

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

Gabriela Sharfi

Do direito fundamental à proteção de dados pessoais: análise sobre os benefícios e malefícios da prática do reconhecimento facial e vigilância em massa.

GRADUAÇÃO EM DIREITO

São Paulo

2023

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

Gabriela Sharfi

Do direito fundamental à proteção de dados pessoais: análise sobre os benefícios e malefícios da prática do reconhecimento facial e vigilância em massa.

GRADUAÇÃO EM DIREITO

Projeto de monografia apresentado à Faculdade de Direito da Pontifícia Universidade Católica de São Paulo, como exigência parcial para a conclusão do Curso de Graduação, sob orientação do Prof. Luiz Alberto D. Araujo.

São Paulo

2023

AGRADECIMENTOS

Dedico a conclusão do meu curso à minha família, principalmente, aos meus pais, Shlomo e Lilian, que me proporcionaram uma graduação de excelência na PUC-SP e sempre estiveram ao meu lado durante os momentos de alegria e tristeza, desafios e conquistas.

Agradeço também a todos os meus amigos, que fizeram parte do meu cotidiano em cinco anos de graduação, tornando os dias mais leves e prazerosos. Sem a presença desses amigos queridos por perto, não seria possível ter concluído essa etapa.

Não poderia deixar de agradecer também a todos os professores que fizeram parte da minha graduação. Esses mentores de excelência foram extremamente importantes para o meu desenvolvimento como aluna de Direito da PUC-SP.

Por fim, agradeço ao Prof. Luiz Alberto D. Araujo., orientador do presente trabalho de conclusão de curso.

RESUMO

O presente estudo tem como objeto central discorrer sobre a efetiva proteção constitucional acerca dos direitos à privacidade, intimidade, vida privada e proteção aos dados pessoais, estampados pelo art. 5º, X e LXXIX, respectivamente, da Constituição Federal de 1988 (“CRFB/88”), adotando como parâmetro o cenário atual de avanços tecnológicos e, em especial, a prática do reconhecimento facial e vigilância em massa. Os dados pessoais dizem respeito a informações intrínsecas a cada indivíduo pertencente da sociedade atual. São informações que caracterizam o indivíduo como único, uma vez que tratam diretamente sobre a sua pessoa, sobre o seu ser. Portanto, os conceitos de dados pessoais estão ligados umbilicalmente às ideias de privacidade, vida privada e intimidade. Sendo assim, para tratar do tema de proteção de dados pessoais, faz-se necessário, primeiramente, criar uma diferenciação entre os conceitos de privacidade, intimidade e vida privada. Esses direitos fundamentais fazem parte dos direitos da personalidade, sem os quais o ser humano não poderia viver em sociedade, já que são conectados também com o direito fundamental da dignidade da pessoa humana. De maneira primordial, é necessário compreender o que a CRFB/88 pretendeu ao preconizar a defesa dos direitos relacionados à intimidade, privacidade e vida privada para, em um segundo plano, introduzir os conceitos de dados pessoais e o interesse em defendê-los através de legislações infraconstitucionais de grande significância a partir de tantos avanços na tecnologia que temos atualmente. O exame sobre a proteção dos direitos fundamentais elucidados no parágrafo acima leva em consideração a importância de se viver em um mundo conectado e interligado por tecnologias, em especial, as Inteligências Artificiais (“IA”) que usam mecanismos altamente avançados para a realização de reconhecimentos faciais e controle de massas. Para a conclusão dessa análise, levou-se em consideração, com a devida importância, a Lei Geral de Proteção de Dados Pessoais – a “LGPD” e demais legislações que abordam sobre esse assunto.

Palavras-chave: Privacidade; intimidade; vida privada; proteção de dados pessoais; direitos fundamentais; avanços tecnológicos; dados pessoais; reconhecimento facial; vigilância em massa

SUMÁRIO

1. INTRODUÇÃO.....	5
2. UMA BREVE INTERPRETAÇÃO DO ART. 5º, X, DA CONSTITUIÇÃO FEDERAL DO BRASIL, DIANTE DAS DISCUSSÕES SOBRE A PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NO BRASIL	7
2.1. Dos direitos da personalidade: direito à intimidade, vida privada e privacidade, garantidos pela CRFB/88.....	7
3. A NECESSÁRIA APLICAÇÃO DE LEIS E REGULAMENTOS INFRACONSTITUCIONAIS DE PROTEÇÃO DE DADOS PESSOAIS.....	18
3.1. Aplicabilidade do Marco Civil da Internet (Lei 12.965/2014).....	18
3.2. Do direito à proteção de dados pessoais garantido pela CRFB/88.....	22
3.3. A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018 – a “ <u>LGPD</u> ”) e seus principais conceitos.....	24
4. DOS AVANÇOS TECNOLÓGICOS NO SÉC. XXI A PARTIR DA ANÁLISE DOS DIREITOS E GARANTIAS CONSTITUCIONAIS ESTAMPADAS PELO ART. 5º, X E LXXI, DA CONSTITUIÇÃO FEDERAL DO BRASIL DE 1988	34
4.1. Da prática do reconhecimento facial e vigilância em massa – breves conceitos	34
4.2. Efetiva proteção dos direitos fundamentais previstos pelo art. 5º, X e LXII, da Constituição Federal do Brasil de 1988, diante da prática do reconhecimento facial e vigilância em massa.....	37
5. CONSIDERAÇÕES FINAIS.....	45
6. BIBLIOGRAFIA.....	47

1. INTRODUÇÃO

O objetivo geral a ser alcançado por esta Monografia é a apresentação sobre a importância das garantias constitucionais sobre intimidade, privacidade, vida privada e proteção aos dados pessoais, diante de tantos avanços tecnológicos que fazem parte do cotidiano atual.

Não há dúvidas de que os avanços da IA e demais tecnologias são benéficos. Se não fosse pela tecnologia de hoje, de fato, o mundo não seria o mesmo. Entretanto, o avanço da tecnologia deve respeitar os direitos básicos do ser humano: seus direitos fundamentais de existência. Nesse sentido, a utilização dessas tecnologias, principalmente, a prática do reconhecimento facial e vigilância em massa, ponto focal a ser estudado nesta Monografia, deve respeitar os direitos fundamentais expressos pela CRFB/88, bem como princípios éticos embasados nesses direitos fundamentais, garantidos também por outras legislações infraconstitucionais.

O uso do reconhecimento facial pode acelerar processos de maneira automatizada, nos campos criminais e investigatórios, por exemplo. Todavia, também pode implicar em uma interferência injustificada nos direitos fundamentais, em particular, o direito à privacidade e intimidade, que vai além da necessidade pública em usar novas tecnologias descontroladamente e sem prévio aviso aos titulares dos dados pessoais. Não obstante, a utilização de tecnologias do reconhecimento facial pode, também, conflitar com os princípios éticos de respeito pela autonomia humana, prevenção de danos e justiça.

O reconhecimento facial, como será abordado, é uma prática que utiliza o rosto humano para finalidades distintas, através da biometria. Esta por sua vez, é definida pela LGPD como dado pessoal sensível e requer, portanto, uma atenção especial no que tange a sua utilização. Nota-se, dessa forma, que não é possível abordar o tema de reconhecimento facial sem antes tratar de privacidade e proteção aos dados pessoais e sobre as regulações envolvidas neste quesito.

Diante dessa problemática, é preciso primeiramente compreender como a CRFB/88 protege os direitos da personalidade, ligados diretamente aos conceitos de privacidade e proteção aos dados pessoais, e, posteriormente, compreender como esses direitos basilares são garantidos atualmente, diante de um mundo mais conectado e digital.

Dessa forma, a presente Monografia se inicia com o estudo sobre a proteção constitucional dos direitos da personalidade ligados à intimidade, privacidade e vida privada, para, na sequência adentrar nas legislações infraconstitucionais sobre a privacidade e proteção de dados pessoais, em especial a LGPD, para, finalmente, abordar sobre a prática do reconhecimento facial e se de fato há proteção aos direitos e garantias fundamentais dependendo de como essa prática é usada.

Para elucidar de forma mais concreta o tema central desta Monografia, serão abordados dois casos práticos para que seja possível realizar um balanceamento entre a proteção das garantias constitucionais e a necessidade de tornar o mundo mais tecnológico, facilitando, por exemplo, a identificação de perfis consumeristas e otimizando os serviços públicos. Para tanto, será abordado o caso do uso de reconhecimento facial na Linha 4 do metrô de São Paulo e nas Lojas Hering, dois casos que ganharam destaque no Brasil do ponto de vista de proteção de dados pessoais.

Através desses casos, serão discutidas as decisões tomadas frente a coleta e tratamento dos dados pessoais em questão, tomando como premissa a utilização da prática do reconhecimento facial e do controle de massas.

2. UMA BREVE INTERPRETAÇÃO DO ART. 5º, X, DA CRFB/88, DIANTE DAS DISCUSSÕES SOBRE A PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

2.1. DOS DIREITOS DA PERSONALIDADE: DIREITO À INTIMIDADE, VIDA PRIVADA E PRIVACIDADE, GARANTIDOS PELA CRFB/88

No ano de 1987, foi instalada a Assembleia Nacional Constituinte com o grande objetivo de trazer uma Constituição com teor mais garantista para a população brasileira, tendo em vista que o Brasil havia acabado de enfrentar 21 longos anos de ditadura militar, a qual se estendeu de 1964 até 1985. Nesse sentido, a Constituição de 1988 buscava trazer aos cidadãos brasileiros uma amplitude de direitos e garantias fundamentais, bem como fortes obrigações prestacionais por parte do Estado.

A CRFB/88, nesse sentido, ampliou, de maneira significativa, a proteção aos direitos fundamentais estampados pelo art. 5º do texto constitucional. O avanço da sociedade brasileira e as mudanças do contexto social refletiram a necessidade de a Constituição abranger ainda mais os direitos fundamentais. Não é coincidência que os direitos fundamentais sejam dotados de características essenciais como, por exemplo, a universalidade, a inalienabilidade/indisponibilidade, a vinculação com os poderes públicos e o fato de os direitos fundamentais serem absolutos, características essas que serão mais detalhadas na sequência.

A sedimentação dos direitos fundamentais como normas obrigatórias é resultado de uma maturação histórica, ou seja, os direitos fundamentais não foram os mesmos em todas as épocas, mas refletiram necessidades sociais em diferentes períodos históricos. Sendo assim, os direitos fundamentais assumem uma posição de realce na sociedade atual e representam, acima de tudo, os deveres que o Estado tem perante seus cidadãos, de maneira a proporcionar uma vida digna e de qualidade.

Os direitos fundamentais expressos pela CRFB/88 são dotados de características relevantes, que os consagram como essenciais para a manutenção da sociedade, como já expresso por esta Monografia. Os direitos fundamentais são, primeiramente, universais e absolutos. São universais, pois todas as pessoas são titulares de direitos fundamentais. Alguns dos direitos fundamentais estampados pelo art. 5º da CRFB/88 são essenciais para todos, como, por exemplo, o direito à vida. Todavia, algumas das categorias ali previstas interessam apenas a uma parcela da

sociedade, como os trabalhadores. Segundo a posição de Gilmar Mendes, em seu Curso de Direito Constitucional (2018), página 20:

[...] isso significa que o constituinte também quis privilegiar certos bens que vêm satisfazer necessidades do homem histórico, isto é, de alguns homens na sua específica posição social. A fundamentalização desses direitos implica reconhecer que determinados objetivos vitais de algumas pessoas têm tanta importância como os objetivos básicos do conjunto dos indivíduos.

