UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS (FCHS)
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

MARINA CAVALLI RIBEIRO DA SILVA

A COLETA DE DADOS BIOMÉTRICOS E A VIOLAÇÃO DO DIREITO FUNDAMENTAL À PRIVACIDADE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

FRANCA
2023

MARINA CAVALLI RIBEIRO DA SILVA

A COLETA DE DADOS BIOMÉTRICOS E A VIOLAÇÃO DO DIREITO FUNDAMENTAL À PRIVACIDADE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Faculdade de Ciências Humanas e Sociais da Universidade Estadual Paulista "Júlio de Mesquita Filho", como pré-requisito para a obtenção do título de Mestre em Direito. Área de concentração: Tutela e efetividade dos direitos de Cidadania.
Orientadora: Profa. Dra. Luciana Lopes Canavez.

FRANCA
2023

S586c

Silva, Marina Cavalli Ribeiro da

A coleta de dados biométricos e a violação do direito fundamental à privacidade à luz da Lei Geral de Proteção de Dados Pessoais / Marina Cavalli Ribeiro da Silva. -- Franca, 2023

130 p.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências Humanas e Sociais, Franca

Orientadora: Luciana Lopes Canavez

1. Direitos fundamentais. 2. Direito a privacidade. 3. Proteção de Dados. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências Humanas e Sociais, Franca. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

IMPACTO POTENCIAL DESTA PESQUISA

O trabalho promove a pesquisa científica na área da inovação ao refletir sobre os impactos das tecnologias e propor mecanismos para a melhoria das capacidades tecnológicas, a fim de que não violem direitos fundamentais e sociais. A pesquisa também incentiva a atuação conjunta e transparente das instituições e fornece ao público informações sobre como proteger seus direitos e exercê-los de forma autônoma.

POTENTIAL IMPACT OF THIS RESEARCH

This work promotes scientific research in the area of innovation by reflecting on the impacts of technologies and proposing mechanisms for improving technological capabilities, so that they don’t violate fundamental and social rights. This survey encourages the transparent and joint action by institutions and provides the public with information of how to protect their rights and how to exercise them autonomously.

MARINA CAVALLI RIBEIRO DA SILVA

A COLETA DE DADOS BIOMÉTRICOS E A VIOLAÇÃO DO DIREITO FUNDAMENTAL À PRIVACIDADE À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Dissertação de Mestrado em Direito apresentada à Faculdade de Ciências Humanas e Sociais da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Franca, Programa de Pós-Graduação em Direito Strictu Sensu, como pré-requisito para a obtenção do título de Mestre em Direito. Área de concentração: Tutela e efetividade dos direitos de Cidadania.

BANCA EXAMINADORA

_____

Presidente: Profa. Dra. Luciana Lopes Canavez

_____

1º Examinador: Victor Hugo Almeida

_____

2º Examinador: Eduardo Tomasevicius Filho

Franca/SP

2023

Gostaria de dedicar este trabalho ao Sr. Danilo Doneda (*in memorian*) que, desde o início dessa pesquisa, foi uma inspiração para mim. Infelizmente, não tive a oportunidade de conhecê-lo pessoalmente. O jurista Danilo Doneda será sempre uma referência na área de proteção de dados pessoais e de privacidade.

AGRADECIMENTOS

Ter a oportunidade de retornar à UNESP para cursar o mestrado foi uma experiência muito gratificante para mim, além de imensamente motivadora. Me instiga poder escrever sobre um tema tão novo e que, hoje, move inúmeros debates na área jurídica.

Com essa pesquisa, acredito que poderei contribuir com o conhecimento científico na área, bem como propor soluções para os desafios do tema na prática.

Deste que me propus a cursar o mestrado, tive em mente que não gostaria de deixar minha pesquisa apenas na parte teórica. Eu sempre quis ir além: quis questionar, analisar, criticar. Por essa razão, busquei efetuar uma análise de caso, bem como estudar documentos (Política de Privacidade). Assim, eu poderia aplicar tudo aquilo que estudei e refletir como, na prática, esses ensinamentos na área de privacidade e de proteção de dados pessoais tem sido aplicado.

Dito isso, aproveito essa oportunidade para agradecer todos aqueles que me apoiaram nessa caminhada.

Em primeiro lugar, agradeço aos meus pais, pois estes, desde o início, me incentivaram a me inscrever no processo seletivo e sempre me apoiaram em cada atividade na qual eu me propunha a participar durante esses dois anos. Também agradeço às minhas tias Silvana e Carol, duas professoras incríveis e que muito me inspiram!

Agradeço, ainda, às minhas grandes amigas e "veteranas" de mestrado, Maria Júlia e Cinthia, que sempre colaboraram comigo. Elas não só me ajudaram e me deram total suporte nessa caminhada, quanto me permitiram trocar experiências e diversos conhecimentos.

Além disso, agradeço aos meus colegas de pesquisa e que se tornaram amigos de uma vida: Isadora Beatriz, Maria Eduarda, Mariana e André. Desde antes do início das aulas, logo no processo seletivo, sempre nos apoiamos e compartilhamos dúvidas, aprendizados, dicas. Durante os dois anos de mestrado, essa aproximação foi ainda maior. A participação deles foi fundamental a tudo que vivi. É curioso que eu e a Isadora nunca nos encontramos presencialmente, mas nossa conexão no mestrado foi tamanha, que parecia que éramos amigas há muito tempo. A Dudinha também foi um presente. Sou muito grata por sua amizade e por tudo o que vivemos juntas nesses últimos anos.

Também deixo meu carinho especial por toda a "torcida" que esteve presente nas minhas bancas de qualificação e de defesa, me enviando boas energias: Júlia, Juliana, Carol, Helena, Duda Leonel, Ana Felizardo, Tauana, Luiza, Mariana, Julie, Isadora, Maria Júlia, Camila M., Bruna, Camila S., Duda Léo, Bianca, Luis, Ianca, Marília, Anita e Thauana.

Agradeço a outro veterano que esteve presente desde a minha primeira pesquisa, na época do TCC: João Victor. Obrigada por sempre estar disposto a conversar comigo e a compartilhar seu aprendizado.

Aos demais amigos “da vida”, espalhados por Ribeirão, São Paulo, Piracicaba que me acompanharam nessa rotina, mesmo que só ouvindo eu contar sobre o mestrado, meu muito obrigada! Agradeço por torcerem por mim, e por me incentivarem sempre a dar meu melhor.

Também deixo meu agradecimento especial à professora Luciana, que sempre me incentivou muito no estudo do tema, sendo que este foi algo novo na área de pesquisa da UNESP Franca. Com seu apoio e confiança, sempre estive muito motivada a pesquisar, escrever e a buscar compreender cada vez mais o assunto, a fim de realizar uma pesquisa bastante completa.

Ademais, gostaria de agradecer aos examinadores Victor Hugo e Eduardo que, na minha banca de qualificação, fizeram considerações de suma importância e que colaboraram sobremaneira com os rumos do meu trabalho. Os comentários realizados no momento de qualificação foram essenciais para meu progresso. Foram eles quem me ajudaram a perceber qual seria o melhor caminho a tomar, o que era importante observar, de maneira que fiquei ainda mais motivada a aprofundar meus estudos.

Agradeço, ainda, ao Nailton por todo o suporte fornecido. Sempre foi muito prestativo comigo e sempre esteve disponível para sanar minhas dúvidas.

Por fim, deixo meu agradecimento à instituição UNESP- Franca, que, além da pós-graduação, também fez parte da minha graduação. Foi a UNESP quem me aproximou da área de pesquisa e me abriu portas incríveis, nas quais pude participar de diferentes projetos, grupos de extensão, os quais contribuíram não apenas com a minha formação acadêmica e profissional, mas também pessoal. Agradeço também todos os professores que tive o prazer de conhecer ou de reencontrar nessa etapa.

Finalizo deixando, de modo geral, minha gratidão a todos aqueles que participaram desse meu caminho, me apoiando, me orientando e me incentivando a construir essa pesquisa no mestrado e, principalmente, a ir atrás daquilo que, internamente, eu mais me identificava.

SILVA, Marina Cavalli Ribeiro da. **A coleta de dados biométricos e a violação do direito fundamental à privacidade à luz da Lei Geral de Proteção de Dados Pessoais**. 2023. 129 f. Dissertação (Mestrado em Direito) – Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista, Franca, 2023.

RESUMO

O conteúdo do direito à privacidade, objeto deste estudo, se modificou ao longo do tempo, de acordo com o contexto em que foi aplicado. Inicialmente, possuía um caráter fortemente individualista, atrelado à proteção da esfera individual de interferências alheias. No ordenamento jurídico brasileiro, este direito é protegido na Constituição Federal e em inúmeros instrumentos infraconstitucionais, dentre os quais se destaca o Código Civil. O desenvolvimento das tecnologias de informação e de comunicação no século XX, aliados ao aperfeiçoamento da internet, trouxeram novos desafios ao direito, sobretudo no âmbito dos direitos da personalidade, onde nos deparamos com a consolidação de um novo ramo do direito à privacidade: o direito a ter controle sobre as próprias informações e dados pessoais. Isto porque a aceleração tecnológica teve como um de seus elementos o tratamento de dados pessoais, os quais, por sua vez, correspondem a informações que servem para identificar o titular a que se referem, permitindo a descoberta de seus interesses, comportamentos, entre outras características. Por constituírem uma representação da personalidade do indivíduo, é primordial que sejam amparados pelo direito, com o intuito de que este continue defendendo seu valor fundamental: a dignidade da pessoa humana. Essa proteção, no Brasil, é primordialmente realizada pela Lei nº 13.709/2018- Lei Geral de Proteção de Dados Pessoais), e incide na relação entre particulares, diante da eficácia horizontal dos direitos fundamentais. Neste contexto, o objetivo deste trabalho é compreender em que medida o tratamento de dados pessoais por particulares pode resultar em uma violação ao direito à privacidade, em sentido amplo, tanto na perspectiva infraconstitucional, quanto constitucional. O foco da presente pesquisa será no estudo do tratamento de dados pessoais sensíveis por particulares, especificamente o uso de tecnologias biométricas, como o reconhecimento facial, para atender interesses particulares. A metodologia empregada neste trabalho consistirá, quanto ao método de procedimento, na pesquisa bibliográfica em materiais que tratem do tema, bem como na pesquisa documental tendo como objeto de estudo a Política de Privacidade da empresa Via Quatro. Pretende-se, ainda, fazer uma análise de um caso concreto relevante envolvendo o Instituto Brasileiro de Defesa do Consumidor e a Concessionária da Linha 4 do Metrô de São Paulo (Via Quatro), ainda em trâmite no Tribunal de Justiça de São Paulo, cuja discussão central envolve a coleta de dados biométricos voltada para fins publicitários. Quanto ao método de abordagem, será empregado o dedutivo na pesquisa bibliográfica, e o indutivo na documental e no estudo de caso. Confirmando sua hipótese inicial, o trabalho demonstra a necessidade de instituição de instrumentos jurídicos específicos de proteção de dados pessoais, ampliando a noção de uma tutela jurídica pautada exclusivamente no direito à privacidade.

Palavras-chave: direito à privacidade. proteção de dados pessoais. sociedade da informação. direitos fundamentais.

ABSTRACT

The content of the right to privacy, object of this study, has changed over time, according to the context in which it was applied. Initially, it had a strongly individualistic character, linked to the protection of the individual sphere from outside interference. In the Brazilian legal system, this right is protected in the Federal Constitution and in numerous infra-constitutional instruments, among which the Civil Code stands out. The development of information and of communication technologies in the 20th century, combined with the improvement of the internet, brought new challenges to the law, especially in the context of personality rights, where we are faced with the consolidation of a new branch of the right to privacy: the right to have control over their personal information and data. This is because technological acceleration has as one of its elements the processing of personal data, which, in turn, corresponds to information that serves to identify the data subject to which they refer, allowing the discovery of their interests, behaviors, among other characteristics. As they constitute a representation of the individual's personality, it is essential that they are supported by the law, with the aim that it continues to defend its fundamental value: the dignity of the human person. This protection, in Brazil, is primarily carried out by Law No. In this context, the objective of this work is to understand to what extent the processing of personal data by individuals can result in a violation of the right to privacy, in a broad sense, both in the infra-constitutional and constitutional perspectives. The focus of the present research will be on the study of the treatment of sensitive personal data by individuals, specifically the use of biometric technologies, such as facial recognition, to meet particular interests. The methodology used in this work will consist, regarding the method of procedure, in the bibliographic research in materials that deal with the subject, as well as in the documental research having as object of study the Privacy Policy of the company Via Quatro. It is also intended to analyze a relevant concrete case involving the Brazilian Institute of Consumer Protection and the Concessionaire of Line 4 of the São Paulo Metro (Via Quatro), still pending in the São Paulo Court of Justice, whose discussion central involves the collection of biometric data for advertising purposes. As for the method of approach, the deductive method will be used in the bibliographic research, and the inductive method in the documentary and case study. Confirming yout initial hypothesis, the work demonstrates the need to establish specific legal instruments for the protection of personal data, expanding the notion of legal protection based exclusively on the right to privacy.

Keywords: right to privacy. personal data protection. information society. fundamental rights.

LISTA DE ABREVIATURAS E SIGLAS

ADI Ações Diretas de Inconstitucionalidade

Art. Artigo

ANPD Autoridade Nacional de Proteção de Dados

CC Código Civil

CDC Código de Defesa do Consumidor

CF Constituição Federal

GDPR General Data Protection Regulation

IA Inteligência Artificial

ICO Information Commissioner's Opinion

LGPD Lei Geral de Proteção de Dados Pessoais

MP Medida Provisória

Nº Número

P. Página

STJ Superior Tribunal de Justiça

STF Supremo Tribunal Federal

TJSP Tribunal de Justiça do Estado de São Paulo

SUMÁRIO

INTRODUÇÃO

Hodiernamente, em razão da evolução tecnológica e dos avanços da internet, descobrimos novas possibilidades de comunicação e de troca de conhecimento. Ocorre a formação do chamado espaço virtual, caracterizado pelo fluxo instantâneo de informações e pelo estabelecimento de relações sociais em rede, que possibilitam uma interconexão cada vez maior entre a sociedade.

Diante deste contexto, deparamo-nos com um fluxo cada vez maior de dados pessoais, os quais podem ser compreendidos como *"*qualquer informação relacionada a uma pessoa de forma que, se em conjunto ou isolada, tornem possível sua identificação" (MIRANDA, 2019, p. 12).

Esclarece-se que, embora o tratamento de dados pessoais não seja uma atividade que apenas surgiu nos tempos atuais, somente agora é que seus impactos foram sentidos de maneira mais intensa e ampla nos diversos aspectos da vida cotidiana. Dentre os instrumentos que colaboraram com esse aumento na intensidade e na forma de processar dados, destacamos o desenvolvimento de softwares e de algoritmos dotados de inteligência artificial, voltados para solucionar problemas cotidianos.

Nesta perspectiva, à medida em que a tecnologia digital se desenvolveu, a vulnerabilidade dos indivíduos, especialmente em relação à vida privada e à intimidade, também cresceu, o que resultou em novos desafios para os direitos humanos.

Isto porque, embora o ordenamento jurídico brasileiro contemple a privacidade como direito da personalidade fundamental, previsto no art. 5º da Constituição Federal, bem como no art. 21 do Código Civil, as noções tradicionais deste direito, baseado na lógica de Warren e Brandeis, no sentido de "ser deixado só", mostraram-se insuficientes e inadequadas para a proteção da pessoa humana, no âmbito do tratamento de seus dados pessoais, os quais demandam soluções diferenciadas.

Neste ínterim, nos deparamos com um conceito contemporâneo do direito à privacidade, correspondente ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações (RODOTÁ, 2008, p. 267).

A esse respeito, por representarem uma grande parte da personalidade da pessoa, os dados merecem tutela jurídica proativa, de modo a assegurar a liberdade, igualdade e a dignidade do indivíduo a que se referem.

A proteção de dados é, hoje, uma questão central de debate, tendo em vista que constitui um direito fundamental expressivo da condição humana contemporânea.[1] Em razão disso, é crucial a instituição de mecanismos que possibilitem ao titular deter conhecimento e controle sobre seus dados.

Como consequência deste cenário no Brasil, foi aprovada em agosto de 2018 a Lei Geral de Proteção de Dados Pessoais (LGPD), a qual tem intuito de disciplinar a gestão de dados pessoais, garantindo ao cidadão uma maior autonomia neste processo de tratamento. A Lei entrou em vigor em setembro de 2020.

Nos dias atuais, a maioria dos tratamentos de dados pessoais é realizada por atores privados, dotados de poder econômico, político e social, as quais atuam como controladores e operadores de dados pessoais (SARLET, 2021, p. 22). Nestas relações, nos deparamos com uma assimetria de poderes entre o titular dos dados e os agentes de tratamento.

Diante do quadro exposto, o presente trabalho tem o objetivo geral compreender em que medida o tratamento de dados pessoais por particulares pode resultar em uma violação ao direito à privacidade, em sentido amplo, tanto na perspectiva infraconstitucional, quanto constitucional.

Para atingir esta meta, a pesquisa conta com os seguintes objetivos específicos: (I) estudar a evolução histórica do Direito à privacidade no Brasil, em âmbito infraconstitucional e constitucional; (II) compreender como as mudanças tecnológicas contribuíram para o desenvolvimento da sociedade informacional e para a supervalorização dos dados pessoais; (III) verificar como se dá a tutela dos dados pessoais no Brasil, em âmbito infraconstitucional, tendo como principal objeto de estudo a Lei Geral de Proteção de Dados, e constitucional; (IV) analisar a aplicação do direito à privacidade e à proteção de dados pessoais nas relações entre particulares, por meio de um estudo de caso; e (V) explorar de forma crítica a política de privacidade da Via Quatro, a fim de aferir se seus termos são adequados para efetivação do direito à privacidade em sentido amplo.

O foco principal da pesquisa será nos dados pessoais biométricos, compreendidos como aqueles que identificam cada indivíduo com base em seus atributos físicos e comportamentais.

A esse respeito, cumpre esclarecer que, por serem dados que expressam uma vulnerabilidade de seu titular, os dados biométricos são considerados dados pessoais sensíveis.

[1] O STF já reconheceu a proteção de dados pessoais como um direito fundamental ao referendar a decisão liminar proferida pela ministra Rosa Weber no julgamento da ADI 6.387. No caso, em síntese, o plenário da Suprema Corte suspendeu a aplicabilidade da Medida Provisória nº 954/2020 e impediu o compartilhamento de dados pessoais dos usuários de telefonia entre as companhias de telefonia e o IBGE.

Ainda, nas palavras de Stefano Rodotá (2008, p. 96), estas informações possuem potencial inclinação para serem utilizadas com finalidades discriminatórias. Em razão disso, podem ocasionar riscos ainda maiores aos direitos fundamentais de seu titular (privacidade, honra, imagem e a própria proteção de dados), motivo pelo qual merecem um regime de proteção ainda mais rigoroso. Além disso, optou-se por estudar especificamente a coleta de dados biométricos por meio de tecnologias de reconhecimento facial.

Tendo em vista a distribuição das seções, inicialmente, pretende-se efetuar uma análise sobre o desenvolvimento do direito à privacidade, apresentando seu conceito, seu objeto, e como este direito é tutelado nos dias atuais, na perspectiva infraconstitucional e constitucional. Além disso, será feita uma breve explanação sobre a eficácia horizontal dos direitos fundamentais nas relações privadas, a fim de que, em um segundo momento, seja possível compreender como o direito à privacidade reflete nestas relações.

Já na segunda seção, pretende-se apresentar o contexto da sociedade tecnológica, bem como a maneira pela qual a informação e os dados pessoais se inserem nessa realidade, com o intuito de possibilitar ao leitor a compreensão do tema que será discutido. Serão apresentadas algumas noções relacionadas à temática, como “big data”, “algoritmo” e “tecnologias de reconhecimento facial”.

Na terceira seção, deseja-se estudar como o desenvolvimento do direito à privacidade e suas consequentes ramificações deu espaço para o surgimento do direito à proteção de dados pessoais, assim como analisar como este direito é tutelado na esfera infraconstitucional, tendo como foco a Lei Geral de Proteção de Dados Pessoais, e constitucional, a partir da análise de recente julgado do Supremo Tribunal Federal e da Proposta de Emenda Constitucional nº 17.

