial em diferentes contextos, como em sistemas de segurança, marketing, autenticação digital e análise de emoções, levanta questões sobre privacidade, proteção de dados pessoais e possíveis violações de direitos fundamentais.

Portanto, pode-se concluir que a jurisprudência nacional ainda apresenta lacunas significativas em relação às questões relacionadas ao reconhecimento facial, especialmente no que diz respeito à violação ou não dos direitos à imagem e privacidade das pessoas, bem como à conformidade de sua utilização com os princípios da finalidade previstos na Lei Geral de Proteção de Dados (LGPD).

CONCLUSÃO

Considerando a aplicação do reconhecimento facial e a coleta de dados para fins de consumo à luz da Lei Geral de Proteção de Dados (LGPD), infere-se que a utilização dessas tecnologias traz consigo implicações significativas no que diz respeito à privacidade e à proteção dos dados pessoais. Embora o reconhecimento facial possa oferecer vantagens substanciais no âmbito da segurança e personalização dos serviços, é fundamental estabelecer limites claros e mecanismos de controle efetivos para salvaguardar os direitos e a privacidade dos indivíduos.

Na elaboração da pesquisa apresentada, abordou-se a evolução dos princípios consumeristas e a importância da LGPD como um marco regulatório de proteção. O estudo, nesse contexto, concentrou-se nos aspectos do reconhecimento facial, suas implicações na coleta de dados para fins de consumo e os debates em torno da proteção da privacidade, explorando as diversas posições no âmbito legal e doutrinário. No contexto específico do reconhecimento facial, é crucial que as empresas e organizações estejam em conformidade com os requisitos estabelecidos pela LGPD. Isso envolve a adoção de medidas técnicas e organizacionais adequadas para proteger os dados pessoais, garantir a segurança dos sistemas de reconhecimento facial e prevenir o uso indevido das informações coletadas.

Tais análises serviram para auxiliar na resposta da indagação inicial desta pesquisa, qual seja, se o uso do reconhecimento facial a fins de consumo respeita ou não a Lei Geral de Proteção de Dados.

Ao longo da pesquisa realizada, verificou-se que o reconhecimento facial a fins de consumo muitas vezes não respeita a Lei Geral de Proteção de Dados, uma vez que o direito do consumidor acaba sendo violado mediante a coleta de dados para adquirir um determinado produto, por muitas vezes não possuir a informação correta o consumidor por ser vulnerável acaba tendo seus dados coletados no momento da disponibilização de informações e sofre com o vazamento de seus dados.

Apesar das medidas e garantias previstas na LGPD para proteger os direitos dos consumidores, ainda existem possíveis riscos de exposição de dados pessoais. O uso do reconhecimento facial nas relações de consumo envolve o tratamento de informações sensíveis e pode apresentar desafios em relação à privacidade e à proteção de dados. Seus princípios são

adotados como referenciais morais, políticos e jurídicos que inspiram e direcionam a elaboração de textos normativos, buscando remediar situações injustas e estabelecer compromissos éticos com todas as partes envolvidas.

Esses princípios são fundamentais para a garantia da equidade nas relações de consumo, visando promover a proteção e o respeito aos direitos dos consumidores de forma abrangente e coerente com os preceitos éticos da sociedade contemporânea.

No entanto, com base nos resultados alcançados até o estágio atual da pesquisa, torna-se evidente que o uso do reconhecimento facial, desde que realizado dentro dos parâmetros legais e sem qualquer tipo de vício, tende a aumentar a aceitação por parte dos clientes.

Tal fenômeno pode ser atribuído ao fato de que essa prática tem o potencial de proporcionar maior segurança nos ambientes de compra, uma vez que a utilização do reconhecimento facial pode efetivamente evitar uma série de burocracias presentes nas transações comerciais. Além disso, a adoção dessa tecnologia pode favorecer uma maior adaptabilidade no tratamento entre consumidores e vendedores, contribuindo para uma experiência mais fluida e personalizada.

Por sua vez, os consumidores devem estar cientes de seus direitos e serem proativos na defesa de sua privacidade, exercendo seus direitos de acesso, correção, exclusão e portabilidade de seus dados pessoais. A conscientização e a educação sobre os riscos e os direitos relacionados ao reconhecimento facial são cruciais para proteger os consumidores nesse contexto.