Pode-se dizer, ainda, que os direitos fundamentais são absolutos, já que se situam no patamar máximo da hierarquia jurídica. Este conceito vem da corrente jusnaturalista de que o Estado existe, justamente, para proteger direitos naturais, como a vida, a liberdade, a igualdade.

Uma segunda característica dos direitos fundamentais é sua historicidade. Ou seja, os direitos fundamentais são um conjunto de faculdades e instituições, os quais somente fazem sentido diante de um determinado contexto histórico. Esse conceito de historicidade ainda implica em dizer que os direitos fundamentais podem surgir em determinada época e desaparecer em outra, pois as necessidades da sociedade, bem como o contexto histórica na qual está inserida, mudou.

Um exemplo ilustrativo para retratar o exposto acima é que tanto a Constituição atual como a anterior vedam a pena de caráter perpétuo. O que antes de 1988 se circunscrevia à esfera das reprimendas penais, passou a ser também aplicável a outras espécies de sanções e, em fins de 1998, o STF entendeu a garantia ao âmbito das sanções administrativas.

A terceira característica é marcada pela inalienabilidade/indisponibilidade. Os direitos fundamentais são inalienáveis, pois não admitem que o seu titular o torne impossível de ser exercitado para si mesmo. Sendo assim, o direito à integridade física, por exemplo, é inalienável, pois o indivíduo não pode vender uma parte de seu corpo. Os autores que sustentam a tese da inalienabilidade afirmam que ela resulta da fundamentação do direito no valor da dignidade da pessoa humana. O homem não pode deixar de ser homem, assim como não pode ser livre para ter ou não dignidade, o que significa dizer que o Direito não pode permitir que o homem se prive de sua dignidade.

O conceito de indisponibilidade, por outro lado, fundamenta-se na dignidade humana, mas nem todos os direitos fundamentais possuem essa característica.

Somente os direitos fundamentais que visam resguardar a potencialidade do homem de autodeterminar deveriam ser considerados indisponíveis. Portanto, os direitos indisponíveis são aqueles que protegem a vida biológica ou que pretendem defender a saúde física e mental e a liberdade de tomar decisões sem coerção externa.

A quarta característica associada aos direitos fundamentais diz respeito à constitucionalização, que é um marco divisor entre direitos humanos e direitos fundamentais. Os direitos humanos, diferentemente dos direitos fundamentais, são aqueles direitos do homem, que não possuem característica básica e positivação em determinada ordem jurídica. É um conceito, portanto, empregado para designar pretensões de respeito à pessoa humana.

Já os direitos fundamentais são os direitos básicos do ser humano, que visam uma ordem jurídica concreta e são assegurados na medida em que cada Estado os consagra de forma definitiva. A distinção de conceito entre direitos humanos e fundamentais não significa que esses direitos estejam em esferas distintas que não se comunicam entre si. Todavia, não são coincidentes no modo de proteção ou no grau de efetividade.

A quinta característica dos direitos fundamentais é sua vinculação aos poderes públicos. O fato de esses direitos estarem previstos pela CRFB/88 acaba por torná-los parâmetros de uma organização e de limitação aos poderes constituídos. A constitucionalização desses direitos, como elucidado anteriormente, impede que esses direitos sejam considerados meramente autolimitações dos poderes constituídos. Os atos do Poder Legislativo, Executivo e Judiciário devem conformidade aos direitos fundamentais.

A partir das características essenciais aos direitos fundamentais, demonstra-se a importância do respeito e garantia a esses direitos da maneira mais expansiva o possível. O objetivo desta Monografia não é dissertar extensamente sobre a CRFB/88 em si ou sobre os direitos fundamentais, mas sim, focar especificamente nos direitos fundamentais relacionados à privacidade, vida privada e intimidade e, posteriormente, os direitos fundamentais relacionados à proteção de dados pessoais, todos previstos pelo art. 5º, X e LXXIX, respectivamente, da CRFB/88.

Nesse sentido, transposta uma breve contextualização sobre a CRFB/88 e os direitos fundamentais garantidos pelo texto constitucional, impõe-se a busca por uma conceituação e apresentação dos direitos fundamentais garantidores da proteção à intimidade e vida privada (estampados pelo art. 5º, X, da CRFB/88). Isto porque,

conhecendo bem do que trata esta categoria de direitos e sobre quais bases ela está alicerçada, a importância de sua tutela, de maneira mais ampla, estará perfeitamente justificada.

Primeiramente, é importante dizer que os direitos da personalidade derivam diretamente do princípio da dignidade da pessoa humana, uma vez que formam as prerrogativas essenciais da pessoa humana, a fim de garantir ao indivíduo o fomento e a expansão de suas potencialidades máximas, afirmando, dessa maneira, a capacidade de autodeterminação da pessoa em seu desenvolvimento.

Adriano de Cupis, em sua obra *Os direitos da personalidade* (2004), ainda deixa claro que existem certos recursos sem os quais a personalidade humana restaria uma susceptibilidade completamente irrealizada, privada de todo o valor concreto: direitos sem os quais todos os outros direitos subjetivos perderiam todo o interesse para o indivíduo – o que equivaleria a dizer que, se eles não existissem, a pessoa não existiria como tal. São os direitos da personalidade. Que a denominação de direitos da personalidade seja reservada aos direitos essenciais justifica-se plenamente pela razão de que eles constituem a medula da personalidade.

A construção atual dos direitos da personalidade é consequência das construções pós-guerra, momento em que era necessário garantir aos indivíduos um mínimo essencial ao desenvolvimento de suas personalidades. Adriano de Cupis preceitua que

[...] todos os direitos, na medida em que destinados a dar conteúdo à personalidade, poderiam chamar-se 'direitos da personalidade. Todavia, no contexto jurídico, essa designação é exclusiva dos direitos subjetivos, que possuem grande significância em relação aos direitos da personalidade, constituindo um *minimum* necessário e imprescindível ao seu conteúdo. (2004, p.)

Maria Helena Diniz, em seu *Curso de Direito Civil* (2011), citando Goffredo Telles Júnior, pontua que:

[...] a personalidade consiste no conjunto de caracteres próprios da pessoa. A personalidade não é um direito, de modo que seria errôneo afirmar que o ser humano tem direito à personalidade. A personalidade é que apoia os direitos e deveres que dela irradiam, é o objeto do direito, para que possa ser o que é, para sobreviver e se adaptar às condições do ambiente em que se encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens. O Direito objetivo autoriza a pessoa a defender sua personalidade, de forma que, para Goffredo

Telles Jr., os direitos da personalidade são os direitos subjetivos da pessoa de defender o que lhe é próprio, ou seja, a identidade, a liberdade, a sociabilidade, a reputação, a honra, a autoria, etc. Por outras palavras, os direitos da personalidade são direitos comuns da existência, porque são simples permissões dadas pela norma jurídica, a cada pessoa, de defender um bem que a natureza lhe deu, de maneira primordial e direta. (p. 90).

Sendo assim, de maneira geral, pensa-se que os direitos da personalidade formam uma categoria de direitos que ultrapassa, de certa forma, a construção tradicional que se tem de direitos subjetivos de ordem patrimonial, uma vez que esses direitos têm por objetivo a proteção à pessoa humana e sua dignidade, valores estes importantes para a boa convivência dos indivíduos em sociedade.

A dignidade da pessoa humana é um valor fundamental do sistema e o núcleo essencial dos direitos da personalidade. Nota-se que a personalidade humana não se concretiza apenas através de direitos subjetivos, mas também através de uma complexidade de situações jurídicas subjetivas que podem apresentar-se sob os mais diversos paradigmas. A personalidade humana, portanto, não é meramente um direito, mas sim, um valor fundamental que abrange diversas situações de existência e que precisam ser tuteladas de maneira eficaz.

Como os direitos à privacidade, intimidade e vida privada fazem parte dos direitos da personalidade, como discutido acima, passa-se agora a uma tentativa de conceituação de cada um desses direitos individualmente.

São várias as discussões envolvendo os temas da privacidade, vida privada e intimidade. A principal dificuldade em definir cada um desses conceitos vem do fato de cada um desses termos se distinguirem a partir de parâmetros não só da época e lugar em que são situados, mas também do *modus operandi* de cada um desses direitos. Por envolverem diretamente aspectos temporais, espaciais, pessoais e socioculturais relacionados diretamente com a evolução tecnológica, devem ser interpretados em sua forma mais dinâmica, para que, de fato, possam acompanhar a evolução social. De um lado, o conteúdo desses direitos parece flexível, mas resguardar a privacidade, diante de tantos aspectos externos, parece ser um interesse conjunto, de todos.

Alguns estudiosos acreditam que não é necessário fazer qualquer distinção entre os conceitos de privacidade, intimidade e vida privada. Para Ana Paula Gambogi Carvalho, a

[...] diferenciação apresenta uma reduzida importância, uma vez que os efeitos jurídicos da violação da intimidade e vida privada são idênticos, ensejando no âmbito civil, o dever de reparação consistente no pagamento de indenização dos danos morais e patrimoniais sofridos pela vítima. (2003, p. 77).

Todavia, o fato de CRFB/88 prever a mesma consequência jurídica para a violação a esses bens, qual seja, o dano moral e material, não significa que os conceitos desses direitos sejam os mesmos e que, portanto, não se faz necessária uma diferenciação entre eles ou que a aplicação da reparação aos danos morais e materiais se daria na mesma intensidade.

Primeiramente, a privacidade é um conceito relacionado diretamente ao desenvolvimento da personalidade humana, uma vez que a garantia ao cidadão de que ele não seja submetido a nenhum controle social que viole a sua privacidade é essencial. Cada indivíduo deve ter a sua privacidade garantida em suas relações internas e externas e tal garantia é um dever do Estado.

A privacidade se refere, em uma primeira análise, ao ambiente doméstico, às relações de família, relações afetivas, aos hábitos, à imagem etc. Nas palavras de José Afonso da Silva, a privacidade é “*o conjunto de informações acerca do indivíduo, que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito*” (1992, p. 188), o que reflete, portanto, em todas as suas manifestações concernentes à personalidade, no aspecto íntimo e privado.

A proteção da privacidade enquanto tutela da pessoa humana deve ser vista como um elemento positivo, o qual funciona como indutor da cidadania, da própria atividade política e dos direitos de liberdade de forma geral. O conceito de privacidade, portanto, deve ser visto como um pressuposto do funcionamento da sociedade democrática atual.

Passando para o conceito de vida privada, pode-se dizer que a vida privada é onde se fixa a noção das relações interindividuais que devem permanecer ocultas ao público. Segundo Gilmar Mendes, o direito à vida privada “[...] *teria por objeto os comportamentos e acontecimentos inerentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público.*” (2008, p.)

Nesse sentido, a vida privada não se confunde com a intimidade, já que é menos

secreta que esta. A vida privada não diz respeito aos segredos íntimos da pessoa, mas sim, à sua vida familiar, sua vida no trabalho, no relacionamento com os seus amigos. A vida privada é um viver entre outros indivíduos, mas que, ao mesmo tempo, exige uma reserva. A vida privada abrange os aspectos que não deveriam cair em meio à esfera pública, ou seja, é tudo aquilo que não devem ser objeto à informação nem curiosidade externa.