Já na quarta e penúltima seção, objetiva-se traçar um breve panorama acerca do caso envolvendo o sistema de Portas Digitais Interativas utilizado na linha 4 do metrô de São Paulo, o qual, a partir da captação de dados biométricos dos usuários, buscava analisar suas emoções e, com isso, direcionar as propagandas publicitárias. Tal projeto foi considerado por muitos operadores do direito como uma forma de violação de direitos fundamentais. Além disso, pretende-se discutir de forma crítica a problemática envolvida no caso - coleta de dados pessoais sensíveis para fins publicitários- à luz dos princípios da LGPD.

Finalmente, na última seção, será feita uma análise da Política de Privacidade disponibilizada no site da ViaQuatro, com o intuito de verificar se ela se mostra adequada às disposições da Lei Geral de Proteção de Dados Pessoais, bem como se ela estabelece soluções

eficazes para os problemas envolvendo a proteção de dados, como resposta à problemática analisada no estudo de caso.

Como a temática ainda é muito recente, o trabalho pretende realizar uma abordagem de caráter eminentemente exploratório, posto que busca promover descobertas por meio da investigação lógica e objetiva para o desenvolvimento de uma investigação mais ampla de uma temática que, hoje, ainda é pouco estudada. (GIL, 2008, p. 230). Assim, a pesquisa busca proporcionar aos leitores uma maior familiaridade com a temática abordada, com o intuito de deixá-la mais explícita.

O trabalho adota como referencial teórico sobre o tema dos direitos fundamentais autores como Ingo Wolfgang Sarlet, Daniel Sarmento, Gustavo Tepedino, Wilson Steinmetz. Por outro lado, no que tange à problemática envolvendo a proteção de dados, a pesquisa utiliza teóricos como Danilo Doneda, Bruno Ricardo Bioni, Laura Schertel Mendes, Stefano Rodotà.

A metodologia empregada neste trabalho consistirá, quanto ao método de procedimento, no levantamento bibliográfico de materiais especializados sobre a temática, e que já foram publicados, como doutrinas, artigos científicos, teses, dissertações, jurisprudência e legislação-com ênfase na Constituição Federal (BRASIL, 1988), no Código Civil (BRASIL, 2002) e na Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018)-, que possam contribuir para o delineamento da base teórica de estudo e para a concretização dos objetivos propostos.

Além disso, será utilizado o método de procedimento documental com vistas a efetuar uma análise de documento previamente selecionado pela pesquisadora, qual seja, a Política de Privacidade da empresa Via Quatro, disponível no site da concessionária. E, a partir da leitura atenta do documento, será possível propor deduções válidas sobre o objeto estudado.

Para que possa explorar o tema de forma prática, pretende-se, ainda, fazer uma pesquisa de estudo de relevante caso em trâmite no Tribunal de Justiça de São Paulo, que envolveu a coleta de dados biométricos por meio do sistema de Portas Interativas Digitais, instaladas na linha amarela do metrô de São Paulo. O estudo de caso tem o intuito de verificar a hipótese em que foi reconhecida a violação do direito à privacidade em razão do tratamento de dados pessoais.

Quanto ao método de abordagem, será empregado o dedutivo na análise dos materiais coletados, fazendo uma análise qualitativa, com o objetivo de, partindo de aspectos teóricos mais gerais dentro da temática do direito à privacidade no Brasil, se chegar a interpretações mais específicas que colaborem para a compreensão da problemática apresentada (MARCONI; LAKATOS, 2003, p. 91).

Ademais, se utilizará o método indutivo para se analisar o estudo de caso e para compreender a Política de Privacidade que é objeto deste estudo, a fim de, a partir de situações particulares, se buscar um panorama geral acerca de como se dá, na prática, a efetivação do direito à proteção de dados pessoais nas relações privadas.

Esclarece-se que, de forma geral, trata-se de um trabalho meta-analítico, pois, irá reunir pesquisas que já existem, a fim de que a pesquisadora possa desenvolver novas interpretações e, a partir delas, propor soluções jurídicas para questões que, na prática, tem desafiado a sociedade e a comunidade jurídica.

Isto porque, apesar de contarmos há anos com a tutela do direito à privacidade no âmbito constitucional e infraconstitucional, no momento atual, tal proteção se mostra insuficiente para lidar com as problemáticas contemporâneas e com os danos gerados pelo uso das novas tecnologias, motivo pelo qual sua noção deve ser aprofundada e atualizada.

O reconhecimento dos novos contornos do direito à privacidade irradia na relação entre particulares, nos termos da teoria eficácia horizontal dos direitos fundamentais, com o intuito de também proteger na esfera privada os riscos oriundos do tratamento de dados pessoais e, desta forma, assegurar a dignidade da pessoa humana e o livre desenvolvimento da personalidade.

Diante da complexidade da questão, faz-se necessária a presente pesquisa, com o intuito de se fornecer mecanismos teóricos para se equilibrar a proteção adequada ao direito à privacidade e à proteção de dados pessoais, com o desenvolvimento dos setores privados, em uma sociedade que é cada vez mais dependente das informações circulantes.

Por fim, esclarece-se que o texto demonstra aderência na área de concentração do Programa de Pós-graduação *Stricto Sensu* em Direito da Universidade Estadual Paulista (UNESP) “Sistemas Normativos e Fundamentos da Cidadania”, assim como à linha de pesquisa “Cidadania Civil e Política e Sistemas Normativos” ao demonstrar que a privacidade, na dimensão referente à proteção de dados, é um direito fundamental para o exercício da cidadania na sociedade da informação, sendo peça crucial para a efetivação dos demais direitos. Deste modo, seu exercício deve ser promovido adequadamente, de maneira específica pelo Direito, e respeitado por todos os sujeitos envolvidos nesta relação.

Outrossim, a pesquisa se harmoniza plenamente ao projeto “Relações Jurídico-privadas, Dignidade da Pessoa Humana e a Eficácia Horizontal dos Direitos Fundamentais”, uma vez que seu escopo principal é a promoção da tutela dos dados pessoais do indivíduo nas relações

jurídico-privadas, promovendo, desta maneira, a efetivação do próprio princípio da dignidade da pessoa humana.

1 O DIREITO À PRIVACIDADE

A presente subseção é de grande importância para o início deste trabalho, pois pretende introduzir o conceito do direito à privacidade, bem como apresentar, brevemente, como ocorreu a construção deste direito no ordenamento jurídico brasileiro. Compreender o direito à privacidade é tarefa primordial para o entendimento da problemática que será abordado ao longo desta pesquisa.

A subseção é dividida em alguns subtópicos. Na primeira parte, pretende-se, justamente, apresentar todo o processo de desenvolvimento do direito à privacidade, inicialmente entendido como o direito de ser deixado só, em uma perspectiva muito mais individualista.

Na segunda parte, objetiva-se analisar o direito à privacidade sob o prisma da Constituição Federal de 1988, em que aquele se insere no âmbito de direitos fundamentais da pessoa humana, alicerçado no princípio da dignidade da pessoa humana e na busca pela tutela integral do indivíduo.

De forma paralela, iremos estudar brevemente como os direitos fundamentais, dentre os quais o direito à privacidade, se inserem nas relações privadas, tendo como fundamento a teoria da eficácia horizontal dos direitos fundamentais. Procura-se esclarecer a importância da observância dos direitos fundamentais pelos atores privados, os quais, muitas vezes, são dotados de poder econômico, social, político, gerando uma relação de desequilíbrio com o titular e que pode, por esta razão, gerar violações de direitos.

Ao final da subseção, faremos uma análise do direito à privacidade sob a perspectiva infraconstitucional, na qual ele é compreendido como um direito da personalidade

1.1 Breve histórico do desenvolvimento do direito à privacidade

O direito à privacidade é um dos principais frutos do pensamento liberal predominante nos séculos XVII e XVIII, tendo aparecido em muitos documentos que buscam tutelar os direitos humanos, como, por exemplo, na Declaração Universal dos Direitos do Homem de 1948, na Convenção Americana de Direitos Humanos, assinada em 1969 em São José da Costa Rica (AVILA; WOLOSZYN, 2017, p. 171).

Inicialmente, cumpre esclarecer que, etimologicamente, o termo “privatus” – raiz do termo privacidade– significa privado, particular, próprio, pessoal e individual (SAMPAIO, 1998, p. 268).

Historicamente, o conceito de privacidade tem se relacionado diretamente com o estado de tecnologia de determinada sociedade. Por essa razão, seu conceito, como veremos, varia ao longo do contexto.

Primordialmente, na Grécia Antiga, a concepção de privacidade, formulada por Aristóteles, estava relacionada à separação entre a esfera pública e a esfera doméstica, sendo esta última considerada o reino da vida privada (MALDONADO; BLUM, 2020, p. 242).

Após, ele foi pensado como o direito de ser deixado só, em estudo até hoje muito famoso desenvolvido por Warren e Brandeis (1890, p. 205), publicado pelo Harvard Law Review, no sentido de não ter a esfera individual invadida ou molestada por qualquer mecanismo não autorizado, ou seja, de estar a salvo das interferências alheias. Nesta época, se pensava em outras hipóteses e invenções que poderiam malferir a esfera humana, como as máquinas fotográficas, que capturavam imagens de pessoas de maneira praticamente imediata. Assim, o objeto da preocupação era distinto.

O conceito de privacidade era de um caráter fortemente individualista, historicamente conectado ao rompimento da sociedade feudal, durante a metade do século XIX, e ao surgimento de espaços privados burgueses, em que predominava a ideologia liberalista. Neste sentido, a privacidade aparecia como um privilégio da Burguesia, com o objetivo de se isolar das demais classes (DONEDA, 2006, p. 92).

Ademais, Leonardo Zanini sugere que Warren e Brandeis ao tratarem do direito à privacidade estabelecem como garantia do indivíduo "[...] uma ampla liberdade contra intromissões não desejadas em sua vida, tutelando seus pensamentos, sentimentos, emoções, dados pessoais e até mesmo o nome" (ZANINI, 2015, p. 11). Ou seja, era uma dimensão mais negativa, ligada à não invasão de espaço, e à abstenção de terceiros. Trazia, ainda, uma ideia de ausência de comunicação entre uma pessoa e as demais.

Além disso, o direito à privacidade compreendia as manifestações do ser, como seus gestos, desenhos, e outras expressões, as quais também eram vistas como objeto de proteção. Ou seja, era um espaço em que o indivíduo poderia desenvolver sua individualidade, poder refletir, sem ser compelido a determinadas condutas socialmente esperadas.

Apesar disso, Warren e Brandeis apontam algumas exceções e limitações neste direito: o direito à privacidade não pode impedir a publicação do que é de interesse geral; assim como não proíbe a comunicação de tudo que é privado, já que existem situações em que tal comunicação é indispensável, como, por exemplo, em um Tribunal.

Posteriormente, influenciada pela transformação do modelo do Estado em um estado mais social (Welfare State) é que a privacidade foi adquirindo uma concepção mais ampla, preocupada com a realização da pessoa, motivo pelo qual seu conceito envolvia também o direito à intimidade, à autonomia privada e ao livre desenvolvimento da personalidade, expressando as pretensões individuais derivadas daquele direito de ser deixado só (MARTINS-COSTA, 2002, p. 34).

Além disso, o direito à privacidade começou a ser visto como um direito de todos os sujeitos, e não apenas de algumas classes sociais, que passaram a demandar uma tutela específica por parte do Estado.

Pela análise deste conceito, não é possível extrair um âmbito de proteção completamente definido. Assim, partindo desta perspectiva mais formal e teórica, o direito à privacidade pode ser variável, de acordo com a visão de cada titular do direito, isto é, daquilo que o sujeito considera que, no âmbito de sua vida pessoal, deverá ser reservado e indisponível aos interesses do Estado e de terceiros. Ademais, o termo "privacidade" também sofre interferência do ordenamento jurídico em que está sendo aplicado, o que dificulta sua redução a um sentido único e comum.

Adiante neste trabalho, veremos como o desenvolvimento da sociedade da informação e o aumento do fluxo de informações entre os indivíduos impactou o conteúdo e o alcance do direito à privacidade, tendo em vista que, com a internet e os novos meios de comunicação, os espaços da esfera privada têm diminuído.

1.2 Perspectiva constitucional: direito à privacidade como direito fundamental

Sob uma perspectiva constitucional, no Brasil, o direito à privacidade é assegurado pela Constituição Federal de 1988 de forma expressa, como um direito humano fundamental, que abrange a preservação da vida privada e da intimidade da pessoa, a inviolabilidade da correspondência, do domicílio, dos dados e das comunicações, em consonância com o previsto no artigo 5º inciso XII[2] (BOFF, FORTES, 2014, p. 119).

[2] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(...) XII - É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

A Carta Maior, nesta seara, segue o âmbito de tutela previsto na Declaração Universal de Direitos Humanos, elaborada pela Organização das Nações Unidas (ONU). Nesta, especificamente em seu artigo 12, consta que ninguém sofrerá intromissões arbitrárias na sua vida privada e, ainda, que, contra tais intromissões ou ataques, toda a pessoa tem direito à proteção da lei.

A Constituição Federal (C.F.), ao tratar da privacidade em sentido amplo, também tutela outros bens jurídicos, como a honra e a imagem (inc. X[3]), sendo que esta última traz a ideia de tutelar todo o aspecto físico, que é perceptivelmente visível no indivíduo (SILVA, 1994, p. 91). Assim sendo, o direito à privacidade, constitucionalmente, dialoga com outros direitos, também consagrados na lei maior, de maneira que deverão ser analisados em conjunto.

Dentre os bens jurídicos que envolvem a tutela da privacidade na Lei Maior, é importante destacar dois: a vida privada e intimidade.

A primeira é compreendida a partir de uma distinção entre aquilo que é público e aquilo que é privado. Consoante aos ensinamentos de José Afonso da Silva (1994, p. 204), é "o conjunto de modo de ser e viver, como direito de o indivíduo viver sua própria vida".

A intimidade, por sua vez, se refere a eventos ainda mais pessoais e particulares do titular, englobando a troca de expressões emocionais entre as pessoas, o exercício de atividades intrínsecas do indivíduo e a própria ideia do direito à tranquilidade (DONEDA, 2020, p. 80)

Nesta pesquisa, optamos por nos referir ao direito à privacidade em sentido amplo, envolvendo tanto aquilo que engloba a esfera mais íntima do indivíduo (privacidade como tutela da intimidade), quanto o espaço delimitado que lhe é privado (privacidade como tutela à vida privada).

Além disso, o direito à privacidade é norteado pelo princípio da dignidade da pessoa humana, previsto na Constituição como baliza de todo o sistema jurídico, sendo indissociáveis. A dignidade da pessoa humana é um dos principais pilares do Estado Democrático de Direito, exigindo que sejam respeitadas as garantias individuais e os direitos humanos.

Consequentemente, ele amplia o âmbito de tutela do direito à privacidade, que também deverá ser garantido pelo Estado. Por este motivo, qualquer ato que afete a privacidade do indivíduo é também um ato atentatório à existência de uma vida digna (MALDONADO; BLUM, 2020, p. 27).

[3] (...) X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

O direito à privacidade como direito previsto na C.F. autoriza que o titular, com base na garantia constitucional, impeça que certas situações de sua vida sejam levadas ao conhecimento de terceiros ou, mais ainda, que sejam turbadas por outros sujeitos. Assim, trata-se de um comando proibitório expressamente dirigido ao Estado, que não poderá violar os direitos previstos na Constituição.

Ainda no âmbito constitucional, o direito à privacidade aparece como direito que deve ser garantido pelo Estado, na defesa da dignidade da pessoa diante dos poderes públicos. Seu objetivo é justamente tutelar a pessoa humana como seu valor máximo, com consequentes deveres negativos e, sobretudo, deveres positivos por parte do Estado, certificando direito à indenização face eventuais danos decorrentes de violação (BITTAR, 2015, p. 114).

A Carta Maior traz mecanismos de salvaguarda, tais como, mandado de segurança, habeas corpus, habeas data- é o que mais se destaca, pois surgiu justamente para permitir que os indivíduos pudessem requerer informações pessoais que estivessem em posse do poder público-, dentre outros, a fim de enriquecer a tutela constitucional dos direitos fundamentais.

Assim, quando determinado sujeito - público ou privado, pessoa natural ou jurídica- praticar determinadas ações e condutas, sejam elas comissivas ou omissivas, que atinjam diretamente a privacidade do indivíduo, sem seu consentimento, o agente que praticou tal conduta ou que se omitiu quando deveria ter atuado de certa maneira, poderá ser juridicamente sancionado.

Com isso, verifica-se que a Carta Maior buscou atribuir ao direito à privacidade um elevado grau de proteção. Por esta razão, sua restrição apenas poderá se justificar em caso de ser demonstrada a necessidade de se proteger outros direitos fundamentais ou bens constitucionalmente relevantes.

Neste contexto, o próprio ideal de democracia previsto no nosso ordenamento está ligado ao cumprimento dos direitos fundamentais, o que implica que, caso estes não sejam respeitados, haverá violação às próprias bases que sustentam a democracia.

A preservação do direito à privacidade também é fundamental, como veremos no tópico 1.4, para assegurar as condições para o livre desenvolvimento da personalidade dos titulares deste direito.

1.3 Eficácia horizontal dos direitos fundamentais nas relações privadas

Neste ponto, é importante compreendermos o contexto em que ocorre a vinculação dos sujeitos particulares aos direitos fundamentais como um todo.

Para tanto, em primeiro lugar, é mister traçarmos algumas considerações sobre o constitucionalismo representa o movimento político, jurídico e ideológico que concebeu ou aperfeiçoou a ideia de estruturação racional do Estado e de limitação do exercício de seu poder, concretizada pela elaboração de um documento escrito destinado a representar sua lei fundamental e suprema. Ele traz ainda a ideia de garantia de direitos aos indivíduos.

No tocante ao conceito de direitos fundamentais, adota-se a concepção trazida por Ingo Wolfgang Sarlet (2012. p.19), no sentido de que:

> (...) constituem o conjunto de direitos e liberdades institucionalmente reconhecidos e garantidos pelo direito positivo de determinado Estado, tratando-se, portanto, de direitos delimitados espacial e temporalmente, cuja denominação se deve ao seu caráter básico e fundamentador do sistema jurídico do Estado de Direito.

A esse respeito, no constitucionalismo desenvolvido no Estado liberal, marcado pelas ideias iluministas e pela intenção da burguesia em assegurar os seus direitos frente ao poder absoluto do monarca, se buscava, em síntese, direitos que protegessem o indivíduo do despotismo do Estado (SARMENTO, 2010, p. 44).

Assim sendo, os direitos fundamentais tinham o intuito de delimitar um espaço no qual não haveria qualquer interferência estatal, garantindo, portanto, um espaço de liberdade e de autonomia aos indivíduos em face do poder do Estado.

Neste sentido, os direitos fundamentais eram compreendidos como direitos públicos subjetivos, oponíveis apenas ao Estado, tendo em vista que somente este era visto como um agente violador dos direitos fundamentais, por conta de sua atividade.

Em razão destas características, os direitos fundamentais tinham um cunho, além de individualista, “negativo”, voltados para a exigência de uma abstenção do Estado (SARLET, 2012, p. 32).

Dentre o rol destes direitos fundamentais se destacam o direito à vida, à liberdade, à propriedade e à igualdade.

Essa relação entre Estado, como detentor absoluto do poder, e particular, é de subordinação. Por este motivo, quando se busca garantir direitos aos indivíduos com o objetivo de se estabelecer um equilíbrio entre as partes desiguais do polo dessa relação de domínio e de subordinação, a doutrina entende que se trata da chamada “eficácia vertical” dos direitos fundamentais, cuja exigência de cumprimento se direciona exclusivamente aos Estados, destinatários das normas que estabelecem direitos fundamentais (LIMA, 2016, p. 17)

Apesar dos reconhecidos avanços trazidos pelo Estado Liberal em matéria de afirmação dos direitos fundamentais, com o fim da 1ª Guerra Mundial (1914-1918) e com o consequente agravamento das crises econômicas e sociais, atrelados aos impactos da industrialização, percebeu-se que o modelo proposto pelo Estado Liberal era insuficiente para garantir uma efetiva proteção da pessoa humana, fato que gerou movimentos reivindicatórios de direitos ao Estado.

Ou seja, percebeu-se a necessidade de se exigir do Estado prestações positivas, com o intuito de garantir as mínimas condições de existência aos indivíduos. Neste contexto, é que se desenvolve o Estado de Bem-Estar Social e se inicia um período de reconstrução dos direitos humanos, tendo como alicerce a dignidade da pessoa humana (SARMENTO, 2010, p. 44).