É importante destacar que a implementação do reconhecimento facial nas relações de consumo deve ser acompanhada de uma análise cuidadosa dos aspectos legais, éticos e de privacidade. As empresas devem buscar orientação jurídica especializada e estar atualizadas sobre as regulamentações e diretrizes relevantes para garantir que estejam em conformidade com a LGPD e respeitem os direitos dos consumidores.

REFERÊNCIAS

- ACCIOLY, C. L. A Proteção De Dados Do Trabalhador: O Direito Do Trabalho Constitucionalizado E Seu Diálogo Com O Direito À Privacidade. *Revista dos Estudantes de Direito da Universidade de Brasília*, n. 15, p. 255–264, 2018.
- ALMEIDA, João Batista, A proteção jurídica do consumidor, 2. ed., *Revista dos Tribunais*, 2000, p. 40.
- ALVES, Fabrício Germano; BEATRIZ, A.; MARIA. Direito à informação, proteção de dados do consumidor e utilização de reconhecimento facial para a publicidade comportamental. *Revista acadêmica de Faculdade de Direito do Recife*, v. 94, n. 1, p. 160–160, 6 maio 2022.
- ALMEIDA, S. DO C. D. DE; SOARES, T. A. Os impactos da Lei Geral de Proteção de Dados - LGPD no cenário digital. *Perspectivas em Ciência da Informação*, v. 27, n. 3, p. 26–45, set. 2022.
- ARAÚJO, Romulo de Aguiar; CARDOSO, Naiara Deperon; DE PAULA, Amanda Marcélia. REGULAÇÃO E USO DO RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA DO BRASIL. Disponível em: <https://revistajuridica.tjdf.t.jus.br/index.php/rdj/article/download/734/135/2758>. Acesso em 08-10-2023. 2021.
- ASSOCIAÇÃO BRASILEIRA DE MARKETING DIRETO. Teoria de reconhecimento facial pode mudar o marketing. 2020. Disponível em: <https://abemd.org.br/noticias/tecnologia-de-reconhecimento-facial-pode-mudar-o-marketing>. Acesso em: 25 maio 2023.
- BARROS, Laura. Direito de imagem: entenda o que a lei fala e a sua aplicação. 2018. Disponível em: <http://www.lumosjuridico.com.br/2018/05/10/direito-de-imagem-entenda-o-que-a-lei-fala-e-a-sua-aplicacao/>. Acesso em: 28 abr. 2023.
- BARRETO, André. LGPD e biometria facial: o que você precisa saber | Unike Tecnologias. Disponível em: <https://unike.tech/blog/2020/01/lgpd-e-biometria-facial-o-que-voce-precisa-saber/>. Acesso em: 13 out. 2023.
- BASAN, Arthur Pinheiro Publicidade digital e proteção de dados pessoais [recurso eletrônico]: o direito ao sossego / Arthur Pinheiro Basan. - Indaiatuba, SP: Editora Foco, 2021.
- BIONI, Bruno. Proteção de Dados Pessoais - A Função e os Limites do Consentimento. Editora Forense. 2018.
- BONNA, Alexandre Pereira et al. Comentários à lei geral de proteção de dados pessoais. Coordenado por Guilherme Magalhães Martins, João Victor Rozatti Longhi e José Luiz de Moura Faleiros Júnior. Indaiatuba, SP: Editora Foco, 2022.
- BLUM, Renato Opice. "LGPD - Lei Geral de Proteção de Dados: Comentada Artigo por Artigo". São Paulo: Thomson Reuters Brasil, 2020.

BLUM, Renato Opice; PINHEIRO, Patricia Peck; VAINZOF, Rony. "LGPD Comentada: Lei Geral de Proteção de Dados Pessoais". Editora Revista dos Tribunais, 2020.

BRAGA NETTO, Felipe Peixoto. Manual de direito do consumidor: à luz da jurisprudência do STJ. 6. ed. rev., ampl. e atual. Salvador: Juspodivm, 2011.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 18 maio 2023.

BRASIL. Portal da Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199418>>. Acesso em: 13 out. 2023. 2019.

BRASIL. Lei n. 10.406, de 10 de janeiro de 2002. Código Civil. Brasília, DF: Presidência da República, 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/ Acesso em: 18 maio 2023.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm Acesso em: 18 maio 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018.. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 27 maio 2023.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13-10-2023. (2018)

OPICE BLUM. Guia para a Lei Geral de Proteção de Dados. Disponível em: https://opiceblum.com.br/wp-content/uploads/2019/07/LGPD_16infograficos_31.08.2020.pdf. Acesso em: 13 out. 2023. 2020.