Tércio Sampaio Ferraz Júnior, em *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado* (1993), p.53, expressa que a vida privada envolve a proteção de formas exclusivas de convivência, ou seja, trata-se de situações em que a comunicação é inevitável e excluídos de terceiros. Terceiro, no caso, seria aquele que não participa da situação, que está interessado em outras coisas. O terceiro faz parte da sociedade, da qual a vida privada se desenvolve, mas não faz parte desta.

A vida privada, resumindo, se desenvolve numa inter-relação entre as pessoas. Em alguns casos, a vida privada pode ser mais reservada, como, por exemplo, no núcleo familiar, mas em outros casos pode ser mais exposta, pensando, por exemplo, em situações em que a pessoa se encontra em um clube, em reuniões, entidades religiosas etc. De toda forma, situando-se na esfera da vida privada, deve haver proteção e tutela a esse direito.

O último pilar do tripé relacionado a esses direitos de personalidade é a intimidade. O termo “intimidade” deriva diretamente do latim *intimus*, que significa “em dentro”. Esse termo traz uma ideia de interior, escondido, algo secreto e pode ser exemplificado através daquilo que o ser humano sente em seu interior, como, por exemplo, os seus medos, angústias, planos futuros e ambições.

Gilmar Mendes buscou definir esse termo dizendo que “*o cerne do direito à intimidade são as conversas e as situações mais íntimas daquele indivíduo envolvendo as relações familiares ou de amizades mais próximas.*” (2008, p.)

José Afonso da Silva, em seu *Curso de Direito Constitucional Positivo* (1992, p. 205), também diz que a intimidade está na esfera mais íntima do indivíduo, na medida que abrange pensamentos, desejos, convicções. Diferentemente da vida privada que significa o direito da pessoa de viver uma vida própria, tendo relações, livremente, com que, quiser.

Manoel Gonçalves Ferreira Filho ainda afirma que

Os conceitos constitucionais de intimidade e vida privada apresentam grande interligação, podendo, porém, ser diferenciados por meio da menor amplitude do primeiro que se encontra no âmbito da incidência do segundo. Assim, o conceito de intimidade relaciona-se às relações subjetivas e de trato íntimo da pessoa humana, suas relações familiares e de amizade, enquanto o conceito de vida privada envolve todos os relacionamentos da pessoa, inclusive os objetivos, tais como relações comerciais, de trabalho, de estudo, etc. (1997, p. 35)

A partir do que já foi dito sobre os conceitos de intimidade e vida privada, pode-se dizer que, de certa forma, esses dois conceitos refletem a ideia de autonomia e refletem o âmbito pessoal que, em tese, não admite interferências externas.

Para José Adércio Leite Sampaio, em sua obra *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte* (1988, p. 240), a intimidade e a vida privada constituem um conjunto de informações pessoais submetidas a um regime jurídico de contenção que se define como (i) exclusão do conhecimento alheio; (ii) como controle de informações pessoais; e (iii) como controle do acesso pessoal ou limitação a este.

Na visão de Manoel Gonçalves Ferreira Filho, embora os conceitos de intimidade e vida privada tenha relação, eles se diferem quanto à extensão, pois, segundo o autor, a vida privada possui maior extensão do que a intimidade. Nesse cenário, percebe-se que o conceito de intimidade envolve segredos que uma pessoa guarda para si própria (ou compartilha com poucos), o que faz com que a intimidade tenha um aspecto bem pessoal. Por isso, a transgressão à intimidade exige que o dano seja maior, conseqüentemente.

Por outro lado, a vida privada compreende fatos e acontecimento que, embora não sejam conhecidos pelo público externo, ultrapassam o indivíduo, já que existe uma relação deste com a sociedade. Exemplos dessa situação seriam o sigilo telefônico e bancário. Muito embora a pessoa não deseje que o conteúdo seja divulgado, não se trata, necessariamente, de um segredo, pois são de conhecimento de um ciclo maior de pessoas.

Alexandre de Moraes também complementa que:

Os conceitos constitucionais de intimidade e vida privada apresentam grande interligação, podendo, porém, ser diferenciados por meio da menor amplitude do primeiro, que se encontra no âmbito de incidência do segundo. Assim, o conceito de intimidade relaciona-se às relações subjetivas e de trato íntimo da pessoa humana, suas relações

familiares e de amizade, enquanto o conceito de vida privada envolve todos os relacionamentos da pessoa, inclusive os objetivos, tais como relações comerciais, de trabalho, estudo, etc. (2011, p. 57)

José Afonso da Silva também fez distinções importantes em seus comentários à CRFB/88. Explica o autor que a intimidade pode ser caracterizada como uma esfera secreta da vida de uma pessoa, sendo possível que essa pessoa tenha o poder de evitar que demais infrinjam essa esfera. No mesmo panorama, Adriano de Cupis define a intimidade (*riservatezza*) como um modo de ser da pessoa que consiste na exclusão do conhecimento de outrem de quando se refira à pessoa mesma. Abrange, portanto, nesse sentido mais reservado, a inviolabilidade do domicílio, o segredo profissional, o sigilo da correspondência. De acordo com Silva:

Não é fácil distinguir “vida privada” de “intimidade”. Aquela, em última análise, integra a esfera íntima da pessoa, porque é repositório de segredos e particularidades do foro moral e íntimo do indivíduo. Mas a Constituição não considerou assim. De destaque ao conceito, para que seja mais abrangente. (...) Parte da constatação de que a vida das pessoas compreende dois aspectos: um voltado para o exterior e outro para o interior. A vida exterior, que envolve a pessoa nas relações sociais e nas atividades públicas, pode ser objeto das pesquisas e divulgações. (...) A vida interior (...) é a que integra o conceito de vida privada. (2011, p. 105)

Desta maneira, com base nos comentários acima, entende-se que, desde que não envolva ato ilícito, ou não invadindo a esfera de terceiros, aquilo que diz respeito à intimidade do indivíduo, não pode ser objeto de ponderação em face dos outros direitos fundamentais envolvendo os direitos de personalidade. Resumindo, portanto, a intimidade é o núcleo capaz de proteger o indivíduo das situações de violação daqueles que compartilham a vida privada com ele.

Assim, como já exposto nessa Monografia, não há como falar de proteção aos dados pessoais, sem antes mencionar os direitos à intimidade, vida privada e privacidade. Dados pessoais dizem respeito ao ser humano como indivíduo de uma comunidade, são as informações que o qualificam como ser único. O nome, sobrenome, seu CPF, número de RG, telefone pessoal, dentre outros, são informações inconfundíveis de uma pessoa para outra, fazem parte de sua intimidade, de sua vida privada.

Portanto, nos próximos capítulos, será detalhado com mais atenção os conceitos de dados pessoais e como a legislação brasileira vem atuando para defender a proteção dos dados pessoais diante de tantos fatores externos que podem comprometer sua integridade. Para a presente Monografia, tomou-se como fator externo determinante para a proteção aos dados pessoais, as práticas do reconhecimento facial e controle de massas, que também serão detalhados posteriormente.

O próximo capítulo é destinado a descrever as principais características de regulações que foram essenciais para criar, no Brasil, uma noção maior sobre a importância de se ter a privacidade regulada legalmente. Na Europa, principalmente, as discussões sobre privacidade, intimidade e proteção aos dados pessoais já são consolidadas há anos, sendo que, no Brasil, essa ideia somente começou a ser mais discutida a partir de 2014, com a entrada em vigor do Marco Civil da Internet.

A regulação sobre dados pessoais em si, a LGPD, somente entrou em vigor em 2018, ou seja, trata-se de regulação extremamente recente e que ainda não está completamente definida quanto aos seus preceitos. Diversas discussões sobre a lei ainda devem ser definidas para que a LGPD esteja válida em sua completude. Nesse sentido, as próximas páginas buscam elucidar sobre como a ideia de proteção à intimidade, privacidade e proteção aos dados pessoais vem sendo regulada no Brasil.

3. A NECESSÁRIA APLICAÇÃO DE LEIS E REGULAMENTOS INFRACONSTITUCIONAIS DE PROTEÇÃO DE DADOS PESSOAIS

3.1. DA APLICABILIDADE DO MARCO CIVIL DA INTERNET (LEI 12.965/2014)

O tratamento de dados pessoais no Brasil, bem como algumas de suas regulamentações, não se deu somente com o advento da LGPD, em 2018. As novas tecnologias existentes no século XXI já refletiam a necessidade de existir algum tipo de regulamentação sobre o tema, principalmente, no campo da Internet.

Diante desse cenário, o Marco Civil da Internet foi uma das primeiras tentativas no Brasil de regular a Internet e as informações que transacionam neste ambiente. Levando em consideração o tema principal dessa Monografia, faz-se necessário um breve estudo sobre o Marco Civil da Internet e quais de suas disposições estão ligadas à privacidade e proteção de dados pessoais.

O maior detalhamento sobre essa regulação torna-se importante na medida em que sua entrada em vigor foi em 2014, 4 anos antes da entrada em vigor da LGPD e das discussões sobre IA, avanços tecnológicos e garantias fundamentais. Certamente, a tecnologia existente em 2014 já não era mais a mesma em 2018, razão pela qual a LGPD considera outros aspectos em relação aos meios nos quais informações e dados pessoais podem transacionar. De toda forma, já em 2014, o tema de privacidade e preservação da intimidade dos indivíduos já era uma pauta existente no Brasil.

Por ser uma legislação de cunho principiológico, o Marco Civil da Internet tem como principal finalidade estabelecer os princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Para isso, instituiu uma série de diretrizes que deverão ser seguidas pelos entes federativos (União, Estados, Distrito Federal e Municípios), provedores de Internet, empresas e todos os outros envolvidos na aplicação, disponibilização e uso do ciberespaço.

Dessa forma, o Marco Civil da Internet constitui lei especial aplicável ao uso da Internet no Brasil, estabelecendo princípios, garantias, direitos e deveres de usuários e provedores. Como tal, em relação às situações específicas que trata, prevalece sobre outros diplomas legais, como o Código de Defesa do Consumidor, ainda que a aplicação deste às relações de consumo estabelecidas na Internet tenha sido expressamente prevista (artigo 7º, inciso XIII).

Para exemplificar, a responsabilidade do provedor de aplicações de Internet pelos danos decorrentes de conteúdo gerado por seus usuários é regida pelas disposições do Marco Civil da Internet (artigos 19 a 21), e não pela norma correspondente do Código de Defesa do Consumidor (artigo 14), que é destinada às relações de consumo em geral, mas não às situações específicas versadas naquele diploma, tendo, portanto, caráter mais geral.

Portanto, as normas do Código de Defesa do Consumidor, do Código Civil e de outros diplomas legais aplicam-se aos provedores de aplicações de Internet e às relações por estes mantidas com seus usuários e terceiros somente nas hipóteses que não sejam expressamente reguladas pelo Marco Civil da Internet.

As normas de direito material do Marco Civil da Internet não dependentes de regulamentação aplicam-se a situações jurídicas ocorridas a partir de 23.6.2014. Não afetam, por conseguinte, situações jurídicas anteriores a essa data, ainda que sejam objeto de demandas em andamento ou futuras. Já as normas de direito material do Marco Civil da Internet pendentes de regulamentação não se aplicam até a entrada em vigor dos respectivos diplomas regulamentadores. Não geram, dessa forma, efeitos a partir de 23.6.2014.