O Estado social de Direito, portanto, aumentou as atividades e funções do Estado e, ainda, fez com que a sociedade também participasse cada vez mais do exercício do poder. O incremento dessa participação maior da sociedade no exercício do poder teve como consequência o surgimento de situações de desigualdades, em razão de um maior ou menor poder social.

Notou-se que alguns grupos e indivíduos eram socialmente mais fragilizados e mais vulneráveis do que outros e que, muitas vezes, ocorria a exploração das parcelas menos favorecidas da sociedade por aquelas mais fortes, bem como o desenvolvimento de lutas “de” e “pelo” poder.

Assim sendo, rompeu-se o paradigma no sentido de que somente nas relações com o Estado haveria uma relação de dominação e subordinação, chegando à conclusão de que a ameaça e violação dos direitos fundamentais também eram causadas por atores privados, detentores de poder político, econômico e social, em relações totalmente desiguais.

Diante do quadro exposto, com o intuito de o Estado proteger os indivíduos contra atos atentatórios de outros particulares, é que os direitos fundamentais deixaram de ser direitos meramente subjetivos, oponíveis ao Estado, e passaram a ter também uma dimensão jurídico-objetiva, trazendo consigo limites e valores irradiantes sobre todo o ordenamento, no âmbito público e privado (SARLET, 2000, p. 06).

Em síntese, o legislador passou a perceber que em determinadas relações privadas, é necessária a interferência estatal, para eliminar as desigualdades fáticas e materiais resultantes das diferentes posições econômicas das partes e, assim, proporcionar uma efetiva igualdade material. Essa vulnerabilidade dos particulares se nota, principalmente, nas relações de

trabalho, de sindicato, de família, bem como nas relações envolvendo grupos de minorias étnicas, religiosas e sexuais.

Assim, partindo da compreensão de que os direitos fundamentais são garantias constitucionais universais, estes também devem produzir efeitos nas relações existentes entre sujeitos particulares, impondo-se ao Estado o dever garantir a dignidade humana também nas relações jurídicas entre particulares, com o objetivo de restaurar o equilíbrio e a igualdade entre as partes (SARMENTO, 2010, p. 113).

Conforme explica Gustavo Tepedino (2000, p. 06), a pessoa humana, devidamente qualificada na determinada relação jurídica em que está inserida, consoante ao valor social de sua atividade e ao grau de vulnerabilidade que apresenta, transforma-se na categoria central do direito privado.

A problemática, nesta situação, seria de como e em que medida ocorreria a incidência dos direitos fundamentais na seara do direito privado, tendo em vista que, diferentemente do Estado, os atores privados são essencialmente livres, sendo que sua autonomia e sua liberdade também são consideradas direitos fundamentais, protegidos pela Constituição.

O questionamento acerca da eficácia dos direitos fundamentais às relações entre particulares é chamado por parte da doutrina de "eficácia horizontal dos direitos fundamentais", uma vez que é aplicada em uma relação na qual os dois polos são, ao mesmo tempo, titulares de direitos fundamentais. Os direitos fundamentais, como valores que transcendem as preferências individuais, passam a poder ser exigidos pelo indivíduo em suas relações interpessoais.

No Brasil, a doutrina majoritária, incluindo autores como Ingo Wolfgang Sarlet, Luiz Edson Fachin, Luís Roberto Barroso, Daniel Sarmento, Gustavo Tepedino, Wilson Steinmetz, já reconhecem a possibilidade de vinculação dos particulares aos direitos fundamentais.

A teoria da eficácia mediata ou indireta, sustentada por Günther Dürig, tem como foco a preservação da autonomia privada. Seus defensores alertam para o fato de que os direitos fundamentais não devem ser aplicados de forma indistinta sobre as relações privadas, sob pena de se exterminar a autonomia privada e de desconfigurar todo o Direito Privado.

Assim, os doutrinadores propõem que sejam aplicadas soluções diferenciadas, mediadas pelo legislador, compatibilizando as cláusulas gerais do direito privado com os valores constitucionais. Ademais, destacam que, em alguns casos, é possível a relativização dos direitos fundamentais na relação entre os particulares, em favor da autonomia privada, permitindo que as partes decidam livremente como exercerão sua liberdade. As cláusulas gerais, portanto, é

que seriam preenchidas pelo intérprete, orientado por valores constitucionais, mas permitindo uma coexistência entre a autonomia privada e os direitos fundamentais.

Acerca desta problemática, Baez e Lima (2016, p. 03) esclarecem que os limites impostos à autonomia privada variam caso a caso, a depender de quais são os direitos envolvidos, se são de caráter patrimonial ou existencial, sendo que estes últimos terão mais proteção e, consequentemente, promoverão maior limite à autonomia privada.

Do mesmo modo, a essencialidade do bem em discussão também contribuirá para definir a intensidade de proteção. Havendo isonomia entre os particulares, a autonomia privada deve prevalecer. Essa atenção se justifica pelo fato de que os particulares, embora vinculados aos direitos fundamentais, também são titulares de direitos.

Cumpre ressaltar que a Constituição Federal de 1988 não contempla expressamente a hipótese da vinculação dos particulares aos preceitos de direitos e garantias fundamentais. Porém, pela primeira vez em uma Constituição brasileira, a questão dos direitos fundamentais é tratada com relevância, estando disposto no art. 5º, § 1º, da referida Constituição que "as normas definidoras dos direitos e garantias fundamentais têm aplicação imediata".

Em razão desta constatação, Ingo Sarlet (2012, p. 35) defende que os direitos fundamentais, na qualidade de princípios constitucionais e, principalmente, por força do princípio da unidade do ordenamento jurídico, devem se aplicar a toda a ordem jurídica, abrangendo também as relações privadas, para proteger os indivíduos não apenas contra atos abusivos do Estado, mas também contra atos atentatórios aos direitos fundamentais causados pelos particulares.

Em síntese, para o autor Ingo Sarlet, a Constituição atua como garantia e limite do direito privado, contribuindo e atuando com este, na proteção dos indivíduos mais fragilizados e vulneráveis.

Sendo assim, diante do exposto, é mister que haja um equilíbrio entre princípios do direito privado e os direitos fundamentais, buscando sempre uma ponderação de valores, a fim de que nenhuma das partes, na qualidade de titulares e de destinatárias de direitos fundamentais, sacrifique demasiadamente seus direitos.

1.4 Perspectiva infraconstitucional: direito à privacidade como direito da personalidade

Paralelamente, sob a óptica infraconstitucional também há uma preocupação em proteger esse direito, principalmente para preencher eventuais lacunas deixadas pela Lei maior, a fim de garantir uma proteção integrada, com focos de atuação mais determinados.

Assim, no Brasil, essa proteção é feita por inúmeros instrumentos, como o Código de Defesa do Consumidor (BRASIL, 1990), o Código Civil (BRASIL, 2002), a Lei de Acesso à Informação (BRASIL, 2011), o Marco Civil da Internet (BRASIL, 2014) e, mais recentemente, a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018).

Nesta seara, destacamos o Código Civil (C.C.), que promoveu uma reconstrução do direito privado, focando na proteção da pessoa humana. O C.C., inclusive, inaugura um capítulo inteiro dedicado aos direitos da personalidade, entre os quais se encontra o da privacidade, realizando, desta maneira, uma consolidação da temática.

Primeiramente, cumpre destacar que, nos termos do art. 2º do Código Civil, a personalidade civil da pessoa natural começa do nascimento com vida da pessoa. No entanto, a lei põe a salvo, desde a concepção, os direitos do nascituro.

Assim, é importante esclarecer o conceito de direitos da personalidade. Para tanto, optamos por adotar o entendimento de Carlos Alberto Bittar, segundo o qual:

> Consideram-se da personalidade os direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, o segredo, o respeito, a honra, a intelectualidade e outros tantos (2015, p. 29).

Para o Professor Eduardo Tomasevicius Filho (2021, p. 133), os direitos da personalidade se voltam à proteção da própria pessoa humana, com o intuito de garantir sua sobrevivência, bem como tutelar sua integridade física e psíquica.

Portanto, o objeto destes direitos é justamente a proteção de determinados atributos físicos, mentais e/ou morais do homem, devidamente individualizados pelo ordenamento jurídico. Em razão disso, ocupam uma posição autônoma no cenário dos direitos privados, recebendo uma atenção ainda mais especial. Assim, são direitos relativos à própria natureza do homem, como ser dotado de personalidade.

Os direitos da personalidade estão inclusos na cláusula geral de tutela da pessoa humana, tendo em vista que reforçam a preocupação do ser humano como valor-fonte do ordenamento

jurídico. (BIONI, 2020, p. 76). Tais direitos da personalidade são intransmissíveis, imprescritíveis, impenhoráveis, vitalícios e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

A conceituação dos direitos da personalidade não deve ser compreendida como um rol taxativo, mas sim expansivo, que possa, frente às mudanças ocorridas na sociedade, ser revisto, à luz da cláusula geral de proteção da personalidade presente na Constituição.

No que diz respeito especificamente ao direito à privacidade, Bittar (2015, p. 57 e 155) o classifica como direito de cunho psíquico, assim como o direito à liberdade e à intimidade. O doutrinador entende que a proteção do direito à privacidade implica em uma defesa da própria personalidade humana em face de intromissões e injunções alheias na vida ou na consciência do titular.

É um resguardo no psiquismo humano, tendo em vista que, nesta situação, o indivíduo não quer que certos aspectos de sua personalidade sejam conhecidos por terceiros. Além disso, esse direito se expande e irradia sobre os âmbitos do lar, da família e da correspondência.

No Direito Civil brasileiro, representado principalmente pelo Código Civil, os direitos da personalidade, dentre os quais o da privacidade, são tratados de maneira apartada e sistematizada no Capítulo II do Título I, do Livro I, da Parte Geral. Logo no início, é reforçado o caráter essencial desses direitos.

O Código Civil, em seu artigo 21, estabeleceu também que "[...] a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (BRASIL, 2002).

A tutela trazida pelos instrumentos acima traz uma dimensão negativa em relação ao direito à privacidade, no sentido de não se invadir espaços privados.

Por outro lado, a Lei Geral de Proteção de Dados Pessoais, de nº 13.709/2018, a qual será abordada mais detalhadamente na subseção 3, traz expressamente o direito fundamental à privacidade, como objeto de proteção da lei, nos termos do art. 1º da LGPD[4]. Analisando o artigo referido, nota-se que o espírito da lei foi justamente proteger direitos fundamentais já consagrados na Constituição, mas que, diante do novo cenário econômico e das novas tecnologias, exigiram maior proteção.

[4] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Além disso, essa mesma lei consagra o respeito à privacidade como um de seus fundamentos, enumerados no art. 2º[5]. Tal fundamento aparece também no art. 17[6] da LGPD, que traz os direitos do titular de dados e, dentre esse rol, está a garantia do direito fundamental à privacidade.

Assim, é possível observar que o direito à privacidade faz parte da disciplina da proteção de dados pessoais no ordenamento jurídico brasileiro, uma vez que, para se garantir uma tutela efetiva do titular de dados é mister que, antes de tudo, se assegure os parâmetros mínimos de proteção de sua privacidade.

Ademais, como veremos adiante, o direito à privacidade tem se expandido para abarcar não apenas o espaço privado, como também o controle, pelo titular, de seus dados e informações pessoais, necessitando de uma proteção mais específica, o que contribuiu para deflagrar a privacidade como fundamento da Lei Geral de Proteção de Dados Pessoais.

[5] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - O respeito à privacidade;

[6] Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

2 SOCIEDADE TECNOLÓGICA E NOVAS DIMENSÕES DO DIREITO À PRIVACIDADE

Esta segunda subseção tem o intuito de analisar como o constante avanço tecnológico e o desenvolvimento de novos meios de comunicação e de troca de informação, no qual ganhou destaque um novo modelo de organização social, voltado para um fluxo cada vez maior de bases de dados pessoais, tem impactado os direitos dos indivíduos, ao trazer novas possibilidades de violações, sobretudo ao direito à privacidade e à proteção de dados pessoais.

Assim sendo, em um primeiro momento, pretende-se apresentar as principais características da sociedade da informação, focando, principalmente, em como ocorre o uso de dados pessoais no âmbito desta sociedade.

A partir desta exposição, na segunda parte da subseção, busca-se compreender em que medida os pessoais constituem uma projeção da personalidade de seu titular.

Outro ponto importante é que essa subseção procura delimitar aos leitores o conceito jurídico de dados pessoais, com base na legislação e na doutrina utilizada nesta pesquisa. A compreensão deste conceito é fundamental para o melhor entendimento do trabalho.

2.1 Sociedade da informação e a exposição constante de dados pessoais

A sociedade atual, marcada pela evolução tecnológica e pela revolução dos meios de comunicação, sobretudo da internet e dos dispositivos eletrônicos, que facilitaram a coleta e a retenção de dados, inaugurou uma nova forma de organização social e econômica, alicerçada no fluxo constante da informação, a qual, por sua vez, passou a ser um bem de extrema importância.

Neste sentido, o capitalismo industrial tem dado cada vez mais espaço a uma sociedade organizada em torno dos dados, os quais passam a afetar todos os aspectos desta, direta ou indiretamente.

As novas tecnologias potencializam as formas de violação aos direitos da personalidade.

Tal situação trouxe reflexos no direito, trazendo para debate o seguinte questionamento: como fica a tutela do direito à privacidade na seara da sociedade da informação? Como os operadores de direito devem atuar para protegê-lo e, principalmente, como os cidadãos devem se proteger? Afinal, toda mudança tecnológica é também uma mudança social. O direito como instrumento de regulação social reflete estas mudanças e deve evoluir com elas.

Diante do exposto, é importante, inicialmente, trazermos uma breve contextualização do problema apresentado.

Historicamente, como vimos no tópico anterior, na primeira metade do século XX, com a implementação do modelo de Welfare State, o Estado passou a promover cada vez mais serviços públicos, referentes a áreas essenciais à população (moradia, trabalho, saúde, entre outros). Com isso, de forma geral, o Estado passou a gerenciar uma quantidade muito maior de dados pessoais de seus cidadãos.

Seguindo uma linha cronológica, consoante os ensinamentos de Castells (2011, p. 412), o século XXI se caracteriza pelo aprimoramento das formas de telecomunicação móvel, bem como pela revolução da tecnologia e da capacidade da informática, o que ensejou uma intensificação do fluxo de informações na sociedade.

Nesta perspectiva, a base material da sociedade passou a ser a informação, sendo esta uma fonte de geração de riqueza, de exercício de poder e, principalmente, de novos códigos culturais, promovendo uma reestruturação socioeconômica.

A esse respeito, de acordo com Sarlet e Keinert (2015, p. 114), a sociedade da informação tem como uma de suas principais características a aceleração dos processos de produção e de disseminação do conhecimento. Isso porque as novas tecnologias romperam os obstáculos físicos e permitiram que a informação fosse apresentada em uma quantidade e em uma velocidade jamais vistas anteriormente.

A rede passou a ser mais aberta e dinâmica, possibilitando o estabelecimento de novas relações sociais e diferentes formas de interação, permitindo que diversas pessoas, em qualquer parte do mundo, pudessem ter acesso a um mesmo fato de forma simultânea.

Para Castells (2011, p. 255), a emergência dessas diversas redes permitiu a intersecção de sistemas distintos, que passaram a se complementar e, muitas vezes, a serem dependentes uns dos outros.

Com isso, permitiu-se ainda que se conhecesse melhor a sociedade e os indivíduos nela inseridos, como, por exemplo, saber sobre seus hábitos, interesses, opiniões (BIONI, 2021, p. 03). A tecnologia, neste sentido, se infiltrou em questões mais íntimas e sensíveis do cidadão.

Além de um instrumento de conhecimento, a informação também é vista como meio de poder e de controle para quem a detém, influenciando as mais diversas tomadas de decisão na seara econômica, social e política (BLUM; SCHUCH, 2019, p. 32).

Nos dias atuais, controlar dados é sinônimo de exercer poder. A soberania do próprio Estado é medida pela sua capacidade de acesso à informação.

Nesta perspectiva, a informação, além de um instrumento de poder, aparece como moeda de troca e de pagamento, uma vez que, nos dias atuais, um indivíduo consegue ter acesso a serviços, comprar produtos, apenas com a disposição de suas informações pessoais (PECK, 2013, p. 43).

Esse reconhecimento da informação como um fenômeno relevante é justamente por conta das inúmeras possibilidades de uso dela. Hoje, ela é vista como matéria-prima necessária para o desenvolvimento de toda e qualquer atividade.

Importante esclarecer que para se chegar à informação consolidada, que tem realmente valor para a sociedade, é preciso, primeiramente, ter acesso aos chamados dados, que representam o estado primitivo da informação. Assim, apenas quando os dados são agregados e organizados é que poderão se transformar em algo inteligível, podendo ser deles extraída uma informação (BIONI, 2021, p. 31).

Assim, esclarece-se que, embora ambos os termos sirvam para se representar um fato, o dado corresponde ao estado primitivo da informação, algo muito mais fragmentado, enquanto a informação revela um conteúdo maior. É algo além da representação contida no dado.

Frente a este contexto, de acordo com Klaus Schwab (2016, p. 15), o século XXI inaugura a chamada "Quarta Revolução Industrial", que se caracteriza por uma integração cada vez maior entre tecnologias, dados e indivíduos. Para o autor, a expressão revolução traz a ideia de uma mudança abrupta e radical.

Para alguns autores, como Fernando Antônio Tasso (2020, p. 98) e Bruno Bioni (2019, p. 132), os dados pessoais são vistos como o "novo petróleo", o verdadeiro insumo da economia da indústria 4.0, uma vez que praticamente todos os aspectos da vida humana são abastecidos por dados.

Nesta seara, também é interessante apontar o termo "Big Data" que, nas palavras de de Amaral (2016, p. 12) pode ser compreendido como "fenômeno de massificação de elementos de produção e armazenamento de dados, bem como o processo de tecnologias, para extraí-los e analisá-los". Usualmente, o termo "Big Data" se refere à coleta e ao armazenamento de uma grande quantidade de dados e de informações, para posterior análise.

O "Big Data" permitiu que nos dias atuais os dados fossem produzidos em uma enorme variedade de formatos, excedendo a capacidade das tecnologias consideradas tradicionais de processamento, em uma velocidade intensa, e em volume expressivo, já que passa a ser possível organizar quantidades elevadas de dados, estabelecendo-se, ainda, diferentes relações entre

eles. Em síntese, a coleta de dados se tornou muito mais fácil e menos custosa. Ainda, o Big Data trouxe a possibilidade de novas formas de aplicações dos dados, antes sequer imagináveis.

Assim, nota-se que o surgimento de um paradigma tecnológico organizado em torno das tecnologias da informação possibilita que a própria informação se transforme em um produto (CASTELLS, 2011, p. 120). O ganho em eficiência e em escala de determinada atividade econômica é justamente por conta da operação envolvendo o tratamento de dados.

Este processo de transformar algum elemento da realidade para um formato numericamente quantificável, que possa ser analisado, é chamado de "*datification"*, de acordo com estudo desenvolvido por Viktor Mayer-Schonberger e Kenneth Cukier (2013, p. 46).

Ao mesmo tempo, o custo para a produção destes dados é cada vez mais reduzido, diante das inúmeras possibilidades de processamento. Ademais, os dados trazem um aspecto de veracidade quanto ao seu conteúdo, permitindo identificar padrões e até prever probabilidades de acontecimentos futuros. Pela união de todas estas características, os dados hoje têm um imenso valor para o mercado, impactando diretamente no desenvolvimento da economia e da sociedade.

Há, ainda, uma mudança qualitativa no processamento de dados, tendo em vista que as atividades relacionadas ao seu tratamento podem ser feitas não apenas por humanos, mas também por máquinas, algoritmos ou outros mecanismos ligados à inteligência artificial- esclarece-se que o tema da inteligência artificial aparece nas discussões matemáticas tecnológicas desde o final dos anos 1940 e início dos anos 1950, contudo, apenas nos últimos anos é que ganhou status relevante nas discussões jurídicas.

Para compreender o tema, optamos por empregar o conceito desenvolvido por Daikohara e Kasemirski (2020, p. 217 e 218) no sentido de que a "implementação de algoritmos, que consiste em um conjunto finito de diretrizes que descrevem como executar uma tarefa, faz com que ocorra um aprendizado na internet, apontando suas preferências e caminhos a seguir". Essas diretrizes são expressas em uma linguagem matemática.