BRASIL. Superior Tribunal de Justiça. Disponível em: <https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=fraude+e+banc%E1ria&refinar=S.DISP.&&b=INFJ&p=true&t=JURIDICO&l=10&i=1>. Acesso em 13-10-2023. 2023

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712. Acesso em: 13-10-2023. 2020

COELHO, Fábio Ulhoa; GAGO, Rodrigo F. Programa de Direito do Consumidor. São Paulo: Editora Saraiva, 2019. Páginas 27-46.

- COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais comentada. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.
- DE LUCCA, Newton; MONTEIRO, Renato Leite. "LGPD e Proteção de Dados Pessoais: Comentários à Lei Geral de Proteção de Dados Pessoais Brasileira". Editora Thomson Reuters, 2019.
- DEEP LEARNING BOOK (Org.). Campos Receptivos Locais em Redes Neurais Convolucionais. Disponível em: <<http://deeplearningbook.com.br/campos-receptivos-locais-em-redes-neurais-convolucionais/>>. Acesso em: 21 maio 2023.
- DONDA, D. (2020). LGPD - Lei Geral de Proteção de Dados: Entenda seus impactos e adequase. São Paulo: Editora Érica.
- DONEDA, Danilo. "Da Privacidade à Proteção de Dados Pessoais" (2ª edição). São Paulo: Revista dos Tribunais, 2021.
- ESCOVAR, João Victor. Especialista comenta polêmica do reconhecimento facial. 2020. Disponível em: <https://www.oconsumerista.com.br/2020/07/privacidade-especialistacomentapolemica-do-reconhecimento-facial/>. Acesso em: 23 maio 2023.
- FARIAS, C.C. de ROSENVALD, N.; NETTO, F.P.B. **Responsabilidade Civil**. 2º ed. São Paulo: Atlas S.A., 2015.
- FILOMENO, José Geraldo B. Direitos do Consumidor, 15ª edição. [Digite o Local da Editora]: Grupo GEN, 2018. E-book. ISBN 9788597017069. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597017069/>. Acesso em: 06 abr. 2023.
- FILHO, Sergio C. Programa de Direito do Consumidor. [Digite o Local da Editora]: Grupo GEN, 2022. E-book. ISBN 9786559772766. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786559772766/>. Acesso em: 07 abr. 2023.
- FILHO, Sergio C. Programa de Direito do Consumidor. São Paulo: Atlas, 14ª edição, 2016.
- GARCIA, Leonardo de Medeiros. Manual do Direito do Consumidor: Direito Material e Processual. 3ª edição. Editora Juspodivm, 2019.
- GUEDES, Paula. 7 recomendações para a regulação do Reconhecimento facial. Disponível em: <https://www.lgpdbrasil.com.br/7-recomendacoes-para-a-regulacao-do-reconhecimento-facial/>. Acesso em: 08-10-2023. 2021.
- GROSSI, Bernardo Menicucci (Org.) Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] / Bernardo Menicucci Grossi (Org.) -- Porto Alegre, RS: Editora Fi, 2020.
- GRINOVER, Ada Pellegrini et al. Código brasileiro de defesa do consumidor. 13. ed. Rio de Janeiro: Forense, 2022. E-book. Acesso restrito via Minha Biblioteca.
- GUARIENTO, Daniel Bittencourt; MARTINS, Ricardo Maffeis. Desafios Na Utilização De

Sistemas De Reconhecimento Facial <https://www.migalhas.com.br/coluna/impressoes-digitais/373540/desafios-na-utilizacao-de-sistemas-de-reconhecimento-facial> Acesso em: 22 maio 2023.

JAFRI, R.; ARABNIA, H. R. A survey of face recognition techniques. *Jips*, v. 5, n. 2, p. 41–68, 2009.

JAIN, A.; BOLLE, R.; PANKANTI, S. *Biometrics: personal identification in networked society*. [S.l.]: Springer Science & Business Media, 2006. Acesso em: 23 maio 2023.

GUIMARÃES, Rafael Miranda. *Reconhecimento facial: desenvolvimento de um protótipo de software de tempo real para registro eletrônico de ponto com utilização do dispositivo kinect*/ Rafael Miranda Guimarães. - São Paulo: Editora Dialética, 2022. E-book: 1 MB.: EPUB.: Acesso em: 23 maio 2023.