Como o objetivo desse item não é detalhar o Marco Civil da Internet em sua completude, mas tão somente reforçar as ideias ligadas à privacidade e proteção de dados pessoais abordados por essa lei, abaixo serão destacadas algumas passagens da lei ligadas a esses aspectos, os quais são diretamente conectados ao tema central desta Monografia.

O Marco Civil da Internet é claro no sentido de que demandas que versem

[...] sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na Internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais (Artigo 19, § 3º). (BRASIL, 2014).

O dispositivo não afasta os pressupostos necessários para a configuração da competência dos Juizados Especiais previstos na Lei nº 9.099/1995, tais como o valor máximo da demanda, correspondente a 40 (quarenta) salários-mínimos, e a menor complexidade da causa.

Essa passagem da lei é importante, pois se relaciona muito ao art. 5º, X, da CRFB/88 que expressa claramente o direito a indenização por violação à intimidade, a vida privada, a honra e a imagem das pessoas.

Não obstante, no âmbito de ações judiciais em que haja a pretensão de tornar indisponível conteúdo gerado por terceiros, inclusive processadas nos juizados especiais, o juiz

[...] poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação” (Artigo 19, § 4º). (BRASIL, 2014).

Assim, ordens judiciais antecipatórias da tutela direcionadas a provedores de aplicações, determinando que tornem indisponível conteúdo gerado por terceiros, proferidas a partir de 23.6.2014, devem levar em consideração, além dos pressupostos previstos no artigo 273, inciso I, do Código de Processo Civil, “o *interesse da coletividade na disponibilização do conteúdo na internet*”.

O Marco Civil da Internet também prevê expressamente a inviolabilidade de um conjunto de dados e informações relacionadas aos usuários da Internet (titulares de dados pessoais), estabelecendo regras para sua coleta, armazenamento, utilização e fornecimento a terceiros.

Além de não conter qualquer definição de dados pessoais, o texto do Marco Civil da Internet estabelece, em diferentes dispositivos, relações distintas entre tais informações e os registros de acesso a aplicações de Internet, o que torna obscura a sua conceituação. Para exemplificar: o artigo 7º, inciso VII, sugere que o conceito de “dados pessoais” abrange os registros de acesso a aplicações de Internet, ao passo que o artigo 10 sugere que o conceito de dados pessoais não se confunde com os registros de acesso a aplicações de Internet, tratando-se de informações diversas. Por fim, a definição legal de registros de acesso a aplicações de Internet não faz qualquer referência a dados pessoais.

O Marco Civil da Internet estabelece que os dados pessoais dos usuários somente podem ser utilizados pelo provedor 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 (artigo 7º,

inciso VIII). Diante da dificuldade de conceituação de dados pessoais, é recomendável que tal obrigação seja compreendida como aplicável, inclusive, aos registros de acesso a aplicações de Internet. Sendo assim, podemos observar, de certa forma, uma relação com os conceitos que posteriormente serão regulados pela LGPD.

O Marco Civil da Internet prevê, ainda, que os dados pessoais devem ser definitivamente excluídos pelo provedor ao término da relação com o usuário, caso este assim requeira (artigo 7º, inciso X), o que não afasta a obrigatoriedade de guarda de registros de acesso a aplicações de Internet na forma e prazos estabelecidos.

Embora o Marco Civil da Internet obrigue os provedores de aplicações de Internet a atenderem, desde logo, à preservação da intimidade, vida privada, honra e imagem das pessoas quanto à guarda e disponibilização dos registros de acesso a aplicações, dados pessoais e conteúdo de comunicações privadas, ainda serão definidos em regulamento os padrões a serem atendidos pelas respectivas medidas e procedimentos de segurança e sigilo (artigos 10, § 4º, e 15).

Portanto, não são exigíveis dos provedores de aplicações de Internet, por ora, padrões específicos aplicáveis às medidas e procedimentos de segurança e sigilo dos registros de aplicações de Internet, dados pessoais e conteúdo das comunicações privadas dos seus usuários.

O Marco Civil Da Internet tinha como objetivo central regular o ambiente da Internet no Brasil em 2014 e seus preceitos são fortemente utilizados em decisões judiciais atualmente no que tange a infrações no meio digital. O foco do Marco Civil da Internet, por outro lado, não era tratar em detalhes sobre a intimidade, privacidade e proteção de dados pessoais, muito embora esses conceitos já fossem amplamente regulados na Europa e Estados Unidos.

O que se observa com as passagens legais acima é que o Marco Civil da Internet, apesar de regular, já em 2014, alguns conceitos relacionados aos dados pessoais, não tratava especificamente sobre as situações nas quais os dados pessoais poderiam ser tratados, compartilhados, armazenados, e não tratava com exatidão as bases legais que justificam o tratamento de dados pessoais. Tal função foi atribuída à LGPD e isso será mais detalhado a seguir.

3.2. DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS GARANTIDO PELA CFRB/88

Antes de abordar sobre a LGPD em si, é importante pontuar o momento em que a proteção à privacidade e aos dados pessoais foi inserida na CRFB/88 como direito fundamental. Normas infraconstitucionais são essenciais para tratar do tema central dessa dissertação, mas a previsão constitucional sobre o tema também é extremamente importante, devido a sua posição de supremacia.

Muito embora estejamos na terceira década do século XXI, ainda existem diversos Estados constitucionais nos quais o direito fundamental à proteção dos dados pessoais não é positivado em suas Constituições, mesmo que, implicitamente, tal direito seja comumente aceito.

No Brasil, foi apenas recentemente que a proteção aos dados pessoais foi inserida no texto constitucional como sendo um direito fundamental. Tal movimento foi feito meio da PEC 17/19, de modo a incorporar um direito fundamental à proteção de dados pessoais ao catálogo de direitos e garantias expressos pela CRFB/88.

A necessidade dessa regulação tem como premissa a elaboração de uma lei brasileira voltada especificamente à privacidade e proteção dos dados pessoais, a LGPD, de 2018. Embora a LGPD não sirva de base e justificativa constitucional direta para reconhecimento de um direito fundamental, o conteúdo e o alcance dessa legislação carece de limitação a partir do marco normativo constitucional.

O direito à proteção dos dados pessoais deve ser associado a alguns princípios e direitos fundamentais de caráter geral e especial, como, por exemplo, o direito fundamental da dignidade da pessoa humana, o direito ao desenvolvimento da personalidade, à privacidade e intimidade. Dessa forma, com a aprovação da PEC e sua posterior promulgação em 2022, através da EC 115/22, a discussão sobre a proteção dos dados pessoais no Brasil foi superada. Conforme prevê tal emenda constitucional, o art. 5 da CRFB/88 passou a ser acrescido da seguinte redação:

Art. 5º, LXXIX: é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Por mais que anteriormente o STF já reconhecia a proteção aos dados pessoais, foi somente com a positivação da EC 115/22 que tal direito foi de fato formalmente atribuído ao texto constitucional. Mediante redação dada pela EC 115/22, o direito

fundamental à proteção de dados pessoais passa estar submetido a uma reserva legal simples, que limita o legislador infraconstitucional a observância das exigências legais.

Dessa forma, o direito fundamental à proteção dos dados pessoais ganha ainda maior relevância. Isso porque a LGPD possui lacunas, já que não prevê a regulamentação do tratamento de dados pessoais nos setores de segurança nacional, de segurança pública, investigação criminal e execução penal, por exemplo. Essas, inclusive, são as áreas de maior utilização da prática do reconhecimento facial e da vigilância em massa. Dessa forma, por assumir caráter de direito fundamental, previsto constitucionalmente, tais lacunas tendem a ser amenizadas.

Os dados e informações pessoais pertencem exclusivamente ao indivíduo e a mais ninguém – é por este motivo que são “pessoais”, intransferíveis. Cabe ao titular desses dados pessoais, portanto, o poder de determinar a quem esses dados podem ser revelados e sob quais circunstâncias.

Hoje em dia, as informações alcançam velocidade que não se tinha no passado e tudo isso foi favorecido pelas novas tecnologias e revoluções de IA, que são capazes de prever e descrever comportamentos e interesses no âmbito coletivo e individual com muita precisão.

Por todo este cenário, faz-se imperativo na modernidade atual que se tenha, no Brasil, um preceito com força constitucional que faça com que a nação tenha comprometimento com a privacidade e proteção dos dados pessoais. O espírito da CRFB/88 é cumprir com a função institucional de oferecer ao Brasil uma legislação moderna, eficiente e que seja capaz de acompanhar os avanços tecnológicos com precisão, para, enfim, proteger a liberdade e a garantia de direitos aos cidadãos brasileiros.

Não há como imaginar atualmente nenhuma atividade na sociedade que não se utilize da tecnologia, mesmo que minimamente. A Internet foi altamente capaz de transformar todas as relações existentes. Transformou as nações, o mercado, as democracias, a ciência, a educação e até mesmo a religião. Todavia, todos esses avanços também possuem riscos.

O avanço da tecnologia traz novos desafios na esfera jurídica. Se por um lado o avanço da tecnologia favoreceu a sociedade e venceu fronteiras, por outro lado, tudo isso vem sendo feito com a utilização cada vez maior de dados pessoais e informações comportamentais da sociedade. Empresas atualmente utilizam dados pessoais dos indivíduos para direcioná-los a compras, investimentos e relações

interpessoais. Por isso, é fundamental compreender a importância dos dados pessoais na sociedade global, assim como é fundamental reconhecer e mitigar riscos que decorrem da sua utilização.

A posituação da proteção aos dados pessoais pela CRFB/88, nesse sentido, é de extrema relevância. Junto aos outros direitos fundamentais ligados à personalidade (direito à intimidade, privacidade e vida privada), a proteção dos dados pessoais faz com que a população brasileira possa, não somente ter como base legal uma lei especificamente voltada à privacidade (a LGPD), como adotar um parâmetro acima dessa lei, qual seja, a CRFB/88, suprema na proteção de garantias e deveres do Estado e seus subordinados.

Como já abordado, além da EC 115/22 que alterou o texto da CRFB/88, foi de extrema importância que o Brasil adotasse uma lei infraconstitucional que fosse capaz de atender a todos os requisitos legais ligados à privacidade e proteção de dados pessoais. A LGPD, mesmo que recente, vem ganhando força incomparável no Brasil. Não é possível falar sobre dados pessoais no Brasil e sobre as consequências de sua utilização sem mencionar a LGPD.

Essa lei, como será detalhado a seguir, traz conceitos extremamente significativos para o tratamento de dados pessoais no Brasil, seja em quesitos comerciais, pessoais ou até mesmo internacionais. Dessa forma, para limitar o tema central dessa Monografia, faz-se necessário, além de pontuar o significado da previsão constitucional de proteção aos dados pessoais como direito fundamental, pontuar os aspectos centrais da LGPD.

3.3.A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI 13.709/2018 – A “LGPD”) E SEUS PRINCIPAIS CONCEITOS

A privacidade no Brasil, de maneira geral, é protegida através da CRFB/88, como mencionado no tópico anterior, do Código de Defesa do Consumidor (Lei nº 8.078/90) e do Marco Civil da Internet (Lei nº 12.965/14). Em agosto de 2018, foi promulgada a LGPD, que se inspira no Regulamento Geral Europeu de Proteção de Dados (*General Data Protection Regulation* - "GDPR").