Os algoritmos consistem em instruções elaboradas de forma organizada e sequencial, agrupadas justamente para se estabelecer referências de como algo deverá ser executado, buscando resolver algum tipo de problema. Ou seja, eles funcionam como um conjunto de regras a serem seguidas, a fim de que determinada questão seja solucionada. Eles são, basicamente, um roteiro de comandos previamente ordenados.

Nos dias atuais, os algoritmos costumam ser programados para extrair padrões e inferências sobre características de uma pessoa, seu estado de ânimo, emocional, entre outros.

A partir da coleta destes elementos, são tomadas decisões. Em muitos casos, essas decisões são tomadas de forma automatizada, isto é, por meio de máquinas, sem a participação do "decidir humano". As máquinas vão se aperfeiçoando por meio do aprendizado baseado em exemplos.

O uso de determinados algoritmos, inclusive, possibilita que se elabore perfis de comportamento dos indivíduos aos quais determinado dado se refere, identificando suas preferências, interesses, situação econômica e até aspectos de sua saúde.

Outrossim, hoje, existem algoritmos que, inclusive, conseguem traçar tendências de futuras decisões e comportamentos de um indivíduo. Os métodos e as técnicas pelos quais a inteligência artificial se desenvolve são extensos. Um perfil obtido desta forma é como uma representação virtual da própria pessoa, podendo se confundir com ela.

Apesar disso, é importante fazer a ressalva de que, por serem processos de abstração, os dados nunca corresponderão a uma descrição 100% (cem por cento) objetiva do objeto de análise, podendo, algumas vezes, trazer resultados parciais, influenciando a maneira pela qual determinado indivíduo é visto e classificado na sociedade (FRAZÃO; TEPEDINO; OLIVA, 2019, p. 12).

Por esta razão, é mister que aqueles que usam algoritmos na tomada de decisão esclareçam como determinado algoritmo funciona e eventuais aspectos falhos (MALGIERI; COMANDÉ, 2017, p. 258/259).

Além das novas formas de manipulação dos dados, a sociedade informacional passou a utilizar diferentes meios de armazenamento de informação, onde é possível acumular inúmeros dados de forma estruturada, seguindo uma determinada lógica pré-estabelecida, nos chamados bancos de dados. Estes, em síntese, de acordo com Doneda (2011, p. 92), consistem em uma ferramenta que permite a sistematização de um volume enorme e bastante detalhado de informações. São as popularmente conhecidas como "nuvens" de armazenamento.

Os bancos de dados podem ser acessados por diferentes sujeitos. Em razão disso, nos deparamos com uma coleta e uma catalogação cada vez maior de dados pessoais, que permite que estes sejam agregados das mais variadas formas. A cada segundo, uma grande quantidade de dados e, consequentemente, de informações são geradas e transmitidas, a um custo cada vez menor.

Nesta perspectiva, a sociedade da informação se diferencia por ter como valores principais aspectos imateriais, já que são os dados, as informações e as tecnologias que mais contribuem para o seu desenvolvimento e para sua organização.

Ademais, ela traz novas possibilidades para que os cidadãos possam exercer seus direitos e liberdades, já que, com a disponibilização de novas tecnologias de comunicação, aqueles passam a dispor de diferentes meios de expressão e de interação.

A esse respeito, é importante fazer uma ressalva: essa nova forma de organização social não se restringe apenas ao meio virtual, mas a toda a sociedade. A tecnologia assumiu um caráter onipresente nas esferas da vida social, econômica, política, cultural (SARLET, 2020, p. 40).

Isto posto, embora o avanço tecnológico facilite a comunicação entre os indivíduos e possibilite o intercâmbio de informações, ele também permite que, muitas vezes, os dados coletados para se gerar uma informação, sejam utilizados de forma abusiva ou excessiva, como instrumento de controle social, de restrição à liberdade e até de discriminação, o que pode levar à vulneração de direitos fundamentais do cidadão, sobretudo seu direito à privacidade, tendo em vista que os dados correspondem exatamente à aspectos da personalidade do indivíduo (MENDES, 2014, p. 20).

O ambiente virtual, de certa maneira, acaba sendo mais propenso a violações no uso de dados, uma vez que estas ocorrem de forma mais imperceptível do que ocorreria no espaço físico, já que no meio virtual nunca se sabe exatamente quais dados estão sendo coletados e como está sendo seu tratamento, enquanto no físico tais processos são mais facilmente percebidos.

Além disso, tendo em vista a vasta dimensão do ambiente virtual, é ainda mais difícil deter o controle sobre o tratamento que está sendo realizado. Assim, a possibilidade de manipulação dos dados também é maior. Aliás, muitas vezes o titular sequer tem conhecimento da exposição e do compartilhamento de seus dados pessoais.

Outro ponto que deve ser visto com atenção é sobre a criação dos já mencionados perfis de comportamento, uma vez que, a construção de perfis eletrônicos, de certa forma, acaba reduzindo a personalidade e a liberdade da pessoa a algo já predefinido por algoritmos.

Isto posto, a violação ao titular pode ocorrer de diferentes maneiras, sendo ocasionadas desde, por exemplo, a falta de disponibilização de informações que lhe dizem respeito, até a prática de comportamentos incoerentes, praticados sem o conhecimento do titular.

Assim, alguns autores, como Sarlet (2015, p. 2016) concluem que a sociedade da informação também é uma sociedade de risco, dotado de certas peculiaridades. O risco é justamente essa possibilidade de utilização dos dados de forma indevida, incorreta ou abusiva, ou, ainda, sem o conhecimento de seu titular.

Como veremos adiante, a sociedade da informação também deu espaço para o surgimento de empresas especializadas na coleta e no processamento de dados pessoais.

Com isso, atualmente, nos deparamos com um problema ainda maior, que atinge diretamente a privacidade e os direitos do titular de dados: a apresentação de campanhas de marketing e de publicidade formuladas a partir do tratamento de dados pessoais dos cidadãos, que, na maioria das vezes, sequer tem conhecimento de que seus dados estão sendo coletados para tais finalidades - ou sequer sabem que está ocorrendo a coleta.

Assim, o Direito se encontra diante de uma situação paradoxal: por um lado, ele deve proteger o direito à privacidade e à proteção de dados pessoais dos usuários, diante dos riscos de uso indevido e abusivo; por outro, o Direito deve regulamentar a livre-iniciativa e a liberdade de as partes contratarem da forma que melhor entenderem (PECK, 2013, p. 44).

Importante esclarecer que a causa do problema envolvendo o direito à privacidade não é o uso da tecnologia em si, mas sim as decisões tomadas pelos agentes que detêm a tecnologia. O desenvolvimento tecnológico pode - e deve- ser harmonizado com a preservação da privacidade e dos demais direitos fundamentais do cidadão, os quais são condições essenciais para o próprio exercício da cidadania na era eletrônica.

Frente a este contexto, tem ganhado relevância o debate acerca da necessidade de se propor limites para o tratamento de dados pessoais e de se exigir mais responsabilidade e transparência daqueles que efetuam seu processamento, a fim de respeitar os direitos fundamentais do cidadão e a dignidade da pessoa humana- sendo tal discussão recorrente não apenas no campo jurídico, mas também na literatura e em diversos outros contextos.

2.2 Dados pessoais como projeção da personalidade

Para melhor compreensão dos dados pessoais como uma projeção da personalidade do indivíduo ao qual se referem, adotamos o conceito de Bruno Bioni segundo o qual a personalidade significa “características ou o conjunto de características que distingue uma pessoa” (2021, p. 77).

Os direitos da personalidade, como exposto, surgem justamente para tutelar esses caracteres que envolvem a pessoa humana, protegendo tudo aquilo que representa uma dimensão de seu titular. O autor ainda complementa que: “sob essa perspectiva, um dado, atrelado à esfera de uma pessoa, pode se inserir dentre os direitos de personalidade de uma

pessoa (...), caracterizando-se como uma projeção, uma extensão ou dimensão do seu titular" (BIONI, 2021, p. 77).

Os dados pessoais, em síntese, são as características exteriorizadas de seus titulares, que os identificam. Justamente por constituírem como forma de prolongamento da pessoa, os dados pessoais também refletem toda a esfera relacional que cerca aquele indivíduo e merecem uma tutela jurídica adequada.

Isto posto, Laura Mendes Schertel explica que, à medida que os dados pessoais são, na verdade, representações do indivíduo na sociedade, ou seja, projeções diretas de sua personalidade, qualquer tratamento que seja feito com estes dados poderá afetar a personalidade daquele titular (2019, p. 45).

Muitas vezes, os dados são a única forma de representação do indivíduo, uma vez que, em determinadas situações, sua presença física não seria possível.

Em razão destas novas possibilidades trazidas pelo uso de dados pessoais, Reis (2018, p. 13) entende que a identidade do indivíduo passa a ser cada vez mais expandida e fluída, combinando o virtual, o artificial, o real e o natural.

É evidente que os gostos, interesses de uma pessoa, se vistos de forma isolada, não trariam graves consequências ao titular. Porém, a partir do momento em que, por meio do agrupamento de dados pessoais, as informações relativas a alguém são processadas e tratadas, é possível construir um compilado da personalidade que pode influenciar a maneira pela qual aquele indivíduo é compreendido na sociedade em que está inserido. Além disso, o tratamento de dados, muitas vezes, pode ser manipulado por terceiros e, assim, trazer aspectos equivocados a respeito do titular ao qual se referem.

2.3 O bem jurídico protegido: a delimitação do conceito jurídico de dados pessoais e de dados sensíveis

Em síntese, a sociedade tecnológica, que passou a ter uma dependência cada vez maior dos fluxos de bases de dados, traz a necessidade de se repensar e se repactuar o compromisso das instituições com os cidadãos, titulares dos dados, os quais merecem uma proteção específica, a fim de que as informações que lhes dizem respeito não sejam utilizadas de forma indevida. Somente assim o titular terá uma tutela integral de seus direitos fundamentais.

É um tema, portanto, que traz aspectos complexos e que merece a devida atenção pelo Direito que, como estrutura organizacional e normativa regulatória, deve desenvolver mecanismos concretos para lidar com tal fenômeno.

Cumpre pontuar que o debate sobre a regulamentação da proteção de dados pessoais surgiu com força, sobretudo, na União Europeia.

Dentre as normas desenvolvidas, destacamos a Carta de Direitos Fundamentais da União Europeia, que reconheceu o direito à proteção de dados [7], a Diretiva 95/46/CE [8], que efetivamente criou uma Autoridade de Garantia, e o Regulamento Geral de Proteção de Dados Pessoais Europeu nº 679 (GDPR), que entrou em vigor em 25 de maio de 2018, com o intuito de abordar a proteção das pessoas físicas no que tange ao tratamento e à livre circulação de dados pessoais, conforme previsto em seu artigo 1º[9].

A legislação buscou, ainda, harmonizar as leis de privacidade e de proteção de dados no âmbito da União Europeia. A UE, inclusive, passou a exigir que os países que quisessem realizar relações comerciais com o bloco, deveriam ter uma legislação que oferecesse regulamentação de dados pessoais de forma semelhante ao GDPR.

No Brasil, o principal marco regulatório, que efetivamente incorporou a temática de proteção de dados pessoais ao debate e uniformizou as normas sobre o assunto, foi a Lei Geral de Proteção de Dados, de nº 13.709/2018, que foi sancionada em agosto de 2018 e entrou em vigor em setembro do ano de 2020 nos termos especificados pela Lei 13.853/2019 e que será exposta com mais detalhes nas próximas subseções. A LGPD teve como influência o próprio GDPR, reproduzindo muitas de suas cláusulas e condições.

Em relação ao conceito de dado pessoal, a LGPD define, em seu artigo 5º, que ele seria: "informação relacionada à pessoa natural identificada ou identificável."

O dado pessoal é aquele elemento que permite, portanto, identificar a pessoa a quem se diz respeito. Esclarece-se, aqui, que o titular é considerado "identificado" quando for possível, dentro de um grupo de pessoas, distingui-lo dos demais. Os dados pessoais compreendem desde

---

[7] Art. 8º. 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.

[8] Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Em seu art. 28, estabelece a criação da autoridade de garantia: "1. Cada Estado-membro estabelecerá que uma ou mais autoridades públicas serão responsáveis pela fiscalização da aplicação no seu território das disposições adoptadas pelos Estados-membros nos termos da presente directiva".

[9] 1.This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

o nome do titular, seu CPF, dados de localização, e-mail, dados biométricos, sendo que estes últimos são chamados de dados pessoais sensíveis.

Importante esclarecer que nossa legislação optou por um conceito expansionista de dado pessoal, tendo em vista que não abrange tão somente a informação relativa à pessoa diretamente identificada, mas também aquela que tem potencial de identificar o titular. Neste sentido, dependendo do contexto da situação em causa e das circunstâncias do caso, determinados dados são suficientes para identificar um indivíduo. A definição, portanto, envolve uma noção mais ampla.

Por outro lado, se estivermos diante de dados que não identifiquem ou nem possam tornar identificável uma pessoa, eles não serão pessoais e, portanto, não serão objeto de proteção das disposições da LGPD.

Para Chiara Spadaccini de Teffé e Mario Viola, a LGPD parte justamente da ideia de que "todo dado pessoal tem importância e valor" (2020, p. 02).

A Lei delimita o bem jurídico que se busca proteger: os dados pessoais e seu titular, indo além de uma abordagem vinculada meramente à proteção da privacidade. A proteção é ampla, vez que se dirige a todo e qualquer dado em que se denote o prolongamento de um sujeito. Proteger dados pessoais, portanto, implica em resguardar a própria personalidade do indivíduo, já que os dados estão diretamente conectados à esfera de uma pessoa.

Ademais, parte do reconhecimento da condição de vulnerabilidade do titular, que está inserido em uma relação assimétrica, em que um dos polos é justamente aquele que usa, controla e exclui seus dados.

Assim sendo, a proteção de dados pessoais tem papel fundamental para que o indivíduo se realize na sociedade e possa exercer seus direitos da personalidade.

É importante destacar que deve haver um vínculo objetivo entre o titular e a informação utilizada. Ou seja, o dado, a informação, devem se referir expressamente a características ou a ações da pessoa, revelando algo sobre ela. A informação deve manter um vínculo indissolúvel com a pessoa, sendo, portanto, uma extensão de sua personalidade.

Neste sentido, opiniões alheias, por exemplo, não devem ser compreendidas como dados pessoais. Do mesmo modo, a produção intelectual de uma pessoa, considerada isoladamente, também não é um dado pessoal (DONEDA, 2011, p. 93).

Há, ainda, uma subcategoria de dados pessoais, denominada de "dados pessoais sensíveis", criada a partir do reconhecimento, pelo legislador, de que o tratamento de certos

tipos de dados poderia gerar um risco ainda maior à personalidade do seu titular, sobretudo diante da possibilidade de os dados serem aplicados de forma discriminatória.

A Lei Geral de Proteção de Dados Pessoais esclarece, de forma exemplificativa, que dados sensíveis são aquelas informações sobre saúde, à vida sexual, origem racial ou étnica, organização de caráter religioso, convicção religiosa, filiação a sindicato, filosófico ou político, opinião política, além dos dados biométricos ou genéticos:

> II - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Neste ponto, vislumbra-se a influência da legislação europeia, o Regulamento Geral sobre a Proteção de Dados da União Europeia, que traz as chamadas categorias especiais de dados pessoais, as quais deverão receber um tratamento legal mais cuidadoso e específico:

> Artigo 9. Tratamento de categorias especiais de dados pessoais.
>
> 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

Os dados sensíveis, conforme esclarecido por Bioni (2020, p. 19), são uma espécie de dados pessoais que, embora também tragam um elemento identificador de uma pessoa, se diferenciam dos dados pessoais em sentido lato, em razão de o seu conteúdo oferecer uma especial vulnerabilidade e poderem gerar discriminação, estigmatização ou exclusão do titular, dependendo do modo pelo qual são utilizados, lesionando, desta forma, a identidade pessoal daquele.

Apesar da LGPD ser recente, o tema relativo aos dados pessoais sensíveis já havia aparecido na Lei do Cadastro Positivo (Lei nº 12.414/11), como “informações sensíveis”:

> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
>
> (...)
>
> II - Informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Os dados pessoais sensíveis, portanto, são dados ligados a informações mais íntimas e sigilosas de uma pessoa e envolvem, por exemplo, sua liberdade de pensamento, de expressão, de religião, de associação, entre outras. Em razão disso, o tratamento destes dados pode implicar em riscos mais gravosos aos direitos e liberdades fundamentais dos titulares.

É importante não limitar a compreensão dos dados pessoais sensíveis em um rol pré-determinado e exaustivo, tendo em vista que, dependendo do contexto e da finalidade em que a informação é utilizada, o dado poderá se tornar sensível.

Além disso, dados que sozinhos seriam apenas dados pessoais, ou seja, dados "não sensíveis", quando combinados com outros podem se tornar ou revelar uma informação sensível, também exigindo a devida proteção (parágrafo 1º do artigo 11 da LGPD). Em razão disso, é fundamental averiguar em cada caso concreto, no contexto do tratamento, se o dado coletado poderá servir como instrumento de estigmatização de seu titular. Para esta análise, é possível utilizar a mesma lógica que fundamenta a cláusula geral da tutela da pessoa humana.

A esse respeito, ensina Doneda (2006, p. 163):

> (...) deve-se ter em conta que a diferenciação conceitual dos dados sensíveis atende a uma necessidade de estabelecer uma área na qual a probabilidade de utilização discriminatória é potencialmente maior – sem deixarmos de reconhecer que há situações onde tal consequência pode advir sem que sejam utilizados dados sensíveis, ou então que a utilização destes dados se preste a fins legítimos e lícitos.

Assim, a definição de dados sensíveis vem justamente para promover a igualdade material de tratamento dos indivíduos, a fim de que estes não sejam discriminados em razão de suas características e informações pessoais e, desta forma, tenham sua dignidade garantida.

Aqui busca-se também proteger as condições relativas ao corpo eletrônico que se constituiu.

Essa diferenciação conceitual dos dados pessoais é justamente para que o ordenamento jurídico possa oferecer, através de uma disciplina normativa adequada, uma tutela mais específica para situações em que a possibilidade de risco e de violação é potencialmente maior.

No Considerando 51 do Regulamento Geral de Proteção de Dados da União Europeia, podemos notar a preocupação ali existente em se tutelar de forma específica os dados dessa categoria:

> (51) Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial

> ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas.

Como veremos nos subtópicos abaixo, as bases legais para o tratamento de dados pessoais sensíveis são diferenciadas e limitadas no artigo 11 da LGPD.

Além disso, a proteção dos dados não deve se limitar apenas àqueles processados por meios digitais, na esfera da informática. Pelo contrário, o bem protegido envolve todo e qualquer dado pessoal independentemente do local (banco de dados) e do modo pelo qual é armazenado, se preocupando, na verdade, com o impacto que o uso daquele dado trará na vida do indivíduo e no livre desenvolvimento da sua personalidade (SARLET, 2020, p. 41).

Outro aspecto é que, por estarem atrelados à personalidade do indivíduo, ainda que o titular, voluntariamente, disponibilize seus dados pessoais para terceiros, eles não podem ser desvinculados. Ou seja, a titularidade dos dados permanece com seu titular.

Nesta seara, é importante fazermos uma ressalva: a proteção de dados e o interesse pelo desenvolvimento tecnológico não devem ser vistos como objetivos totalmente contrapostos. É evidente que o aperfeiçoamento dos meios de comunicação, tendo como instrumento a informação, é, hoje, necessário para a vida em sociedade.

Por este motivo, tais elementos devem ser compreendidos como fatores que se reforçam mutuamente, isto é, a proteção de dados é imprescindível para que haja um desenvolvimento mais adequado da sociedade da informação, já que a violação desse direito prejudica a sociedade como um todo.

O direito à proteção dos dados pessoais, como veremos adiante, inaugura uma nova espécie no rol dos direitos da personalidade, dando elasticidade à cláusula geral da tutela da pessoa humana.

2.3.1 Dados pessoais biométricos: conceito e aplicação

Dentre os inúmeros exemplos de dados pessoais sensíveis, optamos, nesta parte da pesquisa, por focar o estudo na categoria dos dados pessoais biométricos, a fim de compreender seu significado, suas características e suas formas de proteção.

Esse entendimento é fundamental para que o leitor, em um segundo momento, possa compreender a problemática que envolve o subtópico deste trabalho destinado ao estudo de caso prático (uso de portas digitais interativas).