KHOURI, Paulo R. Roque A.. *Direito do consumidor: contratos, responsabilidade civil e defesa do consumidor em juízo*. 7. ed. São Paulo: Atlas, 2021. E-book. Acesso restrito via Minha Biblioteca.

KOHL, Cleize LGPD: da teoria a implementação nas empresas / Cleize Kohls, Luiz Henrique Dutra, Sandro Welter. — 1. ed. — Sao Paulo :Rideel, 2021.

KUTTERER, Cornelia; HOUWING, Lotte; LE GRAND, Gwendal. Facial recognition, a 'convenient' and 'efficient' solution looking for a problem? [1h04min40seg]. Moderator: VELD, Sophie in 't; KORNER, Moritz 13th Computers, Privacy and Data Protection (CPDP) International Conference, 20 jan. 2020. Disponível em: <https://www.youtube.com/watch?v=zVXgB28Qrf0>. Acesso em: 28 jun. 2021.

LI, Stan Z.; JAIN, Anil K. (Ed.). *Manual de Reconhecimento Facial*. A: Springer, 2004. Disponível em: . Acesso em: 30 maio 2023.

LI, Stan Z.; JAIN, Anil K. (Ed.). *Manual de Reconhecimento Facial*. A: Springer, 2004. <<https://epdf.pub/queue/handbook-of-facerecognition6b3f024d0c27687be20b89933aa7d7b780895.html>>. Acesso em: 21 maio 2023. DEEP Learning Book. Disponível em: <<http://deeplearningbook.com.br/o-que-sao-redesneurais-artificiais-profundas/>>. Acesso em: 21 maio 2023.

LINS, Bernardo Felipe; *A evolução da Internet : uma perspectiva histórica*; Cadernos Aslegis, Brasília, jan./abr. 2013.

MACIEL, Rafael Fernandes. *Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)*. RM Digital Education. 1ª Edição. Goiânia – GO. 2019. ISBN: 9781093409420

MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor*. 6. ed. São Paulo: Revista dos Tribunais, 2010. p. 54-67.

MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 7ª ed. São Paulo: Revista dos Tribunais, 2012.

MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: O novo regime*

das relações contratuais. 8. ed. São Paulo: Editora Revista dos Tribunais, 2015.

MIRAGEM, Bruno. Curso de Direito do Consumidor - 6. ed. rev., atual. e ampl.- São Paulo: Editora Revista dos Tribunais, 2016.

MIT 6.S191. Introdução ao Deep Learning. 2020. Disponível em: <http://introtodeeplearning.com/>. Acesso em: 30 maio 2023.

NUNES, Rizzato Curso de direito do consumidor / Rizzato Nunes. – 12. ed. – São Paulo : Saraiva Educação, 2018. 1. Consumidores – Leis e legislação – Brasil 2. Consumidores – Proteção – Brasil I. Título. 17-1612 CDU 34:381.6(07).

NUNES, Luiz Antonio Rizzato. Manual de Direito do Consumidor. 8. ed. São Paulo: Saraiva Educação, 2018.

NUNES, Luiz Antônio Rizzato. Curso de Direito do Consumidor. São Paulo: Saraiva Educação, 16ª edição, 2020.

OLIVEIRA, Júlio Cesar de. Lei Geral de Proteção de Dados Pessoais: Comentários aos Artigos. 1ª ed. Revista dos Tribunais, 2020.

PINHEIRO, Patrícia Peck. Direito Digital. São Paulo: Saraiva, 2021.

PINHEIRO, Patrícia Peck Proteção de dados pessoais: comentários à Lei n. 13.709/2018.
SILVA, J. G. R. P. Direito do Consumidor.

PINHEIRO, Patrícia P. Direito Digital . [Digite o Local da Editora]: Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786555598438/>. Acesso em: 22 mai. 2023.
J. Zhou, Z. Ma, J. Wang, and S. Member, "Face Recognition: Recent Advances, Challenges and Future Directions," in IEEE Access, vol. 6, pp. 68812-68823, 2018, doi: 10.1109/ACCESS.2018.2871037. 2018.

PACK, Patrícia Pinheiro. **Direito Digital**, 6ª edição. Editora Saraiva. São Paulo. 2016.

PASQUALE, Frank. The Black Box Society: The Secret Algorithms That Control Money and Information. Cambridge (Massachusetts), London: Harvard University Press, 2015.