A LGPD entrou em vigor em 18 de setembro de 2020 e trouxe profundas alterações ao tratamento de dados pessoais, prevendo um conjunto de regras a serem

observadas em atividades como a coleta, produção, armazenamento, utilização, transferência, compartilhamento e exclusão de dados pessoais.

De acordo com a LGPD, "**dados pessoais**" são informações relacionadas a uma pessoa natural identificada ou identificável (BRASIL, 2018). Nome, CPF, endereço e data de nascimento são alguns exemplos de dados pessoais, mas informações como hábitos de consumo, localização geográfica, perfil comportamental, preferências, histórico de compras, *score* de crédito e outras informações semelhantes, quando relacionadas com uma pessoa singular identificada ou identificável, também são consideradas dados pessoais. Os dados relativos a pessoas jurídicas não são considerados "dados pessoais" para os fins da LGPD.

A definição de "**dados pessoais sensíveis**" trazida pela LGPD inclui dados pessoais relacionados a origem racial ou étnica, crenças religiosas, opiniões políticas, filiação a um sindicato ou organização religiosa, filosófica ou política, dados sobre saúde ou vida sexual, dados genéticos ou **biométricos** (BRASIL, 2018). Portanto, conclui-se, desde já, que o reconhecimento facial, por utilizar dados biométricos, é um tipo de dado pessoal sensível que merece maior atenção.

A LGPD tem uma vasta gama de aplicações e atinge indivíduos e entidades jurídicas privadas e públicas, independentemente do país onde se encontram ou onde os dados são hospedados, desde que (i) o tratamento de dados pessoais ocorra no Brasil; (ii) a atividade de tratamento se destine a oferecer ou fornecer bens ou serviços ou a tratar dados de indivíduos localizados no Brasil; ou (iii) os dados pessoais em tratamento tenham sido coletados no Brasil / os titulares dos dados estejam localizados no Brasil no momento em que os seus dados pessoais são coletados (BRASIL, 2018).

Levando em consideração seu amplo escopo, a LGPD é capaz de interferir nos negócios de empresas brasileiras e estrangeiras, com impacto no tratamento de dados pessoais, não só no contexto do fornecimento de produtos e serviços, mas também em outras esferas, tais como relações de trabalho e acordos entre empresas.

A LGPD se aplica a qualquer atividade de tratamento de dados pessoais realizada dentro do escopo da LGPD. Para os fins da lei, "tratamento" de dados pessoais significa qualquer operação realizada sobre os dados pessoais, incluindo, mas não limitado a, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018).

A Autoridade Nacional de Proteção de Dados ("ANPD") é responsável por outros regulamentos, orientações e interpretações sobre a lei. Entretanto, dado que a ANPD só se tornou operacional no final de novembro de 2020, ainda há um nível de incerteza sobre a aplicação de algumas disposições da LGPD. Além disso, a LGPD pode muitas vezes ser menos detalhada do que o GDPR, e, nesse sentido, espera-se que a ANPD regule ainda mais os direitos e obrigações e emita diretrizes sobre tópicos relevantes (tais como os mecanismos de transferência internacional). Não obstante, é relevante destacar que a ANPD pode incluir o reconhecimento facial e a regulamentação biométrica em sua agenda regulatória para 2023/2024, que ainda estão em discussão pública.

Deve-se notar que a lei que regula dados pessoais no Brasil é recente e não há muita orientação sobre como ela será interpretada pelas autoridades. Em particular, a LGPD não contém os considerandos abrangentes e úteis que introduzem o GDPR. Entretanto, como mencionado acima, os legisladores brasileiros buscaram inspiração no GDPR para elaborar a LGPD e importaram vários conceitos do GDPR para a LGPD. Portanto, é razoável esperar que as autoridades brasileiras possam buscar mais inspiração na Europa para interpretar e aplicar lei brasileira em alguns casos.

As obrigações previstas pela LGPD podem variar dependendo se uma empresa é considerada como controladora ou operadora. "**Controlador**" é a pessoa física ou jurídica (privada ou pública) que toma as decisões em relação aos dados pessoais coletados. Já o "**Operador**" é a pessoa física ou jurídica (privada ou pública) que trata os dados em nome e sob as instruções do respectivo controlador. Uma empresa pode ser controladora em relação a certas atividades de tratamento e operadora em outras atividades. Tanto os controladores quanto os operadores devem cumprir com a LGPD e estão sujeitos à supervisão da ANPD.

Para fins dessa Monografia também é importante destacar quais são os princípios previstos pela LGPD, já que estes são determinantes para avaliar se determinado tratamento de dados pessoais está ocorrendo em conformidade com a lei ou não. Nesse sentido, conforme expresso pelo Art. 6º, da LGPD, o tratamento de dados pessoais deve respeitar os seguintes princípios:

- a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- d) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- e) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- f) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- g) segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e
- j) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o

cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Como os dados pessoais são únicos e intransferíveis, pois dizem respeito ao âmbito íntimo e pessoal do indivíduo, não seria razoável esperar que esses dados fossem utilizados de qualquer forma, sem nenhuma base legal que o justificasse. Dessa maneira, para fins da LGPD, para toda atividade de tratamento de dados pessoais deve-se atribuir uma das bases legais expressas pelo art. 7º da lei. Tal determinação permite que não haja tratamento de dados pessoais dos titulares sem necessidade ou de forma descontrolada. Segundo o referido artigo da LGPD (BRASIL, 2018):

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

I - mediante o fornecimento de consentimento pelo titular;

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

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

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

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

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

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

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

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

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

No tocante ao tratamento de dados pessoais sensíveis, a LGPD faz uma distinção quanto às possíveis bases legais aplicáveis e as destaca em seu art. 11, conforme o abaixo:

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;

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.

Os controladores estão encarregados de determinar a base legal mais apropriada de acordo com a LGPD. Tal avaliação depende de quais dados serão coletados dos titulares de dados pessoais e para quais propósitos. Os operadores, por outro lado, confiam na base legal identificada pelo respectivo controlador, desde que tal base legal cubra as finalidades do tratamento do qual o operador será responsável.

Como em muitos outros pontos, a LGPD seguiu a estrutura do GDPR em relação às bases legais para o tratamento de dados pessoais. Na legislação europeia, não há base legal que possa ser considerada, de forma absoluta, melhor, mais segura ou mais importante do que as outras. É necessário realizar uma análise caso a caso para que seja possível verificar qual a base legal que melhor se adapta às circunstâncias específicas.

Como consequência, o consentimento é uma das hipóteses legais para o tratamento de dados pessoais previsto pela LGPD, e não como a principal ou preferível base legal. Em termos de técnica legislativa, não há hierarquia entre as bases legais, pois todas elas estão listadas horizontalmente nos itens dos artigos 7 e 11 da LGPD.

Embora no artigo 11 haja uma divisão das bases legais em dois itens (um deles define o consentimento e o outro define as hipóteses com renúncia ao consentimento), não há disposição que estabeleça a prevalência de uma das bases legais neste artigo, assim como não há nada na LGPD que permita atribuir ordem hierárquica às bases legais ou tratar hipóteses que não o consentimento como residual. Pelo contrário, a legislação permite ao controlador escolher a base legal mais apropriada para o caso específico, mesmo quando a obtenção do consentimento do titular é uma alternativa possível.

A presente Monografia traz como tema principal a legalidade da prática do reconhecimento facial e da vigilância em massa diante dos princípios constitucionais sobre a privacidade, intimidade, vida privada e proteção aos dados pessoais, conforme descrito no capítulo anterior e tomando, ainda, como premissa, a legislação brasileira aplicável e, principalmente, a LGPD.

A prática do reconhecimento facial é identificada, pela LGPD, como um dado pessoal sensível, já que trata de dado biométrico. Nesse sentido, para que seja legítimo o tratamento desse dado pessoal sensível, é importante considerar algumas bases legais centrais que poderiam justificar esse tipo de tratamento. São elas, o consentimento, obrigação legal ou regulatória, legítimo interesse e prevenção à fraude, que serão detalhadamente abordadas a seguir.

A base legal do consentimento é expressa pela lei de proteção de dados pessoais em seu art. 7º, II e art. 11, II, a. A LGPD define o consentimento, em seu artigo 5, XII, como "manifestação livre, informada e inequívoca pela qual o envolvido concorda com o tratamento de seus dados pessoais para um fim específico". O consentimento obtido para o tratamento de dados pessoais sensíveis deve ser dado de forma específica e destacada, para fins específicos, de acordo com o artigo 11, inciso I, da LGPD. Se o consentimento obtido não estiver de acordo com os requisitos estabelecidos pela LGPD, poderá ser considerado nulo, nos termos do art. 8º, §§ 3º e 4º, e do art. 9º, § 1º, ambos da LGPD.

Além dos requisitos para que o consentimento seja considerado válido, é importante observar que o uso dessa base legal garante ao envolvido os seguintes direitos: (i) o direito de ser informado sobre a possibilidade de não dar consentimento e sobre as consequências dessa recusa (art. 18, VIII, da LGPD); (ii) o direito de revogar o consentimento (art. 8, §5º, e art. 18, IX, da LGPD), caso em que os agentes de processamento de dados devem cessar o processamento de dados pessoais com base no consentimento (art. 15, III, da LGPD); e (iii) o direito de solicitar a eliminação dos dados pessoais processados com base no consentimento (art. 18, VI, da LGPD), a menos que uma das exceções do artigo 16 da LGPD se aplique (em particular, o cumprimento de uma obrigação legal ou regulamentar).

A base legal do "cumprimento de obrigações legais ou regulatórias pelo controlador" é aplicável sempre que o controlador precisar tratar dados pessoais a fim de cumprir uma obrigação legal/regulatória. Essa base legal é aplicável ao tratamento

de dados pessoais comuns (art. 7, II, da LGPD) e dados sensíveis (art. 11, item II, a, da LGPD).

Em certos casos, o responsável pelo tratamento pode não ter poder discricionário sobre o tratamento de dados pessoais. Portanto, a LGPD prevê que esta base também pode fundamentar a manutenção dos dados mesmo após a finalidade de processamento do responsável pelo tratamento, desde que seja necessário demonstrar o cumprimento de obrigações legais ou regulamentares (por exemplo, uma autoridade pode solicitar ao responsável pelo tratamento que demonstre que cumpriu uma obrigação regulamentar aplicável a ele).

O item IX do art. 7º da LGPD autoriza o tratamento de dados pessoais quando necessário para atender aos interesses legítimos do responsável pelo tratamento ou de um terceiro, exceto no caso em que prevaleçam os direitos e liberdades fundamentais da pessoa em questão e exijam a proteção de dados pessoais. Como previsto pela LGPD, no caso de tratamento de dados sensíveis, o interesse legítimo não é uma base legal disponível, pois não está listado entre as bases legais para tratamento de dados sensíveis no art. 11 da LGPD. O tratamento de dados pessoais com base em interesse legítimo é geralmente a base legal mais flexível dos 10 (dez) disponíveis, pois não está vinculado a uma finalidade específica. Entretanto, nem sempre é a base legal mais apropriada para cada situação.