Embora não seja recente o uso de traços biológicos e comportamentais para confirmar a identidade de uma pessoa[10], nos dias de hoje, observa-se um crescimento exponencial no número de atividades que se utilizam dos dados biométricos tanto para fins de identificação de indivíduos, quanto para fins de acesso a sistemas e de classificação de usuários. O corpo humano passou a se traduzir em uma "senha".

Frente a esta problemática, inicialmente, no que diz respeito aos dados pessoais biométricos, por corresponderem a um tipo particular de dados, possuem uma definição mais específica, que está detalhada no Decreto nº 10.046/2019, que instituiu o Cadastro Base do Cidadão, o qual prevê em seu artigo 2º, inc. II, o seguinte: são "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar" (BRASIL, 2019).

Referidas características são praticamente imutáveis, e acompanham seu titular ao longo da vida.

Uma das primeiras definições acerca dos "dados pessoais biométricos" foi desenvolvida pelo Grupo de Trabalho de Proteção de Dados que, por sua vez, foi instituído pelo artigo 29.º da Directiva 95/46/CE da União Europeia.

Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e de privacidade. Assim, o "Parecer nº 4/2007 sobre o conceito de dados pessoais" traz uma referência específica sobre aquela categoria de dados:

> Estes dados podem ser definidos como propriedades biológicas, características fisiológicas, traços físicos ou acções reproduzíveis, na medida em que essas características e/ou acções sejam simultaneamente únicas a essa pessoa e mensuráveis, mesmo que os padrões utilizados na prática para medi-las tecnicamente envolvam um certo grau de probabilidade. Exemplos típicos deste tipo de dados biométricos são as impressões digitais, os padrões da retina, a estrutura facial, a voz, mas também a geometria das mãos, os padrões das veias ou mesmo uma habilidade profundamente enraizada ou outra característica comportamental (tal como a assinatura manual, caligrafia, forma particular de andar ou falar, etc...) (...) De facto, devido à sua ligação única com uma determinada pessoa, os dados biométricos podem ser utilizados para identificar a pessoa. Este carácter duplo também surge no caso de dados de ADN que fornecem informação sobre o corpo humano e permitem uma identificação clara e única da pessoa.

[10] Aqui é importante esclarecer que o primeiro sistema biométrico foi desenvolvido por Alphonse Bertillon, chefe da divisão criminal do Departamento de Polícia de Paris no ano de 1883, a fim de identificar indivíduos no âmbito penal. Para tanto, eram utilizados atributos físicos como cor do olho, altura e largura da cabeça, tatuagens, cicatrizes. Era algo muito menos automatizado do que hoje e ficava à mercê de muito mais falhas.

No ordenamento jurídico brasileiro, Maldonado e Blum (2020, p. 88) explicam que os dados biométricos são aqueles "resultados de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa que permitam ou confirmem a identificação única dessa pessoa, notadamente imagens faciais ou dados dactiloscópicos". Esclarece-se que estes últimos equivalem à impressão digital dos indivíduos.

Esse conceito decorre diretamente do que dispõe o art. 4 (14) do General Data Protection Regulation (GDPR), principal legislação europeia sobre a temática da proteção de dados pessoais e que, especificamente em seu art. 4, traz definições importantes, a fim de orientar a compreensão da matéria:

> 4.14 biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (EU, 2016).
>
> Tradução nossa: «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

Neste sentido, conforme definições acima analisadas, os dados biométricos são aqueles que, quando processados por meios técnicos específicos, permitem a identificação inequívoca ou a autenticação de uma pessoa singular, distinguindo-a de forma precisa de todas as demais.

Importante observar que a nossa Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) não define expressamente o termo "dados pessoais biométricos", motivo pelo qual, nesta pesquisa, optamos por trazer o conceito do GDPR, que inspirou a doutrina brasileira.

Um exemplo bastante comum de dado biométrico é a imagem do rosto de um indivíduo. Contudo, essa categoria é bem mais ampla, englobando também os próprios comportamentos de um indivíduo, como sua forma única e particular de andar ou falar (movimentações físicas).

A biometria, por sua vez, corresponde ao ramo da ciência que busca estabelecer a identidade de uma pessoa com base nos atributos físicos únicos, como impressões digitais, face, ou comportamentais como, por exemplo, a dinâmica do caminhar, assinatura (ROSS; JAIN, 2015, p. 289). Para tanto, tal tecnologia utiliza métodos estatísticos, biológicos e tecnológicos, se desenvolvendo através da captura de dados pessoais.

Peck Pinheiro (2013, p. 92) complementa, explicando que a biometria consiste "no uso de características fisiológicas mensuráveis para autenticar um usuário, como impressão digital ou reconhecimento facial".

De forma mais genérica e sucinta, a biometria pode ser compreendida como um conjunto de técnicas para identificar pessoas, a partir de seus próprios dados. Dentre essas técnicas, o autor Roger Clarke (1994, p. 6), enumera as 05 principais: (i) aparência (altura, peso, cor); (ii) comportamento social (estilo da fala, sinais corporais); (iii) biodinâmica (modo de assinar); (iv) fisiografia natural (impressão digital, retina, padrões de DNA); e (v) características física impostas (se utiliza tornozeleira, microchip).

Um sistema que trabalha com biometria costuma utilizar sensores específicos para o fim de capturar a característica biométrica de uma pessoa. Após, tal informação, que identifica ou verifica o usuário, é anexada em um banco de dados, deixando de ser exclusiva de seu ser, para ser conhecida por máquinas e por terceiros que conduzem tal procedimento.

A biometria se diferencia por realizar esse processo a partir de características que praticamente todos os seres humanos possuem (universalidade) e, ainda, pelo fato de que tais características são suficientemente singulares em relação a outros indivíduos em comparação (unicidade). Além disso, é fundamental que esta característica dure determinado período de tempo, a fim de evitar falsas correspondências. É o fenômeno da tradução do corpo para o arquivo de dados, estabelecendo uma representação virtual do indivíduo.

Nesta perspectiva, a pessoa humana passa a ser uma fonte de dados coletados e de conteúdos informacionais. Aquilo que, essencialmente, pertencia exclusivamente ao indivíduo, passa a ser conhecido por máquinas.

Após essa coleta, o sistema biométrico consegue realizar comparações com outros dados futuramente coletados e, a partir destas análises, identificar os indivíduos em determinada situação. Este sistema também é muito utilizado para autenticar usuários de um serviço.

Importante esclarecer que o sistema biométrico serve tanto para identificar um indivíduo, quanto para verificá-lo. A identificação busca uma correspondência entre um indivíduo com um modelo inserido no banco de dados (ou seja, dentre todos, a identificação busca saber exatamente quem é aquela pessoa), enquanto a verificação serve para definir se o dado coletado é compatível com outro previamente cadastrado (ou seja, vem comparar se aquele indivíduo é o mesmo que se está buscando. Por exemplo, quando fazemos o acesso biométrico pelo celular).

A coleta de dados biométricos costuma apresentar um risco de erro muito baixo, motivo pelo qual é um dos tipos de informação que mais leva à identificação do titular.

Por revelarem aspectos que podem levar a uma discriminação do indivíduo ao qual se referem, trazendo, por si só, maior vulnerabilidade ao seu titular, os dados biométricos são

compreendidos no ordenamento jurídico brasileiro, representado sobretudo pela Lei Geral de Proteção de Dados Pessoais como dados pessoais sensíveis. Assim, como vimos no subtópico acima, estes dados merecem proteção ainda mais especial, alicerçada no princípio da dignidade da pessoa humana.

2.4 O reconhecimento facial como técnica de construção de perfis a partir da coleta de dados biométricos

Dentre as inúmeras possibilidades de processamento dos dados pessoais biométricos, optamos, neste trabalho, por estudar as tecnologias de reconhecimento facial.

Nos últimos anos, no Brasil, observou-se um grande crescimento na utilização destas tecnologias, com diferentes finalidades, como, por exemplo, para identificação de pessoas em máquinas, em aplicativos de celulares, no controle de acesso a determinados lugares, entre outros. Uma das vantagens desta aplicação é a possibilidade de se capturar os dados à distância e de forma pouco intrusiva.

De acordo com o Professor Doutor Eduardo Tomasevicius Filho (2021, p. 130), o reconhecimento facial consiste, em síntese, no uso de softwares que buscam identificar automaticamente pessoas ou objetos, por meio da comparação com dados que tenham sido coletados anteriormente e que estejam armazenados em determinado banco de dados.

Assim sendo, esse tipo de tecnologia atua analisando um conjunto de dados específico. Se o algoritmo - desenvolvido exclusivamente para essa finalidade- identifica fortes semelhanças entre o dado capturado e o dado previamente armazenado, ativa-se o comando de reconhecimento.

Neste tipo de tecnologia, utiliza-se, primordialmente, o conjunto de características corporais humanas, com foco na imagem facial de um indivíduo para, posteriormente, em outras situações, poder identificá-lo. A ferramenta base são as características próprias de cada rosto humano, tais como formato do rosto e das maçãs, formato da boca, comprimento e largura do nariz, profundidade dos olhos, entre outros traços da face. Há softwares que conseguem capturar cerca de trinta mil características da face de uma pessoa, a fim de compará-las com outras disponíveis no banco de dados.

O Professor Eduardo Tomasevicius Filho, na mesma obra (2021, p. 130), traz como exemplo para que o leitor possa compreender melhor como as tecnologias de reconhecimento facial atuam as atividades de perícia grafotécnica. Em ambas as situações, é feita uma

comparação entre uma informação coletada previamente com uma posterior. Analisa-se, por exemplo, pontos, traços, formas, com o intuito de verificar se são compatíveis entre si.

O reconhecimento, portanto, é feito por semelhança, tendo como resultado a resposta "mais provável", como se fosse uma média ponderada. Quanto mais favoráveis as condições do ambiente em que o software atua, como iluminação, resolução, mais prováveis serão as respostas.

Isto posto, é importante, desde já, compreender que esses sistemas não são "perfeitos", mas estão sujeitos a erros e falhas no processamento de dados, uma vez que os algoritmos de inteligência artificial podem, eventualmente, podem coletar ou interpretar os dados de forma equivocada. A exemplo desta problemática, temos o falso negativo, que é quando ocorre falha em identificar uma face na imagem. Por outro lado, existe o falso positivo, que é quando o algoritmo identifica uma face onde não há uma ou, ainda, quando identifica uma pessoa, quando, na verdade, se trata de outra. Esses erros podem ser influenciados pelo fundo captado, a iluminação, o sombreamento local, entre outros fatores.

A fim de complementar o exposto acima e compreender ainda melhor a forma que esta tecnologia opera, analisamos um material produzido pelo "Information Commissioner's Opinion (ICO)", órgão do Departamento de Digital, Cultura, Mídia e Esporte do Reino Unido.

Hoje, a legislação e as autoridades do Reino Unido são uma das principais referências em matéria de proteção de dados pessoais. Além de possuírem uma base legal sólida, com fundamentos detalhados e bastante explicativos, eles se preocuparam em regulamentar, por meio de guias, algumas dúvidas e questões práticas que têm aparecido sobre dados pessoais (UK, 2021).

De acordo com o "Information Commissioner's Opinion (ICO)", as tecnologias de reconhecimento facial consistem em um instrumento que identifica ou reconhece um indivíduo a partir de sua imagem digital. Esse reconhecimento não se dá por identidade, mas por semelhança, de forma que os resultados não consistem em uma resposta certa, mas na mais provável (juízo de probabilidade, e não de certeza).

Neste sentido, para que possam realizar o objetivo ao qual se propõem - identificar o sujeito ou objeto-, os softwares de reconhecimento facial são dotados de algoritmos de inteligência artificial desenvolvidos especificamente para analisar dados biométricos.

O principal instrumento usado nas tecnologias de reconhecimento facial são as câmeras digitais, que servem para capturar a imagem e, assim, efetuar diretamente a coleta dos dados pessoais biométricos.

A fim de detalhar melhor este procedimento, esclarece-se o seguinte: as câmeras digitais são atreladas a um software específico de reconhecimento facial biométrico que, dotado de elementos de inteligência artificial, como algoritmos, é programado para analisar estes dados e medir as características por ele apresentadas. Após, o próprio software produz um modelo biométrico do indivíduo. Esse modelo é armazenado no próprio software a fim de que ocorra uma retroalimentação contínua do sistema (TOMASEVICIUS FILHO, 2021, p. 134).

Este procedimento permite que o usuário identifique, autentique ou verifique ou categorize indivíduos.

Hoje, com o avanço da tecnologia, é possível que este reconhecimento facial ocorra em tempo real, captando simultaneamente os dados dos indivíduos que passam por uma câmera e, ainda, em grande escala e alcance.

Muitas vezes esses processos também contam com uma intervenção humana, que atua para avaliar se a correspondência realizada pelo algoritmo entre os dados biométricos coletados e a pessoa a que os dados se referem está correta.

Com isso, criam-se os chamados perfis digitais dos indivíduos que, em um segundo momento, podem ser utilizados para finalidades distintas, como para autenticar um serviço, categorizar um grupo por faixa etária, entre outras. Assim sendo, nos dias atuais, os dados biométricos extraídos a partir da imagem facial conseguem identificar o indivíduo em uma variedade de contextos de forma única e precisa.

Essa técnica é conhecida como “perfilamento” ou “profiling” que, nas palavras de Doneda (2006, p. 173) consiste justamente na criação de perfis de pessoas a partir de suas informações pessoais anteriormente coletadas. É como um “avatar” que representa o titular a partir da coleta de seus próprios dados.

Assim, neste processo, são tratadas as características do indivíduo, formando um “mapa de características” que, por sua vez, é utilizado como base para se fazer previsões acerca de futuros comportamentos do titular.

Além disso, a técnica de perfilamento permite que se conheça cada vez mais seus hábitos, costumes, hobbies e interesses.

Neste ponto, é importante fazer uma ressalva: dependendo da forma que são desenvolvidos, os algoritmos podem trazer resultados discriminatórios em relação àquelas pessoas que não corresponderem ao “modelo geral”.

Assim, a inteligência artificial pode acabar reproduzindo desigualdades existentes na sociedade e fomentar preconceitos. Por isso, é fundamental que os sistemas que utilizam

algoritmos sejam constantemente testados e avaliados, a fim de evitar a estigmatização de minorias e, principalmente, de obstaculizar o desenvolvimento da individualidade e da personalidade de cada um.

Este tipo de tecnologia, por si só, possui natureza potencialmente intrusiva nos direitos e nas liberdades fundamentais dos indivíduos, que, na maioria das vezes, não tem consciência ou escolha no processo, motivo pelo qual o uso do reconhecimento facial exige maior cuidado e responsabilidade dos seus controladores, sobretudo em matéria de privacidade e de proteção de dados pessoais, a fim de resguardar os direitos de todos os envolvidos.

Como veremos nos subtópicos abaixo, hoje, no ordenamento jurídico brasileiro não existem garantias preventivas acerca do mal uso dessa tecnologia, de maneira que, muitas vezes, os dados pessoais biométricos são coletados por câmaras e por softwares de reconhecimento facial sem que haja qualquer tipo de controle e, pior, sem que o titular possa fornecer seu consentimento a referido tratamento.

Essa situação se agrava ainda mais quando nos deparamos com as câmaras alocadas em espaços públicos, uma vez que, nestes ambientes, é muito mais difícil exercer qualquer tipo de controle em relação ao que efetivamente está sendo coletado, sendo que o titular, na maioria das vezes, sequer tem conhecimento de que seus dados pessoais estão sendo tratados e armazenados. Desta maneira, a própria liberdade do titular é comprometida.

Assim, embora a tecnologia seja promissora e, muitas vezes, facilite as questões cotidianas referentes à identificação de indivíduos, o reconhecimento facial jamais deve ser utilizado como um meio 100% (cem por cento) seguro e justo. É fundamental que, atrelado ao uso desta tecnologia, a parte por ela responsável, desenvolva procedimentos que garantam o máximo de precisão e a transparência do sistema, minimizando os riscos inerentes a ele.

Atualmente, está em tramitação na Câmara dos Deputados, o Projeto de Lei 4.612/2019, o qual "dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos". Em seu art. 3º, reconhece que as tecnologias de reconhecimento facial e emocional pertencem à categoria de dados pessoais sensíveis.

A intenção do PL é justamente desenvolver um marco regulatório que possa garantir um uso legítimo desse tipo de tecnologia, a fim de que ela seja implementada de forma responsável, preservando a privacidade e a liberdade dos cidadãos.

2.5 O uso das tecnologias de reconhecimento facial como estratégia de direcionamento de publicidade

Podemos observar que, hoje, o uso de tecnologias de reconhecimento facial alterou as lógicas de mercado, trazendo novas formas de estratégias de marketing e de se veicular os anúncios publicitários.

Neste sentido, as técnicas de perfilamento, estudadas no subtópico acima, passaram também a ser aplicadas no ambiente da publicidade que, de acordo com Martins e Basan (2021, p. 342) é "toda informação que visa, em última análise, criar no público a vontade e a necessidade de consumir, mesmo que de maneira indireta".

Explica-se que, nestas situações, os agentes de tratamento coletam dados pessoais dos futuros consumidores com o intuito de compreender e de traçar o "perfil de consumo" de cada indivíduo. Após, a partir de uma análise minuciosa dos dados, por meio de um algoritmo desenvolvido exclusivamente para essa finalidade, o agente consegue ofertar os produtos e serviços que sejam do interesse de determinado sujeito.

No tocante especificamente ao uso de tecnologia de reconhecimento facial, por meio de câmeras de vídeo instaladas em lugares específicos, como portas, outdoors, é possível que os agentes de tratamento coletem dados pessoais de diferentes titulares, inclusive dados pessoais sensíveis, e os processem com a finalidade de medir o envolvimento dos sujeitos com os anúncios publicitários vinculados naquela localização - ou seja, por quanto tempo os indivíduos observam o anúncio, como reagem a ele (se gostam, não gostam).

Assim, a partir dos dados coletados por meio de reconhecimento facial, o agente de tratamento consegue identificar desejos, necessidades e comportamentos dos sujeitos. Até mesmo suas emoções são identificadas pelos sensores.

A esse respeito, segundo Darren Bridger (2018, p. 19), hoje alguns softwares conseguem até medir batimentos cardíacos e detectar flutuações, ainda que minúsculas, na expressão facial dos indivíduos, a fim de interpretar suas reações ao que estiver sendo vinculado na tela.

Atrelado a este uso, após a coleta e a análise dos resultados, os agentes controladores também compreendem melhor sua audiência, por meio de uma categorização dos indivíduos em critérios como idade e gênero.

Com todas as informações coletadas e armazenadas, o agente de tratamento passa a direcionar os novos anúncios publicitários de acordo com o interesse dos indivíduos que circulam no ambiente e até fornecer experiências mais interativas entre o anúncio e as partes

circulantes. A Internet, neste contexto, oferece inúmeras possibilidades de trabalho com sons, imagens e sensações.

Assim, como bem sintetiza Leonel (2022, p. 27) as informações contidas nos bancos de dados são transformadas em um verdadeiro conhecimento para aqueles que operam as campanhas de marketing, com o objetivo de induzir seu público ao consumo de produtos e de serviços.

É a chamada publicidade direcionada e personalizada, feita justamente para influenciar a decisão do usuário do serviço. Isto tudo, certamente, sem que o titular dos dados tenha qualquer conhecimento sobre o procedimento.

Um exemplo desta problemática envolvendo as estratégias de marketing e de publicidade, por meio da coleta de dados pessoais biométricos, é o caso envolvendo as Portas Digitais Interativas da linha amarela do metrô de São Paulo - que ainda está em trâmite no Tribunal de Justiça do Estado de São Paulo e será objeto de estudo de caso específico nesta pesquisa, no subtópico nº 4.

Assim, apenas para contextualizar brevemente, naquela situação foi denunciado que a ViaQuatro, concessionária do metrô, estaria utilizando dados pessoais biométricos, coletados por meio de reconhecimento facial, para obter insight e fornecer produtos publicitários.

Os riscos aos direitos fundamentais do titular, nestes casos, são imensos, uma vez que o sujeito acaba sendo manipulado pelos agentes de tratamento, tendo sua autonomia de vontade totalmente prejudicada, sem que sequer saiba que isso está ocorrendo.

Assim, é mister que se tracem limites regulatórios para a publicidade que envolva o tratamento de dados pessoais, tendo a promoção da personalidade e da dignidade da pessoa humana como fundamento, a fim de que aquela não seja abusiva e enganosa.