RESENDE, Ubiratan. Reconhecimento facial: como aprimorar o atendimento ao cliente. 2019. Disponível em: <https://www.proxima.com.br/home/proxima/howto/2019/07/05/reconhecimento-facial-como-aprimorar-o-atendimento-ao-cliente.html>. Acesso em: 25 maio 2023.

RIO DE JANEIRO. Tribunal de Justiça do RJ. DECIMA QUINTA CAMARA DE DIREITO PRIVADO. Des(a). RICARDO ALBERTO PEREIRA. APELAÇÃO, 0040375-55.2022.8.19.0038. Julgamento: 31/05/2023. Disponível em: Tribunal de Justiça do Estado do Rio de Janeiro (tjrj.jus.br). 2023.

RIO GRANDE DO SUL. Tribunal de Justiça do RS. Nona Câmara Cível. Apelação Cível, Nº

50282839020178210001, Relator: Carlos Eduardo Richinitti, 2022.

SANTOS, F. A. DOS. A lei geral de proteção de dados pessoais (LGPD) e a exposição de dados sensíveis nas relações de trabalho. Revista do Tribunal Regional do Trabalho da 10a Região, v. 24, n. 2, p. 145–151, 2020.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020.

SIQUEIRA Antônio Henrique Albani. Disposições preliminares. In Comentários à Lei Geral de Proteção de Dados - Ed. 2019. 2 Ed, São Paulo, 2019 Thomson Reuters Brasil.

SILVA, Victor Hugo. Por que o uso de reconhecimento facial na segurança é controverso?. Disponível em:

<https://tecnoblog.net/especiais/por-que-o-uso-de-reconhecimento-facial-na-seguranca-e-controverso/>. Acesso em: 08-10-2023. 2020.

SIVA, Daniel Cavalcante: Manual da Lei Geral de Proteção de Dados para instituições de Ensino [livro eletrônico] / Daniel Cavalcante Silva, Adriana Carla Arouca.—1. ed.—Brasília: 2020. PDF.

SOUZA, Carlos Affonso; Monteiro, Alexandre. LGPD - Lei Geral de Proteção de Dados Pessoais Comentada. 1ª ed. Forense, 2020.

SCHWARTZ, Fabio- Manual de direito do consumidor: tópicos e controvérsias/ Fabio Schwartz - Rio de Janeiro: Processo, 2018.

SOUZA, Sylvio Capanema de; WERNER, José Guilherme V.; NEVES, Thiago F C. Direito do Consumidor. [Digite o Local da Editora]: Grupo GEN, 2018. E-book. ISBN 9788530981273. Disponível

<https://integrada.minhabiblioteca.com.br/#/books/9788530981273/>. Acesso em: 06 abr. 2023.

SANTA CATARINA. Tribunal de Justiça de SC. Primeira Câmara de Direito Civil, Apelação n. 5000097-34.2022.8.24.0216, rel. Flavio Andre Paz de Brum. 2022.

SANTOS, Coriolano Aurélio de Almeida Camargo; CHEVTCHUK, Leila. **A proteção aos dados pessoais no ordenamento jurídico brasileiro e o ...** Disponível em:

<<https://www.migalhas.com.br/coluna/direito-digital/220187/a-protecao-aos-dados-pessoais-no-ordenamento-juridico-brasileiro-e-o-anteprojeto-do-ministerio-da-justica>>. Acesso em: 13-10-23

SOLERE, Bertrand. O que a LGPD prevê sobre reconhecimento facial?. Disponível em: O que a LGPD prevê sobre reconhecimento facial? - LGPD Soluções (lgpdsolucoes.com.br). Acesso em: 13-10-2023.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Cap. 10, p. 281-318.

THEODORO JÚNIOR, Humberto Direitos do consumidor / Humberto Theodoro Júnior. – 9. ed. ref., rev. e atual. – Rio de Janeiro: Forense, 2017.

TARTUCE, Flávio Manual de Direito do Consumidor: direito material e processual, volume único / Flávio Tartuce, Daniel Amorim Assumpção Neves. – 10. ed. – Rio de Janeiro: Forense; Método, 2021.

VIDOR, Daniel Martins. Conheça a origem da Lei Geral de Proteção de Dados (LGPD). 2019. Disponível em: <https://www.plugar.com.br/conheca-a-origem-da-lei-geral-de-protecaode-dados-lgpd/>. Acesso em: 20 jun. 2023.