Sempre que o tratamento for baseado em interesse legítimo, o responsável pelo tratamento deverá adotar medidas que (i) garantam a transparência desse tratamento, conforme expressamente determinado pelo parágrafo 2 do art. 10 da LGPD, informando as pessoas em causa que esse compartilhamento ocorrerá, e (ii) possibilitem ao envolvido o exercício dos direitos previstos na LGPD.

É importante ressaltar que não existem precedentes judiciais ou administrativos relevantes no Brasil que ajudem na interpretação do uso do interesse legítimo como base legal para o tratamento de dados pessoais, dada a recente aprovação da LGPD e, conseqüentemente, o entendimento brasileiro se baseia essencialmente na interpretação teleológica da LGPD, bem como em conformidade com a interpretação dada a disposições similares da GDPR.

A LGPD fornece uma base legal que autoriza o tratamento de dados pessoais sensíveis baseado na prevenção de fraude e segurança dos titulares dos dados pessoais, em procedimentos de identificação e autenticação de registros em sistemas eletrônicos. A LGPD inovou em relação à prevenção de fraude como base legal

autônoma (como fez na base legal de proteção ao crédito). No GDPR, o tratamento de dados pessoais para fins de prevenção à fraude é baseado, mais comumente, em interesses legítimos. O GDPR não fornece "prevenção à fraude" como base legal.

Embora a LGPD não tenha definido o conceito de "prevenção de fraude" e considerando a atual falta de diretrizes para a aplicação da LGPD, entendemos que, neste momento, a "prevenção de fraude" deve ser interpretada como base legal para o tratamento de dados sensíveis (por exemplo, dados biométricos) no contexto da gestão de risco de autenticação e identificação de uma pessoa, e de operações de crédito e prevenção de fraude quando relacionadas às atividades de crédito que ela envolve.

Com o exposto acima sobre os principais conceitos da LGPD, pode-se observar que a prática do reconhecimento facial, como dado pessoal sensível, pode ser baseada em algumas bases legais, conforme mencionada neste item. A determinação da base legal mais adequada à utilização do reconhecimento facial, todavia, depende de cada caso analisado separadamente.

A indicação da base legal levará em consideração a finalidade para o tratamento de biometria, os motivos que levaram ao tratamento desse tipo de dado pessoal sensível, bem como a possibilidade de os titulares de dados pessoais poderem ser afetados de alguma forma por esse tipo de tratamento.

Dessa forma, sem regulamentações específicas, como a LGPD, os avanços tecnológicos não possuiriam freios. Cada vez mais empresas corporativas e de alta performance utilizariam dados e informações comportamentais dos titulares, sem qualquer tipo de limitação. A LGPD, nesse sentido, ganha extrema relevância, pois pretende proteger a intimidade, a privacidade e a vida privada dos indivíduos, fatores delicados e que merecem especial atenção diante de tantos avanços e entraves externos.

A análise sobre os casos práticos envolvendo dados biométricos que serão abordados nesta Monografia utilizam como pontos chave de argumentação passagens da LGPD. Tal fato apenas reforça que não é possível tratar sobre os avanços tecnológicos e sobre a prática do reconhecimento facial sem antes mencionar os dispositivos da LGPD e como eles devem ser compreendidos diante desses casos práticos.

As próximas páginas destinam-se a um maior detalhamento sobre o que é o reconhecimento facial e como ele está ligado umbilicalmente com as noções de privacidade e proteção de dados pessoais.

4. DOS AVANÇOS TECNOLÓGICOS NO SÉC. XXI A PARTIR DA ANÁLISE DOS DIREITOS E GARANTIAS CONSTITUCIONAIS ESTAMPADAS PELO ART. 5º, X E LXXI, DA CRFB/88

4.1. DA PRÁTICA DO RECONHECIMENTO FACIAL E VIGILÂNCIA EM MASSA

Como já exposto nesta Monografia diversas vezes, atualmente, há de se conviver com as mais diferentes tecnologias. Praticamente tudo que se usa para conviver minimamente em sociedade envolve aparelhos eletrônicos e IA. Essas tecnologias claramente são benéficas para a sociedade e para suas relações, já que, certamente, seria muito difícil conviver socialmente sem as tecnologias presentes no mundo.

O reconhecimento facial, como tema central desta Monografia, é uma das possíveis tecnologias que podem ser utilizadas pelos próprios cidadãos, mas também por autoridades ou órgãos governamentais que, na maioria das vezes, não transparece aos titulares desses dados o motivo do uso de tal tecnologia.

Nesse sentido, o objetivo deste capítulo é abordar mais especificamente sobre do que se trata a prática do reconhecimento facial e qual sua relação com os dados pessoais e, conseqüentemente, com a LGPD. Não obstante, serão abordados dois casos práticos e recentes que envolvem a temática para melhorar elucidar o assunto. Os próximos parágrafos explicarão o que é o reconhecimento facial e como os dados utilizados para essa prática se relacionam com a LGPD.

O rosto, assim como as impressões digitais, constitui nossa biometria; dados específicos e exclusivos que variam de indivíduo para indivíduo. Assim como as pessoas podem ser identificadas por meio de suas impressões digitais, elas também podem ser identificadas pelo registro preciso de seus rostos. É com base nessa premissa que surgiram as tecnologias de reconhecimento facial, que são o conjunto de ferramentas digitais usadas para executar tarefas em imagens ou vídeos de rostos humanos.

O reconhecimento facial é um dado biométrico e, portanto, é considerado um dado sensível pela LGPD, como já citado nessa Monografia. No entanto, apesar de se enquadrarem na categoria de dados biométricos, os dados obtidos a partir do reconhecimento facial possuem características específicas relacionadas ao seu modo

de coleta e uso da informação, pois podem: (i) ser utilizados à distância (diferentemente das impressões digitais, por exemplo); (ii) ser operacionalizados sem o conhecimento do indivíduo; (iii) ter sua precisão relacionada às condições de uso (por exemplo, luminosidade e foco); (iv) identificar um indivíduo em uma variedade de contextos diferentes (individualmente ou em grupos); (v) ser utilizados para estimar ou inferir outras características, como idade, gênero, origem racial ou etnia - sendo os dois últimos dados pessoais sensíveis.

A LGPD não trata especificamente de dados biométricos ou do reconhecimento facial, mas aborda o tema em seu artigo 5º, II, que classifica os dados biométricos como dados sensíveis e, portanto, traz maiores especificações sobre como eles devem ser tratados. De acordo com o artigo 11, g, da LGPD, os dados biométricos poderão ser utilizados pelas empresas na "garantia de prevenção de fraudes e segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e ressalvadas as hipóteses de direitos e liberdades fundamentais do titular que exijam a proteção de dados pessoais".

Atualmente, não há leis específicas no Brasil com relação à biometria ou ao reconhecimento facial, apenas projetos de lei pendentes de aprovação, tais como:

- i. PL 12/2015, que trata do uso da verificação biométrica e da segurança das informações nela contidas, exigindo o consentimento do titular dos dados para o armazenamento de dados biométricos; e
- ii. PL 4612/2019, que trata do desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional e outras destinadas à identificação de indivíduos e à previsão ou análise de comportamento.

Não há leis ou projetos de lei no Brasil que proíbam ou busquem proibir o uso da tecnologia de reconhecimento facial pelo setor privado. Como mencionado anteriormente, a regulamentação do reconhecimento facial e da biometria poderia ser incluída na agenda regulatória da ANPD para 2023/2024 (atualmente está em discussão pública e a agenda ainda não foi publicada).

Muito embora não existam projetos de lei ou leis que proíbam a prática do reconhecimento facial, pode-se aplicar, em casos concretos, as sanções e multas

administrativas previstas pela LGPD. Não obstante, é importante ressaltar as multas administrativas previstas pela LGPD.

A violação à LGPD pode resultar na aplicação de sanções civis e administrativas. Isso significa que todos aqueles estão sujeitos às disposições da LGPD, caso a descumpram, estarão sujeitos às suas penalidades. No atual momento, em que a ANPD ainda é recente, o objetivo não é aplicar multa a todos que, de certa forma, não tratam dados pessoais em conformidade com a lei. O objetivo, por outro lado, é conscientizar a sociedade brasileira sobre a importância de se ter uma legislação específica sobre dados pessoais, a fim de protegê-los nas relações humanas. Enquanto na Europa esse tema já está consolidado, no Brasil, ainda existe um longo percurso para que os agentes de tratamento e os titulares de dados pessoais possam compreender a importância dos dados pessoais como parte de sua singularidade.

Sendo assim, a Autoridade Nacional de Proteção de Dados Pessoais pode aplicar as sanções administrativas dispostas no artigo 52 da LGPD, tais como (a) advertências; (b) multas de até 2% (dois por cento) do faturamento da empresa, grupo ou conglomerado no Brasil, limitadas a R\$50.000.000,00 por infração; (c) multas diárias, observado o mesmo limite de R\$ 50.000.000,00; (d) publicitação da infração; (e) bloqueio dos dados pessoais ao qual a ofensa se refere; (f) eliminação dos dados pessoais a que se refere a infração; (g) suspensão parcial do funcionamento do banco de dados pessoais a que se refere a infração por até 6 (seis) meses, prorrogável pelo mesmo período; (h) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração por até seis meses; e (i) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Órgãos e entidades administrativas (como Procon e Senacon) podem investigar a violação à LGPD, bem como impor sanções previstas no Código de Defesa do Consumidor ou no Marco Civil da Internet (se os dados foram obtidos online), tais como multa (já tivemos experiência de multa aplicada no valor de R\$10.000.000,00), suspensão de atividade, entre outras.

O Ministério Público também tem sido ativo na defesa de proteção de dados pessoais, através de processos administrativos que podem resultar em termos de ajustamento de conduta ou propositura de ação civil pública. No âmbito judicial, entidades governamentais e privadas (tais, como associações de defesa de proteção de dados), bem como indivíduos podem propor ação judicial por violação à LGPD,

requerendo a cessação da conduta, bem como pagamento de indenização por danos morais e materiais.

4.2. EFETIVA PROTEÇÃO DOS DIREITOS FUNDAMENTAIS PREVISTOS PELO PELO ART. 5º, X E LXII, DA CONSTITUIÇÃO FEDERAL DO BRASIL DE 1988, DIANTE DA PRÁTICA DO RECONHECIMENTO FACIAL E VIGILÂNCIA EM MASSA

A partir das noções gerais estampadas acima sobre a prática do reconhecimento facial, passa-se agora para o estudo e análise de casos práticos que aconteceram no Brasil sobre a temática. É interessante analisar que, apesar de as decisões e discussões a respeito dos incidentes não terem sido especialmente voltadas para a LGPD, os argumentos construídos a partir de outras legislações, como o Código de Defesa do Consumidor, também falam em liberdades individuais e em consciência do titular a respeito da coleta de dados pessoais sensíveis.

Os casos analisados a seguir serão dois. O primeiro é específico sobre o caso da Loja Hering do Shopping Morumbi, que instalou câmeras para capturar as imagens de consumidores e, assim, identificar o gênero do consumidor, bem como o seu perfil consumerista, sem o prévio conhecimento dos consumidores. A análise deste caso será pautada, principalmente, a partir da manifestação do IDEC sobre o reconhecimento facial utilizado pela Loja Hering e os argumentos traçados para defender a ilegalidade do incidente.