3 O DIREITO À PROTEÇÃO DE DADOS PESSOAIS

A terceira subseção busca justamente analisar uma das problemáticas principais deste trabalho: as novas perspectivas do direito à privacidade e como, hoje, este direito também é compreendido como um direito do titular a ter controle sobre as próprias informações e, assim, possui ligação direta com o direito à proteção de dados pessoais.

Na segunda parte da presente subseção, pretende-se verificar a inserção da proteção de dados como um direito da personalidade, de acordo com os conceitos estudados na subseção anterior, e quais as consequências dessa compreensão na perspectiva infraconstitucional.

Diante desta problemática, será feito um estudo específico sobre a Lei Geral de Proteção de Dados Pessoais- LGPD, de nº 13.709/2018, a qual entrou em vigor em setembro de 2020, como fruto de inúmeros debates legislativos e doutrinários, com vistas a internalizar uma disciplina específica de proteção de dados pessoais no ordenamento jurídico brasileiro.

Pretende-se analisar os principais conceitos da lei, seus princípios e fundamentos, com o intuito de, na próxima subseção, podermos compreender como pode ocorrer, no caso concreto, a violação ao direito à proteção de dados pessoais. A Lei reconhece a assimetria de poder entre os titulares de dados e aqueles que realizam seu tratamento, dentre os quais, os atores privados, foco deste trabalho.

Por fim, buscaremos analisar o direito à proteção de dados pessoais em uma perspectiva constitucional, isto é, como um direito fundamental e quais os impactos desta nova compreensão. Para tanto, estudaremos, brevemente, a decisão proferida pelo Supremo Tribunal Federal no julgamento das Ações Diretas de Inconstitucionalidade nº 6387, 6388, 6389, 6390 e 6393, bem como a Proposta de Emenda à Constituição (PEC) 17/2019, aprovada recentemente pelo Senado.

3.1 O direito à privacidade como controle sobre as informações pessoais

Tendo em vista os desafios trazidos pela sociedade da informação, que geraram novas formas de exposição- sequer pensadas anteriormente- e de abuso de direito em razão do tratamento inadequado de dados, as noções tradicionais de privacidade mostraram-se insuficientes e inadequadas, demandando do operador do Direito um cuidado em desenvolver novos instrumentos para a proteção da pessoa humana no âmbito de sua personalidade.

Uma das preocupações, inclusive, foi com o uso de dados pessoais pelas grandes corporações que frequentemente coletam e processam dados e, desta forma, por terem mais poder econômico, conseguem adquirir modernas tecnologias da informação e, desta forma, podem exercer um controle ainda maior sobre os cidadãos.

Além disso, esse fluxo mais intenso de informações permitia que diversas parcelas da população tivessem sua privacidade invadida, e não apenas aqueles sujeitos considerados de "grande relevo social" (DONEDA, 2006, p. 91).

É neste contexto complexo que ganha relevância um novo aspecto do direito à privacidade, do qual deflui a disciplina da proteção de dados pessoais, que, portanto, é resultado das modificações sociais e tecnológicas trazidas no século XX, sobretudo com a chegada da internet que, como vimos, expandiu as possibilidades de comunicação e de trocas de informações, resultando em novas questões conflituosas relacionadas à privacidade.

Vale destacar que, paralelamente, também ocorria uma transformação da própria função do Estado, cada vez mais garantidor de direitos - Welfare State.

A privacidade está cada vez mais se distanciando de seu conceito inicial, ligada ao direito de ser deixado só, para ser considerada sob a perspectiva da atual sociedade da informação e sob as novas formas de organização de poderes. É um contexto complexo, que envolve as mais diversas situações que trazem consequências diretas para os cidadãos.

Assim, ao falar de privacidade nos aproximamos do direito de o cidadão apenas revelar ao mundo aquilo que deseja, tendo mais controle sobre suas informações pessoais. Isto porque o acesso a dados pessoais, por mais discreto que seja, poderá trazer graves implicações sobre a privacidade do sujeito. Ora, a privacidade não pode ser apropriável e circulável, mas deve ser protegida, a fim de proteger, em último nível, a dignidade humana (ABADE, ALVES, 2017, p. 119).

Historicamente, ganha relevância a decisão do Tribunal Constitucional alemão, no julgamento do caso Volkszahlung, que teve como pano de fundo a "Lei do Recenseamento de População, Profissão, Moradia e Trabalho" de 25 de março de 1982.

A referida Lei tinha como objetivo efetuar um recenseamento da população, com dados sobre a profissão, moradia e local de trabalho, por meio da coleta de dados pessoais. O caráter do tratamento de dados, portanto, era, supostamente, estatístico.

Contudo, a lei também previa a possibilidade de que os dados coletados fossem comparados com outros já levantados em registros públicos e, ainda, que fossem transferidos de forma anônima para repartições públicas (MARTINS, 2016, p. 55)

Em razão do conteúdo da lei, foram ajuizadas contra ela diversas Reclamações Constitucionais, mediante a alegação de que ela teria violado diretamente alguns direitos fundamentais dos reclamantes, sobretudo o direito ao livre desenvolvimento da personalidade.

Na decisão paradigma[11], o Tribunal alemão mostrou pela primeira vez uma preocupação com a temática da proteção de dados, ao reconhecer que todas as informações coletadas, independentemente de serem íntimas, privadas ou públicas, são importantes e, ainda, que todos os dados existentes em nossa sociedade têm um valor, não existindo, portanto, dados insignificantes.

Isto porque o tratamento de quaisquer desses dados poderia trazer riscos à personalidade de seu titular. Em virtude deste posicionamento, o Tribunal declarou nulos todos os dispositivos que fizessem referência à transmissão de dados.

Foi nessa mesma decisão que se articulou o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade, que culminou no direito fundamental à autodeterminação informativa, oponível em face do Estado, e vinculado ao direito "geral" da personalidade, também tutelado naquele ordenamento (SCHWABE, 2005, p. 240).

Neste sentido, para o Tribunal alemão, a capacidade do indivíduo de autodeterminar seus dados pessoais, ou seja, de decidir se e como gostaria de fornecer seus dados, é parcela fundamental do próprio direito do indivíduo de desenvolver livremente sua personalidade.

Em síntese, foi neste momento que se percebeu, ainda que de forma sutil, que um tratamento de dados pessoais de forma ilimitada poderia gerar danos ao livre desenvolvimento da personalidade, razão pela qual deveria se pensar em instrumentos jurídicos voltados para esta tutela específica.

Stefano Rodotà articula a ulterior definição do direito à privacidade como "o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada" e, ainda, como direito de "conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas" (RODOTÀ, 2008, p. 92). Ele resume

[11] Nos termos do acórdão proferido pela corte alemã: "(...) esse poder [do uso de dados] necessita, sob as condições atuais e futuras do processamento automático de dados, de uma proteção especialmente intensa. Hoje, com ajuda do processamento eletrônico de dados, informações detalhadas sobre relações pessoais ou objetivas de uma pessoa determinada ou determinável (...) podem ser, do ponto de vista técnico, ilimitadamente armazenados e consultados a qualquer momento, a qualquer distância e em segundos. Além disso, podem ser combinados, sobretudo na estruturação de sistemas de informação integrados, com outros bancos de dados, formando um quadro da personalidade relativamente completo ou quase, sem que a pessoa atingida possa controlar suficientemente sua exatidão e seu uso. Com isso, ampliaram-se, de maneira até então desconhecida, as possibilidades de consulta e influência que podem atuar sobre o comportamento do indivíduo em função da pressão psíquica causada pela participação pública em suas informações privadas" (MARTINS, 2005, p. 237).

o novo âmbito do direito à privacidade no seguinte eixo "pessoa-informação-circulação-controle"[12].

Além disso, conforme Vieira (2007, p. 305) o direito à privacidade também se estende para compreender o direito de não ser monitorado, não ser registrado e de não ser reconhecido, sendo que este último está relacionado ao fato de que o cidadão não pode ter, simplesmente, seus registros pessoais expostos e publicados, mas cabe a ele determinar quais atributos de si poderão ser usados por outros. Vinculado a este último está o direito de o sujeito não ser discriminado com base nas informações existentes sobre ele.

A privacidade, portanto, passa a estar relacionada com os conceitos de autonomia, autodeterminação e empoderamento dos titulares de dados, a fim de que estes não sejam submetidos a qualquer forma de controle social. É o indivíduo que então decide quando, como e onde serão dados poderão circular. Ela passa a ter uma dimensão positiva, no sentido de que o legislador e os demais agentes de tratamento de dados atuem com o intuito de proteger as garantias referentes à circulação de dados e, desta forma, ao desenvolvimento da personalidade.

Assim, a privacidade que antes era vista apenas como espaço de não interferência na esfera privada- dimensão negativa-, em que bastava tão somente garantir o direito de recusa ou proibição do titular para que terceiros não tivessem acesso a seu espaço, passa a incluir uma tutela mais proativa no sentido de garantir ao titular mais conhecimento e, principalmente, mais controle sobre os elementos referentes ao tratamento de seus dados, inclusive quando estes já estivessem sendo controlados por terceiros- dimensão positiva.

Sob essa perspectiva, em síntese, o direito à privacidade precisa assegurar: (a) transparência do processamento de dados, sem a qual não é possível sequer se proteger contra os riscos do processamento; (b) conhecimento e acesso do titular aos dados armazenados; e (c) possibilidade de correção e cancelamento dos dados (MENDES, 2014, p. 133).

Nesta seara, nos deparamos com o conceito de "autodeterminação informativa", que coloca o indivíduo titular dos dados como o protagonista das matérias e das decisões que dizem respeito ao tratamento das informações que lhe são relativas.

Somente o indivíduo pode determinar o âmbito de sua privacidade, ou seja, ele define em que medidas as informações que lhe dizem respeito poderão ser utilizadas. Assim, de forma atrelada ao controle, existe o próprio exercício de liberdade do titular, relacionado, sobretudo, à possibilidade de escolha e de construção da esfera pessoal.

[12] Antes desse entendimento, a privacidade, para Rodotá, era compreendida como "pessoa-informação-sigilo".

Diante desta nova problemática é que Sarlet (2020, p. 25) aponta para o surgimento, ainda que de forma implícita, do chamado direito à proteção de dados pessoais. Para o autor, este direito é amplo e engloba desde o direito de acesso e de conhecimento acerca dos dados salvos em banco de dados, bem como o direito de conhecimento sobre os responsáveis pelo tratamento, sobre a finalidade das operações, e, ainda de, eventualmente, impedir ou excluir referido tratamento por terceiros.

Assim sendo, o direito à proteção de dados pessoais surge como um nexo de continuidade da disciplina da privacidade, sendo uma espécie de herdeiro desta, já com características próprias, voltadas para as demandas da sociedade atual, no sentido de controlar a exposição de sua vida pessoal e a disponibilidade das informações que lhe dizem respeito. É o titular quem decide a quem, onde e em que condições divulgará suas informações.

Nos dias atuais, esse direito já se consolida como um direito autônomo, a partir da constatação de que já existem situações de fato que ensejam proteção legal específica, justamente por envolverem o tratamento puro e simples de dados pessoais (PECK, 2013, p. 82).

A proteção de dados pessoais como forma de proteção da privacidade passa a ser cada vez mais necessária para que o indivíduo possa construir uma esfera privada própria, já que praticamente tudo que aquele faz, sente, pode ser registrado em um dado. Por esta razão, é importante não confundir tais institutos, embora, como veremos, eles podem, muitas vezes, se tangenciar.

Nesta seara, um instituto de suma importância é o consentimento para o tratamento de dados pessoais. Ele representa a autonomia privada, uma forma de manifestação do titular a respeito de suas escolhas e de suas vontades, no exercício de sua liberdade. O consentimento é, portanto, o ponto de referência de toda a nova tutela em torno do direito à privacidade.

Bioni alerta que, além do controle e do consentimento do titular em relação ao tratamento de seus dados, é importante assegurar que o fluxo informacional atenda às suas legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade (2021, p. 68).

Por outro lado, esta nova configuração do direito à privacidade como direito à proteção de dados pessoais também apresenta uma dimensão coletiva, perpassando a esfera meramente individual, mas trazendo consequências na relação entre o indivíduo e o mundo exterior, já que vários interesses e direitos se conectam. Assim, é necessário buscar o equilíbrio entre a proteção adequada da privacidade e dos dados pessoais com os interesses da sociedade e da economia, que utilizam estas informações para seu desenvolvimento.

Em síntese, a noção da privacidade, hoje, abrange a noção de proteção de dados pessoais, trazendo novos contornos sobre a discussão envolvendo a coleta de informações e a tutela do indivíduo, titular dos dados.

No Estado Democrático de Direito, este novo paradigma relacionado ao direito à privacidade aparece como condição para o exercício de outras liberdades fundamentais e da própria cidadania, se tornando um dos fundamentos do Estado (DONEDA, 2006, p. 90), e propõe uma reflexão acerca da necessidade da proteção da pessoa humana como um todo, guiada pelo princípio da dignidade da pessoa humana, valor axiológico máximo do ordenamento jurídico brasileiro.

3.2 Perspectiva infraconstitucional: inserção da proteção de dados como direito da personalidade

Como vimos, a principal função dos direitos da personalidade é justamente promover uma proteção jurídica direcionada para o desenvolvimento da pessoa humana. Tal perspectiva abre caminho para o reconhecimento da proteção dos dados pessoais como um direito da personalidade com seus próprios contornos, a fim de atender aos desafios trazidos pela sociedade da informação e pelo uso das novas tecnologias.

Adotando o conceito de Bioni (2020, p. 78) segundo o qual a "personalidade significa as características ou o conjunto de características que distingue uma pessoa da outra", os dados, atrelados à esfera de uma pessoa, fazem parte de sua personalidade, como uma dimensão de seu titular.

Assim sendo, por representarem parte da personalidade do indivíduo, os dados pessoais merecem tutela, o que justifica sua inserção dentre os direitos da personalidade, a fim de que, desta forma, possa também se assegurar outros direitos fundamentais do cidadão, como o da liberdade, da igualdade e da privacidade.

Além de representarem um prolongamento da personalidade, os dados pessoais também refletem aspectos sociais e relacionais do indivíduo, ou seja, sua relação com a sociedade. Isto posto, entender o direito à proteção de dados pessoais como direito da personalidade implica em permitir que o sujeito possa se desenvolver livremente na sociedade em que ele se insere.

Como vimos nos tópicos anteriores, a personalidade civil começa do nascimento com vida. Assim sendo, em relação ao direito à proteção de dados pessoais, qualquer pessoa, a partir do momento que nasce com vida, automaticamente já possui os direitos tutelados pela LGPD. Ademais, tendo em vista que o ordenamento brasileiro põe a salvo, desde a concepção, os

direitos do nascituro, a tutela dos dados pessoais já é protegida neste momento, em razão de sua personalidade jurídica (MALDONADO; BLUM, 2020, p. 107).

Na legislação infraconstitucional, o instrumento que mais tem relevância sobre a tutela da proteção de dados pessoais é a Lei Geral de Proteção de Dados Pessoais, a qual será abordada com detalhes no próximo subtópico. Ela surgiu como resposta para as demandas da sociedade da informação e da economia movidas a dados pessoais, com o intuito de fornecer poder e controle ao titular.

Ademais, a LGPD foi sancionada para que o Brasil pudesse ter um sistema mais sólido de proteção de dados e, assim, conseguisse negociar com outros países, sobretudo os países da União Europeia que, por estarem se preocupando cada vez mais com a matéria, tem exigido dos países que queiram negociar com eles uma proteção de dados pessoais efetiva e concreta, sob pena de não permitirem o envio de informações de seus cidadãos.

Antes da LGPD, o Código de Defesa do Consumidor, Lei nº 8.078/90, já trazia, em seu artigo 43, a enumeração de alguns direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros":

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> (...)
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

Ainda no tocante ao Código de Defesa do Consumidor, hoje está em trâmite o Projeto de Lei nº 3.514/15, o qual pretende alterar a Lei nº. 8.078/90 e, dentre outras disposições, busca incluir como direito básico do consumidor "a privacidade e a segurança das informações e dados pessoais prestados ou coletados, por qualquer meio, inclusive o eletrônico, assim como o acesso gratuito do consumidor a estes e a suas fontes".

Posteriormente, a Lei de Acesso à Informação (Lei nº 12.527/2011) trouxe o conceito de informação pessoal, estabelecendo, no inc. IV de seu art. 3º, que "informação pessoal é

aquela relacionada à pessoa natural identificada ou identificável", conceito que, após, foi incorporado na LGPD.

A Lei de Acesso à Informação também levantou a importância de que o tratamento das informações do indivíduo seja realizado respeitando os demais direitos da pessoa, como a vida privada, a intimidade, como bem definiu no art. 31: "tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais".

Outro instrumento que muito contribuiu para a consolidação de uma legislação própria sobre a matéria de proteção de dados pessoais, foi a Lei nº 12.965/2015, conhecida como Marco Civil da Internet, a qual surgiu com o objetivo de tentar regulamentar o espaço virtual. Dentre os princípios da internet no Brasil, o Marco Civil apontou, no inciso III do seu artigo 3º, a proteção de dados pessoais (FRAZÃ; TEPEDINO; OLIVA, 2019, p. 27)..

Ademais, o Marcos Civil traz, em seu artigo 7º, alguns incisos cuja matéria envolve justamente o âmbito da proteção de dados, como, por exemplo, o direito do usuário de ter acesso a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais; o direito de consentir com eventual coleta e armazenamento de seus dados; a exigência de que as informações sejam utilizadas apenas para finalidades que justifiquem sua coleta, não estejam vedadas pela legislação e, ainda, especificadas em contratos.

Por fim, importante pontuar que, nos dias atuais, está em trâmite no Senado o Projeto de Lei n° 21, de 2020 que, embora traga princípios e diretrizes bastante semelhantes ao teor da LGPD, traz algumas disposições mais especificamente voltadas para a inteligência artificial. Este PL, em síntese, estabelece fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil, frente a seu uso cada vez mais frequente na sociedade.

Um dos princípios trazidos no Projeto de Lei nº 21/20 é justamente a privacidade e a proteção de dados pessoais. De acordo com as disposições do Projeto, quaisquer sistemas de inteligência artificial que tratem dados pessoais deverão observar o previsto na Lei nº 13.709/2018.

Frente a esta problemática, nota-se que a geração atual de normas envolvendo proteção de dados pessoais se preocupa não apenas em fazer frente ao poder estatal, como também ao poder privado, como, por exemplo, as empresas da economia da informação, com o objetivo de se disciplinar as circunstâncias do tratamento de dados e fornecer ao cidadão um maior poder de controle sobre seus próprios dados.

3.3 Visão panorâmica da Lei Geral de Proteção de Dados Pessoais

A Lei nº 13.709/2018 é um marco legal de grande impacto para o ordenamento jurídico brasileiro, por consolidar as normas referentes ao tema da proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações, por qualquer meio, inclusive digital, seja por pessoa natural, seja por pessoa jurídica, atingindo um nível de proteção de dados inclusive em âmbito internacional (PECK, 2020, p. 69).

Esta lei está dividida em 10 (dez) capítulos, com 65 (sessenta e cinco) artigos, buscando sistematizar toda a problemática relacionada ao tratamento de dados pessoais, trazendo ainda institutos novos e próprios da matéria.

No geral, a Lei Geral de Proteção de Dados Pessoais se caracteriza por ser uma norma de caráter mais principiológico, ao apresentar conceitos, princípios, direitos e obrigações relacionados ao uso de dados pessoais, de maneira que exige uma aplicação procedimental dentro dos modelos de negócios empresariais (PECK, 2020, p. 40).

O fato de prevalecer, no âmbito da LGPD, princípios em detrimento das regras ocorre justamente para acompanhar as mudanças tecnológicas e a busca por soluções práticas e rápidas, que satisfaçam o dinamismo que a matéria de proteção de dados pessoais envolve.

É também uma lei de governança, uma vez que sugere políticas e padrões de boas práticas para uma efetiva proteção de dados.

Seu âmbito de aplicação é muito amplo, justamente para permitir a proteção de dados pessoais dos indivíduos em um maior número de circunstâncias possíveis.

Também podemos dizer que a lei é cultural, pois reflete os principais anseios do tema em cada ordenamento jurídico. Ela procura implementar uma cultura de privacidade e de proteção de dados no país, de forma inovadora, voltada tanto para os titulares de dados, a fim de que estes estejam mais conscientes de seus direitos, e aos agentes de tratamento, para que realizem as operações envolvendo os dados pessoais de maneira coerente.

A LGPD parte do reconhecimento de que existe uma assimetria de poderes entre os titulares de dados pessoais e os agentes de tratamento - entidades privadas e Poder Público, uma vez que, na maior parte das situações, são estes quem detém maior acesso à informação que está sendo circulada ou tratada. Assim, diante do poder que a informação hoje representa, fica evidente que aqueles que possuem maior acesso à ela, terão mais poder.

Frente a esta situação, a lei surge para reconhecer que, na economia informacional, é fundamental estabelecer limites e contornos sobre este tratamento de dados a fim de que se encontre um equilíbrio entre a satisfação dos interesses dos agentes e a preservação dos direitos

dos titulares, os quais jamais devem ser vistos como valores totalmente contrapostos, mas como elementos que se reforçam mutuamente (WIMMER, 2018, p. 286).

Neste sentido, a lei está amparada na ideia central de que o indivíduo, titular dos dados, tenha conhecimento e controle sobre a coleta e o processamento de suas informações (KLEE, PEREIRA NETO, 2019, p. 16).

Importante esclarecer que a lei não protege dados de pessoas jurídicas.

A LGPD, logo em suas disposições preliminares, esclarece seu objetivo que, nos termos do art. 1º é "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural".

No mesmo sentido, o artigo 2º preconiza como fundamento da disciplina da proteção de dados, dentre outros, o respeito à privacidade (inc. I), os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (inc. VII).

Assim, a lei geral de proteção de dados pessoais se firmou como uma das formas mais eficazes de proteger a privacidade. Nota-se, neste ponto, uma correspondência - explícita e/ou implícita- com os próprios fundamentos da Constituição Federal, decorrentes do princípio da dignidade da pessoa humana.

Os fundamentos dizem respeito à causa e à razão de ser de algo (MALDONADO; BLUM, 2020, p. 17). A partir desta perspectiva, eles têm o intuito de trazer uma base para que se estabeleça um equilíbrio entre o desenvolvimento tecnológico e econômico com a inviolabilidade dos direitos do indivíduo. Assim, os fundamentos induzem à ideia de que qualquer limitação aos direitos deve ser feita de maneira moderada.

Isto posto, a partir do momento que a LGPD fundamenta sua existência no livre desenvolvimento da personalidade e na dignidade, verifica-se uma preocupação da lei em refletir fielmente a personalidade do titular a que os dados pessoais se referem.

Refletindo este caráter principiológico da lei, nos deparamos com o art. 6º, o qual informa os principais princípios pelos quais as atividades de tratamento legítimo, específico e explícito de dados pessoais deverão ser pautadas: finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas.

Para Wimmer (2021, p. 280), os princípios servem justamente para limitar de forma objetiva a extensão do tratamento de dados. Eles são decorrência da eficácia jurídica dos direitos fundamentais nas relações privadas, motivo pelo qual devem ser aplicados como parâmetro

para qualquer tratamento de dados, com o intuito de se evitar lesões aos direitos da personalidade dos indivíduos e contribuir para a promoção da dignidade da pessoa humana.

A LGPD também inova ao trazer conceitos importantes sobre a temática de proteção de dados pessoais, a fim de contribuir com a interpretação e a aplicação do seu conteúdo.

Nesta seara, a LGPD ainda esclarece quem são os titulares de dados, como todas as pessoas naturais identificadas e identificáveis a quem se referem os dados pessoais que são objeto de algum tratamento. Isto posto, a preocupação trazida pela lei não atinge diretamente dados de pessoas jurídicas ou outras informações, como fórmulas, segredos de negócios, patentes, que não estejam relacionadas à pessoa natural (MALDONADO; BLUM, 2020, p. 22).

Nesta seara, de acordo com o art. 5º, inc. X[13], o tratamento consiste em toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, entre outras, desde que a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Importante, aqui, fazer uma ressalva: conforme previsto no art. 4º [14] da Lei nº 13.709/2018, a LGPD não incide em determinada relação jurídica se o tratamento de dados pessoais ali for realizado exclusivamente para fins particulares e não econômicos; ou, ainda, para fins jornalísticos, artísticos ou acadêmicos, segurança pública; defesa nacional; segurança do Estado; ou em atividades de investigação e repressão de infrações penais; ou, por fim, quando o tratamento ocorrer fora do território nacional e não for objeto de comunicação, uso

---

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

[14] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
II - realizado para fins exclusivamente:
a) jornalístico e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;
III - realizado para fins exclusivos de:
a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou
d) atividades de investigação e repressão de infrações penais; ou
IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.
§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados.

Sob a ótica da LGPD, os destinatários do direito, isto é, aqueles que deverão observá-lo e respeitá-lo, são o Estado e os particulares, pessoas físicas ou jurídicas, pois são estes que realizam o tratamento de dados nas mais diversas atividades cotidianas. Neste ponto, importante destacar que a pessoa jurídica, a partir do momento que adquire personalidade, estará apta a responder pelo cumprimento das disposições da LGPD.

A Lei ainda apresenta no art. 5º quem são os agentes de tratamento de dados. São eles: os controladores, os operadores e os encarregados.[15] Cada operação envolvendo um tratamento de dados pessoais terá seus agentes, de forma que uma pessoa poderá, em determinada situação, atuar como controladora e, em outro caso, como operadora.

Os controladores, em síntese, são aqueles sujeitos que tomam as decisões a respeito do tratamento de dados.

Na prática, é o controlador quem determina os elementos essenciais do tratamento, como, por exemplo, as finalidades para as quais os dados estão sendo coletados, o tempo e as condições nas quais serão armazenados ou, eventualmente, compartilhados e, por fim, as formas de eliminação. Ademais, é o controlador que fundamenta o tratamento em uma das bases legais previstas (MALDONADO; BLUM, 2020, p. 103). Neste sentido, o controlador também é responsável por instruir os operadores sobre como o tratamento de dados deverá ser realizado.

Os operadores, por sua vez, são os sujeitos que realizam algum tratamento de dados pessoais, conforme o interesse e as finalidades já determinados pelo controlador, agindo sob o comando deste. Cabe aos operadores tão somente a definição de elementos não essenciais do tratamento, como, por exemplo, o detalhamento de medidas de prevenção e de segurança (ANPD, 2022).

É importante esclarecer que referidos agentes de tratamentos, quando pessoas jurídicas, são definidos a partir de seu caráter institucional, de maneira que não podem ser considerados como controladores ou operadores os funcionários de uma organização, que apenas atuam obedecendo ao poder diretivo daquele que seria o verdadeiro agente de tratamento. Por outro

[15] (...) VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

lado, é possível que uma pessoa natural atue de maneira independente e em nome próprio, situação na qual será considerada, por si só, um agente de tratamento (ANPD, 2022).

Saber de forma clara a diferença entre o controlador e o operador, na prática, é fundamental, pois a nossa legislação traz obrigações e responsabilidades específicas para cada um dos sujeitos.

Além disso, traçar os panoramas desta distinção é imprescindível para a compreensão do estudo de caso que será realizado ao final desta pesquisa, no qual abordaremos justamente as decisões tomadas pelo controlador no tratamento de dados por ele determinado, bem como os cuidados por ele executados - ou, ainda, a falta destes cuidados- durante toda a operação.

A LGPD também apresenta, em seu artigo 41, um sujeito novo na relação jurídica, o encarregado de proteção de dados pessoais, responsável por estabelecer uma comunicação entre o titular e o agente de tratamento e por direcionar a adequação de determinado setor à legislação.

É o encarregado quem recebe eventuais reclamações dos titulares, quem presta esclarecimentos sobre as práticas do agente de tratamento, entre outras atividades descritas no §2º do art. 41 da referida lei. De forma geral, é ele quem orienta as providências práticas em relação à cultura de proteção de dados pessoais.

Além disso, a lei determina que o tratamento de dados somente poderá ocorrer se for apresentada uma base legal que o justifique e o autorize. Portanto, existem hipóteses pré-determinadas por lei permitindo o tratamento. Algumas delas estão enumeradas no art. 7º da LGPD:

> 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 aos dados pessoais classificados como sensíveis, dentre os quais, como visto, os dados biométricos, estes merecem proteção ainda mais especial, razão pela qual a base legal que fundamenta seu tratamento deverá estar elencada no rol do art. 11 da LGPD:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> 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.

Embora algumas das bases legais de ambas as categorias de dados se assemelhem, o tratamento de dados pessoais sensíveis não pode ocorrer por legítimo interesse ou em razão de proteção de crédito.

Além disso, observa-se que o foco dado à necessidade de “consentimento” do titular é muito maior no art. 11. Nesta situação, o consentimento apenas poderá ser descartado se, nos termos da própria lei, for indispensável ao cumprimento das demais bases legais ali previstas. Ou seja, as hipóteses previstas no inciso II são as exceções permitidas pela lei.

É possível perceber que a lei busca proteger o titular dos dados de situações que apresentam maior risco de discriminação e, por isso, traz algumas restrições nas bases legais que poderão fundamentar o tratamento destes dados. Ou seja, quando se estiver frente a uma

situação na qual os dados ali coletados poderão gerar consequências lesivas e discriminatórias ao titular, as regras que envolvem aquele tratamento serão mais rigorosas.

Atrelada à base legal, deverá ser apontada a finalidade da coleta de dados, a qual deverá ter propósitos legítimos específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I, da LGPD[16]). Os procedimentos envolvendo tratamento de dados, portanto, devem ser transparentes e compatíveis com a finalidade que, como vimos, é um dos princípios estruturantes da lei.

Além de ser informado, o usuário deve ter a liberdade de exercer seu direito de escolha quanto à coleta dos dados, em razão do princípio da autodeterminação. A LGPD ainda enumera outros direitos em relação aos dados que o titular poderá exigir a qualquer momento daquele que está realizando o tratamento, como, por exemplo, confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação, todos previstos no art. 18 da referida lei.

Dentre os direitos elencados, é mister esclarecer o tocante à "anonimização" de dados pessoais. Este procedimento, de acordo com Doneda (2020, p. 142) consiste na retirada do vínculo entre a informação e a pessoa a que se refere, com o intuito de diminuir eventuais riscos que o tratamento daquela informação pode gerar ao titular.

Esclarece-se que o dado anônimo é justamente aquele incapaz de revelar a identidade de alguém, considerando a utilização dos meios técnicos razoáveis e disponíveis na ocasião do tratamento. Não tem nome, não tem rosto. Nesta situação, é muito mais difícil, portanto, fazer uma associação entre o dado e uma pessoa (BIONI, 2020, p. 195)

Em regra, os direitos dos titulares de dados são exercidos em face do agente controlador.

Outra proposta trazida pela LGPD é a obrigação de os agentes de tratamento adotarem medidas de segurança, técnicas e administrativas em relação à forma de armazenamento das informações por elas tratadas, medidas estas que deverão ser aptas a proteger os dados pessoais, evitando tratamentos ilícitos ou inadequados, bem como incidentes de segurança em geral, nos termos do art. 46 da lei.

Importante ressaltar que o marco regulatório da Lei Geral de Proteção de Dados Pessoais vem acompanhado por pela instituição da Autoridade Nacional de Proteção de Dados, por meio

[16] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

da Lei 13.853 de 2019, sendo esta um elemento substancial para a garantia da eficácia da Lei e dos direitos nela previstos.

A ANPD, de início, foi criada como um órgão da administração pública federal, é integrante da Presidência da República, nos termos do art. 2º da Lei 13.844/2019, cuja estrutura organizacional foi definida pelo Decreto 10.474/2020. Ela acumula as funções normativa, regulamentar, fiscalizatória e sancionatória, podendo, inclusive, resolver litígios que envolvem violação às normas da LGPD, a fim de fazer cumprir as normas de proteção de dados pessoais.

No ano de 2022, foi editada a Medida Provisória nº 1.124, de 13 de junho de 2022, com o intuito de alterar a Lei nº 13.709/2018 e, dessa forma, transformar a ANPD em autarquia de natureza especial, com patrimônio próprio. Com essa mudança, a Autoridade passou a ter autonomia administrativa e orçamentária.

Para Doneda (2021, p. 460), a criação de uma autoridade especializada surge justamente para promover uma tutela mais adequada e efetiva dos direitos relativos à proteção de dados pessoais, além de aproximar os titulares de dados dos agentes de tratamento.

A ANPD, por ser uma autoridade especializada tecnicamente na matéria, tem também um papel educativo e orientativo em relação à proteção de dados, a fim de que os cidadãos possam ter mais conhecimento sobre o tema e sobre a importância da proteção de seus dados. Suas atribuições institucionais estão previstas no art. 55-J, VI e VII[17] da LGPD.

A Autoridade Nacional de Proteção de Dados nos dias atuais contribui com a regulamentação da LGPD, seja resolvendo questões que foram deixadas de forma mais ampla pela lei, seja trazendo esclarecimentos mais práticos a respeito da aplicação da lei.

Um exemplo desta regulamentação são os guias orientativos formulados pela ANPD ao longo dos anos de 2021 e 2022 (Guia Orientativo para Definições dos Agentes de Tratamento De Dados Pessoais e do Encarregado; Guia Orientativo para Tratamento De Dados Pessoais Pelo Poder Público; Guia Orientativo Aplicação Da Lei Geral De Proteção De Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral; entre outros), os quais, inclusive, foram utilizados como material bibliográfico nesta pesquisa (ANPD, 2022).

Por fim, a obediência da LGPD também é resguardada por meio de sanções estabelecidas na própria lei, que prevê desde multas até punições mais severas, como a

[17] Art. 55-J - Compete à ANPD:
VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

proibição parcial ou total do exercício de atividades relacionadas ao tratamento de dados pessoais.

3.4 Perspectiva constitucional: proteção de dados como direito fundamental

Como vimos, a preocupação com a proteção aos direitos fundamentais é bastante evidente no art. 2° da LGPD, que pode ser relacionado ao texto constitucional brasileiro no que concerne ao conteúdo, haja vista que a Constituição Federal Brasileira é pautada na proteção aos direitos fundamentais e à dignidade da pessoa humana.

Sob a ótica constitucional, é possível observar que, gradualmente, tem ocorrido a incorporação do direito à proteção de dados pessoais como direito fundamental, em um campo próprio, paralelo ao direito à privacidade que, como visto, tem se mostrado insuficiente para uma tutela efetiva das informações pessoais armazenadas em bancos de dados.

No Brasil, o Supremo Tribunal Federal, em decisão histórica proferida no julgamento ocorrido nos dias 06 e 07 de maio de 2020, reconheceu o direito à proteção de dados como direito fundamental, sendo que a privacidade, também neste aspecto, deverá ser protegida a nível constitucional.

Trata-se do julgamento das Ações Diretas de Inconstitucionalidade (ADIs) nº 6.387, 6.388, 6.389, 6.390 e 6.393 movidas pelo Conselho Federal da Ordem dos Advogados do Brasil- OAB (ADI 6387) e pelos partidos políticos Partido da Social Democracia Brasileira (PSDB) (ADI 6388), Partido Socialista Brasileiro (PSB) (ADI 6389), Partido Socialismo e Liberdade (Psol) (ADI 6390) e Partido Comunista do Brasil (PcdoB) (ADI 6393).

Nas ADIs, em síntese, os requerentes alegaram que a Medida Provisória (MP) nº 954/2020[18], que, em síntese, obrigava as empresas de telecomunicações a compartilhar nome, telefone e endereço de seus consumidores com o Instituto Brasileiro de Geografia e Estatística - IBGE, violava alguns direitos fundamentais tutelados pela Constituição Federal, tais como o da dignidade da pessoa humana, da inviolabilidade da intimidade e da vida privada e a autodeterminação informativa.

Outro ponto levantado nas ADIs foi sobre a necessidade de se tutelar expressamente o direito fundamental à proteção de dados.

[18] A Medida Provisória nº 954, de 17 de abril de 2020, dispunha sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020".

Esclarece-se que referida MP determinou o compartilhamento de informações sobre dados de seus consumidores às empresas concessionárias de Serviço Telefônico Fixo Comutado (STFC) e do Serviço Móvel Pessoal (SMP), sob a justificativa de que seria realizada a pesquisa trimestral PNAD (Pesquisa Nacional por Amostra de Domicílios Contínua) Covid, voltada à quantificação do alastramento da pandemia da Covid-19, com quesitos que poderiam direcionar políticas contra a Covid-19 durante o período de quarentena.

Em 24/04/2020, a Ministra Rosa Weber, relatora do caso, em decisão monocrática liminar, deferiu a medida cautelar requerida pela parte autora com o intuito de suspender a eficácia da Medida Provisória n. 954/2020, determinando, em consequência, que o IBGE parasse imediatamente de requerer a disponibilização dos dados objeto da referida medida provisória:

> (...) **defiro a medida cautelar requerida, ad referendum do Plenário desta Suprema Corte, para suspender a eficácia da Medida Provisória n. 954/2020**, determinando, em consequência, que o Instituto Brasileiro de Geografia e Estatística – IBGE se abstenha de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tenha feito, que suste tal pedido, com imediata comunicação à(s) operadora(s) de telefonia. 25. Por fim, considerando que as ações diretas de inconstitucionalidade nº s 6388, 6389, 6390 e 6393, a mim distribuídas por prevenção (art. 77-B, RISTF), igualmente impugnam a validade constitucional da Medida Provisória n. 954/2020, determino a tramitação conjunta dos feitos, com a reprodução desta decisão nos autos respectivos. À Secretaria Judiciária. Publique-se. Intime-se, com urgência (Medida Cautelar na Ação Direta de Inconstitucionalidade 6.390 Distrito Federal. Rel., Ministra Rosa Weber. Data da decisão: 24/04/2020). Grifos nossos.

Analisando as razões que fundamentaram a decisão acima, verifica-se que a Ministra pontuou expressamente que a medida provisória não explicava, de forma explícita, a relação entre os dados pessoais coletados e a elaboração de políticas de enfrentamento da pandemia da Covid-19, além de não mencionar as razões e o modo pelo qual ocorria o tratamento de dados.

Por fim, outro argumento importante trazido pela Ministra foi no sentido de que, ainda que os dados fossem coletados para o fim de colaborar com a resolução da situação de saúde pública, ela não poderia prejudicar direitos fundamentais dos titulares de dados.

Ademais, a Ministra Relatora ressaltou que, em quaisquer circunstâncias, as garantias fundamentais previstas na Constituição Federal deverão ser respeitadas, vez que o foco da tutela é a pessoa humana e sua dignidade.

Após, com dez votos favoráveis, o Plenário da Suprema Corte referendou a Medida Cautelar concedida pela Ministra Rosa Weber, e suspendeu a eficácia da Medida Provisória

954/2020. A Corte reconheceu que no atual contexto de desenvolvimento tecnológico não existem dados insignificantes, de maneira que todo e qualquer dado que identifique ou possa identificar um indivíduo deverá ser protegido, nos termos da ementa abaixo:

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. **Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo 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), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados (...) 4. Consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória nº 954/2020, nos moldes em que editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia. 5. **Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação quanto à sua adequação e necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades**. 6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros (...) 9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição. 10. Fumus boni juris e periculum in mora demonstrados. **Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.** 11. Medida cautelar referendada (Supremo Tribunal Federal. ADI 6.387-DF.

> Min. rel. Rosa Weber. Data de julgamento: 07 de maio de 2020. Publicado em 03 de junho de 2020). Grifos nossos.

Analisando a ementa cima, em conjunto com os votos proferidos naquele julgamento, observa-se que o STF sugeriu uma proteção ampla, bastante aberta, a fim de que pudesse ser aplicada em diferentes situações, envolvendo não apenas os dados, mas o titular daqueles, já que a pessoa é quem efetivamente arcará com os eventuais riscos e danos causados pelo tratamento indevido e/ou abusivo de dados pessoais (SUPREMO TRIBUNAL FEDERAL, 2020).

Partindo-se do eixo constitucional existente, não se trata de proteger os dados pessoais em si, mas a pessoa que está por trás deles, em seu verdadeiro direito de personalidade.

Conforme destacado por Schertel e outros (2021, p. 65) “a interpretação constitucional conferida foi a de que qualquer dado que leve à identificação de uma pessoa pode ser usado para a formação de perfis informacionais de grande valia para o mercado e para o Estado e, portanto, merece proteção constitucional”.