Já o segundo caso analisado será sobre o uso do reconhecimento facial por um serviço público acessado por milhares de brasileiros diariamente – o caso da ViaQuatro do metrô de São Paulo que instalou painéis de reconhecimento facial para analisar o perfil dos brasileiros. Este caso será particularmente analisado a partir da decisão proferida pelo Tribunal de Justiça do Estado de São Paulo e pelos argumentos trazidos na decisão para declarar o ato da ViaQuatro como ilegal. Passemos agora para a análise dos casos citados:

I. Loja Hering – Shopping Morumbi

O primeiro caso discutido será o relacionado ao uso do reconhecimento facial pela Loja Hering do Shopping Morumbi. Atenta à utilização de novas tecnologias para

o tratamento de dados pessoais de consumidores, a Secretaria Nacional do Consumidor (“SENACON”) aplicou penalidade de R\$ 58.767,00 (cinquenta e oito mil, setecentos e sessenta e sete reais) à Cia Hering, por ter utilizado reconhecimento facial em sua loja localizada no Shopping Morumbi, em São Paulo, sem o prévio conhecimento dos titulares de dados pessoais que frequentavam o local.

A atuação da SENACON vem, primeiramente, de uma denúncia feita pelo Instituto Brasileiro de Defesa ao Consumidor (“IDEC”). Diante disso, a SENACON entendeu que houve prática abusiva do dever de informação e de direitos de personalidade dos cidadãos, já que houve captação de reações dos consumidores para a finalidade de marketing e de melhoria de compra dentro do estabelecimento, porém sem o prévio consentimento destes.

Por mais que a Loja Hering tenha eliminado os registros de dados pessoais que captou de seus clientes posteriormente, a SENACON entendeu que a condenação deveria ser mantida em razão da falta de comunicação aos titulares sobre o tratamento que foi realizado. Não obstante, o valor da multa aplicada considerou a primariedade da Loja Hering em desrespeitar a legislação de proteção de dados e de defesa dos consumidores, além de ter cessado a prática como forma de minimizar os efeitos.

O IDEC, em sua manifestação escrita em 13 de maio de 2020, expôs os argumentos à SENACON para comprovar os fatos já alegados. Tal manifestação demonstra o ocorrido e como de fato essa prática violaria os dados pessoais dos consumidores que adentrassem na Loja Hering para realizar compras.

Afirma o IDEC que *“O emprego de tecnologia de reconhecimento facial tem se intensificado ao redor do mundo, trazendo consigo grandes investidas para sua regulação, com estabelecimento de parâmetros para um uso adequado, ou até mesmo através de moratórias ou banimentos. A preocupação decorre dos graves riscos às liberdades civis e direitos fundamentais, uma vez que a tecnologia utiliza dados sensíveis dos indivíduos analisados, podendo servir como ferramenta de controle e ocasionar práticas abusivas, discriminações e incidentes de vazamentos.”*

Nesse sentido, o caso da Hering se destaca pelo impacto causado à esfera íntima do consumidor, com a utilização de tecnologias classificadas como “invasivas”, capazes de detectar gênero, faixa etária, emoção e movimentação dentro do estabelecimento, sem nenhum tipo de aviso ao consumidor.

Para enfatizar a sua manifestação, o IDEC trouxe também bases constitucionais que serão abordadas nessa Monografia, conforme a seguir. Afirmou o IDEC que, no

Brasil, não há dúvidas de que a proteção de dados pessoais é um direito decorrente do direito constitucional à vida privada e intimidade, conforme definido pela CRFB/88 em seu art. 5º, X, como já tanto abordado.

Em decisão recente do STF (a respeito da autorização de compartilhamento de dados pessoais de consumidores de serviço de telefonia com o IBGE para fins de produções estatísticas) houve defesa desse entendimento. Em sua decisão liminar, a Min. Relatora Rosa Weber reforçou que

[...] Relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). (BRASIL, 2020).

A relatora enfatizou que é necessário ter respeito aos preceitos fundamentais das liberdades dos indivíduos. O Min. Gilmar Mendes, em seu voto, afirmou que diante da evolução do conceito de privacidade e de novas tecnologias deve-se ter um cuidado maior. Constatou o Ministro que

O direito fundamental à igualdade – enquanto núcleo de qualquer ordem constitucional – é submetido a graves riscos diante da evolução tecnológica. A elevada concentração de coleta, tratamento e análise de dados possibilita que governos e empresas utilizem algoritmos e ferramentas de data analytics, que promovem classificações e estereotipações discriminatórias de grupos sociais para a tomada de decisões estratégicas para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por vieses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham. (BRASIL, 2020).

A manifestação do IDEC ainda ressalta que para obtenção da análise almejada, ou seja, o perfil consumerista de certo indivíduo a partir de seu gênero, faixa etária e emoções, há necessária coleta de imagem, bem como sua utilização, acesso, processamento, modificação e eliminação. Todos esses processos são definidos como tratamento de dados pessoais, segundo a LGPD e são necessários para o funcionamento do reconhecimento facial isto é “*captura da imagem, detecção facial, normalização da imagem, extração de atributos e, por fim, seu descarte.*”

Nesse sentido, a imagem dos indivíduos analisados pelo reconhecimento facial é um dado pessoal sensível e a posterior eliminação da imagem e anonimização das informações extraídas não imuniza a empresa e tampouco apaga o tratamento de dados pessoais já realizado.

A manifestação também aborda a violação do direito de informação e à necessidade de consentimento. O consumidor é parte vulnerável na relação de consumo e se sujeita aos riscos de ter ferida a sua autonomia quanto à possibilidade de discriminação no mercado de consumo. Isso acontece por meio de atividades de tratamento de dados que ocorrem com suas informações pessoais por tecnologias as quais muitas vezes o consumidor sequer é capaz de entender plenamente. Nesse sentido, diante da ampla vulnerabilidade técnica, o consumidor pode ser tido como hipervulnerável.

O direito do consumidor à proteção de dados visa justamente tutelar essa hipervulnerabilidade, envolvendo, conforme ensina Laura Schertel Mendes, uma dupla dimensão:

(i) a tutela da personalidade do consumidor contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais; e (ii) a atribuição ao consumidor da garantia de controlar o seu fluxo de dados na sociedade. (2014, p. 203).

O consentimento, nesse sentido, é o elemento que garante ao consumidor a retomada da sua autonomia, por meio do controle sobre o fluxo de suas informações. Analisando a situação à luz dos conceitos de privacidade e proteção de dados pessoais, pode-se afirmar que a Hering, ao não informar os consumidores (titulares de dados pessoais) sobre o uso de suas expressões para delinear perfis consumeristas, violou a LGPD. Conforme dispõe o art. 6º, da LGPD, o tratamento de dados pessoais deve adotar como princípio a finalidade, necessidade, transparência, dentre outros princípios enumerados pela lei.

Fica claro que a Hering utilizou a prática de reconhecimento facial com o objetivo de traçar o perfil do consumidor e induzi-lo a compras que estejam de acordo com o seu gosto. Todavia, ao fazer isso, a Hering violou os princípios da necessidade e transparência, uma vez que não deixou claro aos consumidores que suas imagens eram usadas para tal finalidade. Além disso, a loja Hering poderia ter adotado outros

métodos para alcançar os mesmos objetivos, como, por exemplo, uma enquete em seu site ou algo similar.

Não obstante, o uso da biometria, conforme dispõe a LGPD, é tratado como dado pessoal sensível, o que exige a aplicação de outras bases legais, diferentes daquelas expostas pelo art. 7º, para justificar o seu tratamento. De acordo com o art. 11 da LGPD, a base legal que mais se aplicaria ao caso concreto seria de fato o consentimento.

Em suma, resta claro que a Hering ofendeu valores fundamentais resguardados pela CRFB/88 e pelas legislações infraconstitucionais ao não informar seus consumidores sobre a extração e análise de seus dados, sem dar-lhes oportunidade de escolha. Não houve informação transparente e clara ao consumidor, assim como seu devido e expresso consentimento.

Desse modo, a empresa violou a privacidade de seus consumidores e incorreu em abuso de direito, com violação aos direitos de informação e de escolha. Há expressa violação de direitos básicos do consumidor, garantidos pelo artigo 5º, X, da CRFB/88, estes sendo intimidade, vida privada e a imagem. Também violou direitos expressos no Código de Defesa do Consumidor como segurança (art. 6º, inc. I), o direito à liberdade de escolha (art. 6º, inc. II), o direito à informação adequada e clara sobre os serviços prestados pela loja (art. 6º, inc. III) e o direito a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais (Lei nº. 12.965/2014 - Marco Civil da Internet - art. 7º, inc VIII).

Por fim, houve violação direta LGPD por não ser transparente com os seus consumidores no tocante ao tratamento de seus dados pessoais, além de não ter dado a eles a opção de consentir com o tratamento realizado.

Observa-se, com base no acima exposto sobre o caso da loja Hering, que o avanço das tecnologias está sendo observado pelas entidades reguladoras de maneira a proteger os consumidores finais, que nada mais são do que os próprios titulares dos dados pessoais coletados e tratados a seu respeito. A manifestação do IDEC foi assertiva quanto a falta de transparência e de conscientização dada aos frequentadores da loja sobre o uso de seus dados pessoais. O direito de escolha e de consentimento, no caso em tela, era essencial, e, uma vez não cumprido, deve ser sancionado.

II. Concessionária Da Linha 4 Do Metrô De São Paulo S.A. (Via Quatro)

Um outro caso emblemático que envolve a utilização de reconhecimento facial, sem a devida coleta de consentimento dos passageiros, foi o da Linha 4 do metrô de São Paulo. A ViaQuatro, que detém a concessão da linha 4-amarela do metrô de São Paulo, acabou sendo condenada a pagar R\$100.000,00 (cem mil reais) pela captação de imagens pela prática do reconhecimento facial dos passageiros, sem a coleta de consentimento. A sentença do Tribunal de Justiça do Estado de São Paulo (“TJSP”), por sua vez, responde a uma ação civil pública do IDEC, a qual foi movida contra a empresa detentora da linha 4 do metrô no ano de 2018.

Em abril de 2018 a ViaQuatro informou que instalou “portas de plataforma interativas” em diversas estações como a Luz, Paulista e Pinheiros. Tais portas interativas tinham lentes com um sensor que era capaz de reconhecer a presença humana e identificar a quantidade de pessoas que passavam e olhavam para aquela tela. Conforme indicou a ViaQuatro, o sistema captava expressões de emoções (raiva, alegria, neutralidade) e algumas características gerais que podiam indicar se o rosto do passageiro era feminino ou masculino.

Na ação civil pública movida pelo IDEC, houve argumentação de que o sistema promovido pela ViaQuatro era ilegal, pois não havia coleta de consentimento dos passageiros e de que a imagem é um direito garantido constitucionalmente. Na Justiça, todavia, a ViaQuatro argumentou que as câmeras apenas detectavam as imagens para finalidades estatísticas e que aqueles dados não eram utilizados para vinculação a nenhuma identidade e que muito menos havia armazenamento desses dados pessoais coletados.

A leitura da sentença sobre o tema, proferida em 7 de maio de 2021, pela Juíza Dra. Patrícia Martins Conceição, expõe que na ação civil pública proposta pelo IDEC havia pretensão a condenação da ViaQuatro (i) a não utilizar os dados biométricos ou qualquer outro tipo de identificação dos consumidores e usuários do transporte público, sem o consentimento do usuário do transporte público; (ii) ao pagamento de indenização pela utilização indevida da imagem dos consumidores; e (iii) indenização por danos coletivos em valor não inferior a R\$ 100.000.000,00. A ré, por sua vez, defendia a legalidade da utilização do equipamento, já que não há coleta ou armazenamento de dados pessoais no sistema, mas tão somente de detecção facial para finalidades estatísticas.

A Juíza, todavia, pontuou que a limitação do sistema em apenas utilizar as imagens dos usuários para fins estatísticos, sem que existisse identificação específica não restou comprovada nos autos. Diante do fato incontroverso de que existia um equipamento de gravação de imagem dos usuários do metrô para fins publicitários e estatísticos, cabia à ré, como concessionária de serviços públicos, demonstrar que o sistema, de fato, não armazenava dados pessoais dos usuários que trafegavam pelo metrô e, tampouco, realizava a prática do reconhecimento facial. Todavia, tal comprovação não foi realizada pela ViaQuatro.

Nesse sentido, a Juíza afirmou que *“sem que tenha havido interesse da ré em demonstrar concretamente neste feito a real destinação dada às informações inequivocamente coletadas pela empresa detentora dos equipamentos instaladas nas dependências das estações administradas, conclui-se não ter havido demonstração de fato impeditivo ou extintivo do direito demonstrado pelo autor. E ainda que se constatasse concretamente a ausência de efetivo reconhecimento facial pelo equipamento instalado, não há dúvidas de que há captação da imagem de usuários, sem o seu conhecimento ou consentimento para fins comerciais que beneficiam a ré e a empresa por ela contratada.”*

Dessa forma, fica claro que, na sentença, a prática do reconhecimento facial foi constatada e atestou-se que os painéis digitais detectavam informações como gênero, faixa etária, reação à publicidade veiculada no mesmo equipamento, entre outros. De toda forma, apesar de a LGPD ser posterior ao início do reconhecimento facial apresentado nos autos, a decisão proferida pela Juíza tomou como base diversos artigos da referida lei, como será demonstrado a seguir.

O reconhecimento facial, ou até mesmo a detecção facial, sem o devido consentimento dos usuários, já violaria a LGPD. Reforça a Juíza do presente caso que somente na hipótese de consentimento claro e específico do titular, ou sem o consentimento do titular, nas situações elencadas no rol do inciso II do art. 11 da LGPD que a coleta e tratamento dos dados pessoais seria válida. Entretanto, a Juíza entendeu que nenhuma das outras hipóteses de bases legais estampadas pelo art. 11 da LGPD se aplicaria ao caso concreto, ou seja, realmente seria necessária a coleta do consentimento dos usuários para a continuidade da utilização dos painéis interativos.

A decisão também ressalta que a finalidade do tratamento deveria ter tido propósitos legítimos, explícitos e informados ao titular de dados, sem possibilidade de

tratamento posterior de forma incompatível com essas finalidades, conforme expõe o art. 6º, I, da LGPD. Neste cenário, a situação deste caso concreto é diferente da captação de imagens dos passageiros para sistemas de segurança com o objetivo de, por exemplo, melhorar a segurança dos usuários ou manutenção da ordem, o que são fatores necessários já que a ViaQuatro é uma prestadora de serviços públicos.

Todavia, o que ficou comprovado pela sentença proferida pelo TJSP é que a captação de imagens estava sendo utilizada para fins publicitários e, conseqüentemente, de cunho comercial, uma vez que buscava alcançar as principais características dos indivíduos e suas emoções em reação às publicidades dos painéis. A conduta da ViaQuatro, nesse sentido, violou também o direito à imagem dos consumidores usuários do serviço público, as disposições sobre a proteção dos dados pessoais sensíveis e o direito à informação e proteção às práticas abusivas de mercado.

A ViaQuatro, por ser prestadora de serviços públicos, tinha igualmente o dever de alertar os usuários sobre a coleta e tratamento de seus dados pessoais, em especial, de seus dados pessoais sensíveis. A LGPD, como já expresso, alerta que toda atividade de tratamento com dados pessoais deve ser legítima, com uma finalidade adequada e com uma base legal que a justifique, sem mencionar, também, o quesito da transparência. Dessa forma, considerando que a base legal aplicável ao caso em tela seria o consentimento, o qual deve ser livre, inequívoco e informado, não poderia ter a ViaQuatro ignorado tal previsão legal. Dessa forma, a decisão proferida pelo TJSP foi assertiva nesse sentido.

5. CONSIDERAÇÕES FINAIS

As tecnologias avançadas já fazem parte do cotidiano do ser humano e isso é um senso comum – quase tudo o que se faz depende do uso, de alguma forma, de tecnologia. Como reiteradamente afirmado nesta Monografia, não há dúvidas de que não chegaríamos aonde chegamos sem a tecnologia presente em nossas vidas. Os meios tecnológicos facilitaram, expressivamente, a forma de viver e de se relacionar em uma sociedade mundialmente conectada. Por outro lado, não se pode permitir que as tecnologias passem a dominar a sociedade ou que terceiros se utilizem da tecnologia para vantagens indevidas, e tal entendimento não poderia ser diferente para a prática do reconhecimento facial, já que se trata de prática envolvendo tecnologia.

A Internet e os meios tecnológicos externos de comunicação, muitas vezes, não são capazes de garantir a privacidade e a intimidade de seus usuários por si só. Especificamente, no Brasil, todavia, a garantia à privacidade, à intimidade e vida privada são direitos constitucionalmente garantidos. Esses direitos, embora tenham conceitos diferentes, como abordado no primeiro capítulo desta Monografia, buscam, de maneira geral, a preservação da esfera interna de cada um dos indivíduos que faz parte de uma sociedade. Em meio a tantos relacionamentos e a tantas interações às quais estamos sujeitos, é mais do que legítimo e válido que possamos ter a esfera interna, que diz respeito a um ser em particular, protegida pela CRFB/88 e demais legislações. Nossos pensamentos, vontades, desejos e relações fazem parte do que nos compõe como pessoas e essas são características que jamais podem ser tiradas ou violadas pelo uso abusivo da tecnologia.

Nesse cenário, a proteção aos dados pessoais também ganha extrema relevância na medida em que tais dados são exclusivos de um indivíduo apenas. Pessoas podem ter nomes iguais ou podem ter as mesmas datas de nascimento, mas a partir do momento que esses dados são agregados a outras informações, forma-se um perfil único e não comparável. Os direitos de personalidade, nesse sentido, buscam proteger a forma única e interna de cada uma das pessoas.

O usufruto das tecnologias e, especialmente, a prática do reconhecimento facial, não pode, portanto, violar esses direitos constitucionalmente garantidos. Certamente, o uso do reconhecimento facial para fins criminais e investigatórios é extremamente benéfico, mas a utilização desse controle de maneira desenfreada, sem a devida

garantia dos direitos de personalidade, principalmente da privacidade e intimidade, e da proteção aos dados pessoais, ultrapassa as barreiras impostas pela CRFB/88 e pelas legislações infraconstitucionais, em especial, a LGPD.

Pelo fato de o reconhecimento facial utilizar dados biométricos, que é um tipo de dado pessoal sensível, conforme expresso pela LGPD, não é possível tratar desse assunto sem adentrar nos principais tópicos abordados pela LGPD. De acordo com a lei, todo tratamento de dado pessoal pode ser legítimo, desde que respeitados os princípios estampados pela lei e desde que atendidas as finalidades pelas quais os dados pessoais tenham sido coletados em primeiro lugar. Não obstante, fato importante a ser considerado é a atribuição de bases legais para justificar os diversos tipos de tratamento com dados pessoais.

A partir dos dois casos concretos referentes a utilização do reconhecimento facial pela Loja Hering, para traçar o perfil de consumidor de seus clientes, e pelo metrô da linha 4 de São Paulo, para fins de marketing, pode-se observar que os requisitos de cumprimento à lei, no tocante à coleta de consentimento dos usuários e de transparência, não foram cumpridos. Com a falta desses elementos, os usuários tiveram sua privacidade e intimidade violadas, uma vez que não tiveram a opção de consentir com os tratamentos realizados, ou seja, não tiveram opção de escolha de negar o uso de seus dados pessoais para as finalidades de cada entidade.

Resta claro, portanto, que os meios tecnológicos e as práticas de reconhecimento facial continuarão em nossos cotidianos, independentemente de nossas vontades particulares. A grande questão é a conscientização, particularmente, no Brasil, de que existem direitos fundamentais e proteções à intimidade, à privacidade e aos dados pessoais e que esses direitos não devem ser violados em prol de marketing ou de serviços públicos, sem que exista uma finalidade legítima para esses tratamentos e sem que haja uma base legal adequada para justificar essas práticas.

Nesse sentido, entende-se que a prática do reconhecimento facial, quando não vislumbrar os direitos fundamentais de personalidade e não respeitar os dispositivos legais aplicáveis, não será válida. O aspecto íntimo de cada ser humano deve ser protegido acima de qualquer meio tecnológico, de maneira a fazer zelar pela prevalência dos direitos e garantias atribuíveis aos brasileiros.

BIBLIOGRAFIA

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 maio 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/l13709.htm. Acesso em: 17 maio 2023.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6387/DF – Distrito Federal. Relatora: Ministra Rosa Weber. *Medida Cautelar de Urgência*, 24 abril 2020. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf>. Acesso em: 17 maio 2023.

CARVALHO, Ana Paula Gambogi. O consumidor e o direito à autodeterminação informacional: considerações sobre os bancos de dados eletrônicos. *In: MARQUES, Claudia Lima. Revista de Direitos do Consumidor*, São Paulo: Editora Revista dos Tribunais, n. 46, 2003, p. 77.

CUPIS, Adriano de. *Os direitos da personalidade*. Tradução Afonso Celso Furtado Rezende. Campinas: Romana, 2004, p. 17-24.

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro: responsabilidade civil*. 25 ed. São Paulo: Saraiva, 2011, p. 90.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do estado. *Revista da Faculdade de Direito*, Universidade de São Paulo, São Paulo, v. 88, p. 439-459, 01 jan. 1993.

FERREIRA FILHO, Manoel Gonçalves. *Comentários à Constituição Brasileira de 1988*, 2. ed. São Paulo: Saraiva, 1997, p. 35.

MENDES, Gilmar Ferreira. *Curso de Direito Constitucional*. 13 ed. São Paulo: Saraiva Educação, 2018.

MENDES, Gilmar Ferreira. *Curso de Direito Constitucional*. São Paulo: Saraiva, 2008.

MENDES, Laura Schertel. *Privacidade, Proteção de Dados e Defesa do Consumidor: linhas gerais de um novo direito fundamental*. São José dos Campos: Saraiva Jur, 2014, p. 203.

MORAES, Alexandre de. *Constituição do Brasil Interpretada*. 5 ed. São Paulo: Atlas, 2011.

SAMPAIO, José Adércio de Leite. *Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte*. Belo Horizonte: Del Rey, 1988, p. 240.

SILVA, José Afonso da. *Comentário Contextual à Constituição*. 9 ed. São Paulo: Malheiros, 2011.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 8 ed. São Paulo: Malheiros Editores, 1992, p. 188-205.