O julgado do Supremo Tribunal Federal esclarece que é necessário estabelecer um equilíbrio entre o fluxo de dados pessoais para obter as vantagens pretendidas no âmbito do mercado, buscando, assim, proteger a dignidade dos indivíduos, tendo em vista que, havendo qualquer uso inadequado de seus dados, aqueles poderão ficar expostos a riscos e sofrer lesões. Com essa decisão, o STF trouxe maior segurança jurídica no tratamento de dados e gerou um ambiente de maior confiança por parte dos cidadãos.

Frente a este contexto, embora se reconheça o papel relevante que a informação, sobretudo seu compartilhamento, detém em nossa sociedade, cada vez mais tecnológica, não se pode olvidar que a proteção à privacidade e aos dados pessoais também são fundamentais.

Em razão das próprias características do Estado Democrático de Direito, verificamos que este exige, no mínimo, balizas jurídicas claras e seguras quanto a essa coleta ou transferência.

De um lado, essa proteção se desdobra como liberdade negativa do cidadão oponível perante os agentes de tratamento, demarcando seu espaço individual de não intervenção (dimensão subjetiva).

De outro lado, ela estabelece um dever de atuação protetiva dos agentes que realizam o tratamento, no sentido de estabelecer condições e procedimentos aptos a garantir o exercício e a fruição desse direito fundamental (dimensão objetiva) (MENDES; JÚNIOR; FONSECA, 2021, p. 68).

Além disso, em 20 de outubro de 2021, o Senado aprovou a Proposta de Emenda à Constituição (PEC) 17/2019, para incluir a proteção de dados pessoais, inclusive nos meios digitais, no rol de direitos e garantias fundamentais previstos no artigo 5º da Constituição Federal.

Com a posterior promulgação e a consequente publicação do texto no Diário Oficial da União em 11/02/2022 a PEC 17/2019 se transformou na Emenda Constitucional nº 115 de 10/02/2022. Em razão disso, o texto constitucional passou a ser escrito da seguinte forma:

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

Outra alteração trazida por esta Emenda foi que a proteção de dados passou a ser matéria de competência legislativa exclusiva da União, de maneira que caberá apenas a esta legislar sobre o tema, além de organizar e fiscalizar a proteção e o tratamento de dados pessoais. Dessa forma, os artigos 21 e 22 da Constituição Federal passaram a vigorar como:

> Art. 21. Compete à União:
>
> (...) XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.
>
> Art. 22. Compete privativamente à União legislar sobre:
>
> (...) XXX - proteção e tratamento de dados pessoais.

Com isso, o direito à proteção de dados passa a ser reconhecido no mesmo patamar de outros bens constitucionalmente assegurados, sendo considerado em eventual caso de conflitos entre direitos, inclusive como valor axiológico a ser observado nas decisões proferidas pelo Poder Judiciário.

A constitucionalização do direito à proteção de dados pessoais representa um avanço significativo não apenas em relação à própria proteção de dados dos titulares, mas também ao direito à privacidade, à autodeterminação informativa e à liberdade dos cidadãos, pois garante que todos os dados são importantes e merecem o devido cuidado. Ademais, ela reforça a importância de se promover um esforço multissetorial, envolvendo Estado e atores particulares, na garantia deste direito.

A esse respeito, na justificação inicial da PEC, seus autores, dentre os quais o Senador Eduardo Gomes, sustentam que:

> A proteção de dados pessoais é fruto da evolução histórica da própria sociedade internacional: diversos são os Países que adotaram leis e regras sobre privacidade e proteção de dados. Isso porque o assunto, cada vez mais, na Era informacional, representa riscos às liberdades e garantias individuais do cidadão. O avanço da tecnologia, por um lado, oportuniza racionalização de negócios e da própria atividade econômica: pode gerar empregabilidade, prosperidade e maior qualidade de vida. Por outro lado, se mal utilizada ou se utilizada sem um filtro prévio moral e ético, pode causar prejuízos incomensuráveis aos cidadãos e à própria sociedade, dando margem, inclusive, à concentração de mercados. Por isso, países de todo o planeta já visualizaram a importância e a imprescindibilidade de se regular juridicamente o tratamento de dados dos cidadãos (SENADO, 2019).

Outro aspecto a se avaliar é que a aprovação da PEC contribui para o fortalecimento de uma cultura de privacidade e proteção de dados no Brasil, trazendo, ainda, reflexos na interpretação e na aplicação das legislações infraconstitucionais.

Percebe-se, portanto, um reconhecimento gradual do direito fundamental à proteção de dados pessoais como direito autônomo, com contornos e âmbito de proteção próprio.

Para Doneda (2015, p. 151), essa inclusão, ainda que de forma inicial, da proteção de dados pessoais como direito fundamental, decorre do fato de que, em nossa sociedade, muitas vezes, o indivíduo pode ser discriminado e estigmatizado em razão do tratamento abusivo ou excessivo de seus dados.

Assim, a compreensão como direito fundamental implica em garantir a liberdade do indivíduo dentro da sociedade, sem exposições desnecessárias de suas informações pessoais, bem como em promover a ideia de o próprio titular decidir sobre a exposição de seus dados.

Diante do exposto, concluímos que o reconhecimento do direito fundamental à proteção de dados pessoais surge como resposta, a nível constitucional, à busca por uma proteção mais efetiva da dignidade humana no contexto da sociedade da informação, em que o risco do processamento de dados de forma abusiva e indevida é cada vez maior.

Assim, passa a se consagrar materialmente na Carta Maior um direito que há muito já se tentava proteger, por meio das legislações infraconstitucionais, colocando o “direito à proteção de dados pessoais” como um comando a ser observado pelo Estado e pelos particulares. Ele é o limite e, ao mesmo tempo, um postulado de proteção, que irradia seus efeitos sobre toda a ordem jurídica.

Além disso, o reconhecimento desse direito fundamental se alinha com os fundamentos sob os quais o Estado democrático de direito se orienta.

4 INCIDÊNCIA DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES PRIVADAS

Como vimos, sob o aspecto de direito fundamental, o direito à proteção de dados deve orientar toda a ordem jurídica, inclusive os atos privados, tendo em vista que, de acordo com a teoria da eficácia horizontal dos direitos fundamentais, estes também são oponíveis aos atores particulares (SARLET, 2021, p. 50).

A esse respeito, na seara da proteção de dados, esta questão ganha ainda mais relevância, uma vez que os atores privados, representados principalmente pelas grandes corporações, possuem alto poder econômico, político e social, quando comparados com os titulares de dados, o que pode gerar um desequilíbrio ainda maior nas relações jurídicas e, desta forma, cometem violações de direitos.

Esta subseção pretende analisar, por meio do estudo de relevante caso concreto envolvendo o Instituto Brasileiro de Defesa do Consumidor - IDEC e a Concessionária da Linha 4 do Metrô de São Paulo (Via Quatro), ainda em trâmite no Tribunal de Justiça de São Paulo[19], como o direito à proteção de dados pessoais incide nas relações privadas.

De acordo com os ensinamentos de Feferbaum e Queiroz (2019, p. 58), o estudo de caso propõe uma análise qualitativa, em que a atenção do pesquisador se volta para compreender a solução adotado no caso concreto, bem como sua fundamentação teórica e jurídica, realizando, portanto, uma abordagem mais integrada, a fim de proporcionar uma melhor compreensão sobre o problema. Ademais, o estudo de caso permite uma discussão mais contextualizada, que vai além do plano meramente teórico e abstrato.

Vale esclarecer que tal técnica não busca a mera descrição dos fatos, mas sim uma análise qualificada sobre determinada situação, para que o pesquisador possa extrair ensinamentos do caso e propor novas soluções sobre o problema envolvido ou, ainda, entender melhor os riscos e possíveis desafios no tema.

Especificamente em relação a um estudo de caso judicial, é fundamental que se avalie as consequências do caso, bem como se demonstre a razão pela qual a investigação escolhida é importante como paradigma para a solução de outras situações futuras e semelhantes (MEZZAROBA; MONTEIRO, 2019, p. 127).

---

[19] Processo nº 1090663-42.2018.8.26.0100. Ação Civil Pública. Requerente: Idec - Instituto Brasileiro de Defesa do Consumidor. Requerida: Concessionária da Linha 4 do Metrô de São Paulo S.A. (Via Quatro). Ajuizada na 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo.

O estudo de caso nesta pesquisa tem o intuito de verificar como as instituições democráticas, como o Poder Judiciário, têm respondido às demandas da sociedade da informação e analisar seu grau de compromisso na garantia e na tutela do direito à proteção de dados. À nível nacional, observa-se que, aos poucos, estão sendo colocadas em pauta questões de interpretação e de aplicação da Lei Geral de Proteção de Dados Pessoais.

Esclarece-se que a escolha deste caso envolvendo o IDEC e a ViaQuatro se deu pelos seguintes motivos:

Em primeiro lugar, porque trata-se de um conflito inovador em matéria englobando novas tecnologias e proteção de dados pessoais, proposto diante do Poder Judiciário e que, em razão disso, poderá definir precedentes na matéria. Isto posto, envolve uma decisão inédita no ordenamento jurídico brasileiro, no que se refere ao uso de tecnologias, sobretudo de algoritmos de Inteligência Artificial, e à importância da proteção de dados pessoais.

Em segundo lugar, a escolha se deu por conta da repercussão que o caso tem tido na mídia e nos debates atuais, uma vez que envolveu o tratamento de dados de milhares de pessoas, as quais diariamente utilizam o serviço de transporte da linha 4, em um espaço público. Assim sendo, trata-se de um caso que, além de ser bastante conhecido e de fácil acesso aos leitores, afetou os dados pessoais de um número expressivo de indivíduos.

Em terceiro lugar, esta autora se propõe a estudar o caso, pois ele envolve a discussão a respeito da coleta de dados biométricos de usuários do transporte coletivo para fins de implementação de um sistema de reconhecimento facial e, posteriormente, para fins de alinhar estratégias de marketing e de publicidade. Os dados biométricos são classificados como dados pessoais sensíveis. Por apresentarem maior risco ao titular, sua tutela merece ser ainda mais especial e específica.

Por fim, porque foi um caso que acompanhou toda a transição da Lei Geral de Proteção de Dados Pessoais, tendo sido ajuizado antes da vigência da lei, porém, sentenciado quando ela já estava em vigor.

Assim, diante das razões expostas, conclui-se que, por meio do estudo deste paradigma, será possível analisar os principais conceitos trazidos ao longo deste trabalho, bem como realizar uma análise crítica a respeito do desenvolvimento do direito à privacidade, como forma de controle sobre os próprios dados, e da consolidação de um ramo autônomo do direito à proteção de dados pessoais e, por fim, visualizar, na prática, como os institutos têm sido aplicados e quais os principais impactos destes “novos direitos” na sociedade atual.

Nesta perspectiva, importante fazer uma ressalva: embora a sentença estudada faça referências, em sua fundamentação, ao Código de Defesa do Consumidor e aos direitos previstos ao consumidor, a presente pesquisa pretende focar apenas naquilo que for referente à Lei Geral de Proteção de Dados Pessoais, bem como ao que diz respeito ao direito fundamental à privacidade e à proteção de dados pessoais, com o intuito de delimitar a análise ao objeto proposto para este trabalho.

4.1 Estudo do caso do Metrô da linha amarela de São Paulo

Inicialmente, é fundamental contextualizar brevemente o caso envolvendo o Instituto Brasileiro de Defesa do Consumidor (IDEC) e a concessionária da linha 4 do Metrô de São Paulo (ViaQuatro), objeto deste estudo, em que se discute essencialmente a prática de coleta, utilização e armazenamento de dados pessoais por meio de uma plataforma digital.

Em agosto de 2018, o Instituto Brasileiro de Defesa do Consumidor (IDEC) ajuizou uma ação civil pública em face da concessionária da linha 4 do Metrô de São Paulo (ViaQuatro), na qual, em síntese, alegou que em sete estações da Linha 4-Amarela: Luz, República, Paulista, Fradique Coutinho, Faria Lima, Pinheiros e Butantã estaria ocorrendo o tratamento de dados pessoais de usuários, consistente no seu reconhecimento facial, sem seu consentimento, por meio do sistema de Portas Interativas Digitais, para fins publicitários.

Esclarece-se que esse sistema reconhecia a presença de rostos humanos quando estavam na frente dos anúncios publicitários, bem como capturava suas expressões e dados pessoais. Assim, a partir das informações coletadas, o sistema identificava as emoções, gênero e faixa etária dos titulares de dados e, mais ainda, ele reconhecia um padrão de comportamento dos usuários para, em um segundo momento, compartilhar dados com terceiros, que, por sua vez, direcionavam propagandas que fossem mais adequadas àquele público.

Os usuários do metrô não sabiam que estavam sendo filmados e muito menos que suas informações seriam repassadas para fins publicitários. Ou seja, tratava-se de uma pesquisa de opinião totalmente compulsória, na qual os dados pessoais obtidos eram comercializados sem o consentimento de seus titulares.

O IDEC aduziu que tal prática era abusiva uma vez que não informou os usuários de forma clara sobre a operação, além de não permitir que aqueles escolhessem pela coleta (ou não) de seus dados, tendo em vista que os indivíduos sequer sabiam sobre a operação envolvida no funcionamento das Portas Interativas, e, por fim, o sistema não tinha qualquer finalidade de

melhorar o serviço prestado pela ViaQuatro, que é referente ao transporte público, ultrapassando, portanto, o seu real objetivo.

Em razão disso, o IDEC requereu que fossem cessados e proibidos a coleta e o tratamento das imagens e dos dados biométricos dos usuários que utilizavam aquela linha de metrô, com a condenação da empresa responsável ao pagamento de indenização pela utilização indevida da imagem dos usuários e de danos coletivos. A parte autora, inclusive, pleiteou tutela de urgência neste sentido, para que fosse comprovado o desligamento das câmeras, sob pena de multa.

Em sua defesa, a requerida Via Quatro defendeu a legalidade de utilização da Porta Interativa, sob o argumento de não haver violação ao dever de transparência, à privacidade ou à proteção de dados pessoais dos usuários da Linha 4 do Metrô de São Paulo. Disse ainda que a operação realizava apenas uma detecção facial dos usuários para fins estatísticos, no sentido de se efetuar um levantamento demográfico sobre o público, ou seja, verificar quantas pessoas transitavam diariamente por aquela região.

Apesar disso, em determinado trecho de sua defesa (fls. 369 do processo referido), a Via Quatro acabou confessando que a "tecnologia embarcada nas Portas Interativas Digitais se limita a contaras pessoas, visualizações, tempo de permanência, tempo de atenção, gênero, faixas etárias, emoções, fator de visão, horas de pico de visualizações e distância de detecção". Ou seja, ficou evidente que, além da contagem de pessoas, a tecnologia capturava suas reações, bem como suas características relacionadas à gênero e à idade.

Disse ainda que não armazenava dados pessoais dos passageiros, pois as informações seriam apagadas após a coleta. Ademais, a Via Quatro alegou que os dados que fossem eventualmente armazenados seriam anonimizados. Requereu que a ação fosse julgada totalmente improcedente, em razão da ausência dos requisitos da responsabilidade civil, sobretudo da não comprovação do dano coletivo.

Importante destacar que, tendo em vista que a ViaQuatro é concessionária de serviço de transporte público, a Defensoria Pública do Estado de São Paulo foi intimada para se manifestar. Além disso, por se tratar de um caso que envolve a tutela de direitos coletivos, teve a participação do Ministério Público.

E, ainda, contou com a presença do Instituto Alana, na condição de *amicus curiae*, já que envolve a coleta de dados pessoais de crianças e de adolescentes- ressalta-se que este trabalho não terá como foco a análise das violações de direito oriundas do tratamento de dados

pessoais de crianças e de adolescentes, cuja matéria é extensa, com característica muito particulares, razão pela qual merece um tópico de estudo próprio.

O feito tramitou na 37ª Vara Cível da Comarca de São Paulo, no estado de São Paulo.

Tendo em vista que a questão discutida era exclusivamente de direito, a magistrada responsável pelo caso, Dra. Patrícia Martins Conceição, optou por julgar o feito de forma antecipada, isto é, sem determinar a produção de outras provas, além daquelas que já haviam sido juntadas no processo. Assim, as provas utilizadas para dar embasamento à sentença foram os diversos documentos juntados nos autos pelas partes envolvidas.

A ação foi julgada parcialmente procedente pela Dra. Patrícia Martins Conceição, a qual, de forma resumida, condenou a Via Quatro a se abster de coletar as imagens sem consentimento dos usuários, assim como a pagar R$100.000,00 (cem mil reais) à título de indenização por danos morais coletivos, conforme dispositivo da sentença transcrito abaixo:

> Ante o exposto, JULGO PROCEDENTES EM PARTE os pedidos, com resolução do mérito, na forma do artigo 487, I do Código de Processo Civil, para (i) determinar que a requerida se abstenha de captar as imagens, sons e quaisquer outros dados pessoais dos consumidores usuários, através das câmeras ou outros dispositivos envolvendo os equipamentos instalados na Linha 4 Amarela do metrô, sem consentimento prévio do consumidor, confirmando a liminar anteriormente concedida pela decisão de fls. 327/332; (ii) determinar à requerida que, caso deseje readotar as práticas tratadas nos autos, deverá obter o consentimento prévio dos usuários mediante informação clara e específica sobre a captação e tratamento dos dados, com adoção das ferramentas pertinentes; e (iii) condenar a requerida ao pagamento de indenização por danos morais coletivos no valor de R$100.000,00, corrigida segundo a tabela prática do Egrégio Tribunal de Justiça de São Paulo, desde a data da publicação da sentença, e com juros de mora de 1% ao mês, incidentes a partir da citação, por se tratar de ilícito contratual, na forma do artigo 405, do Código Civil, a ser revertido para o Fundo de Defesa de Direitos Difusos - FDD, criado na forma do artigo 13 da Lei nº 7.347/85.

Ao proferir a sentença, a magistrada entendeu ser incontroverso que havia a utilização de equipamentos de gravação de imagens, com a consequente captação de dados pessoais para fins publicitários e estatísticos nas estações administradas pela parte ré, destacando que não restavam dúvidas acerca da captação de imagens sem consentimento e sequer sem conhecimento dos titulares dos dados.

Além disso, esclareceu que embora a Lei Geral de Proteção de Dados fosse posterior ao início da captação das imagens discutidas, a questão dos autos envolve o tratamento de dados pessoais com efeitos futuros, motivo pelo qual estaria submetida aos parâmetros da lei.

Assim, concluiu-se que o reconhecimento facial ou mesmo a mera detecção facial, com acesso à imagem do indivíduo, estaria abrangida no conceito de dado biométrico, o qual, para a LGPD, é considerado um dado pessoal sensível, que merece proteção especial e mais específica, de acordo com as bases legais previstas no rol do artigo 11 da LGPD.

No caso em tela, o principal fundamento da magistrada em sua conclusão foi de que nenhuma das hipóteses legais previstas na Lei Geral de Proteção de Dados Pessoais havia sido respeitada, estando evidente a violação à previsão legal.

Outro fundamento ao qual ela se baseou foi de que o princípio da finalidade, segundo o qual o tratamento de dados deve ter propósitos legítimos, específicos, explícitos e informados ao titular, também não foi respeitado, tendo em vista que a coleta estava sendo realizada com evidente finalidade comercial.

A magistrada também observou que os usuários sequer foram comunicados acerca da captação de sua imagem e, principalmente, de suas emoções em relação à publicidade veiculada no equipamento, o que viola seu direito à informação clara e adequada sobre os produtos e serviços, bem como o direito à proteção contra a publicidade enganosa e abusiva, dispostos no art. 6º do Código de Defesa do Consumidor.

Ressaltou ainda que, conforme o §3º do art. 11 da lei referida, o uso de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação.

Outro ponto crítico identificado na sentença é que o anúncio veiculado na linha amarela captava, inclusive, imagens de crianças e adolescentes, cujos dados pessoais gozam de uma proteção ainda maior, em razão de sua vulnerabilidade. Neste sentido, destacou que a preservação e a proteção da imagem destes sujeitos é prioridade absoluta do Estado, já reconhecida no art. 227 da Constituição Federal[20] e no art. 17 do Estatuto da Criança e do Adolescente[21].

Em face da sentença, foram interpostos Recursos de Apelação por todas as partes, sendo que estas, inclusive, já apresentaram as Contrarrazões sobre os recursos.

---

[20] Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

[21] Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Os autos foram encaminhados para a 20ª Câmara de Direito Privado, que não conheceu os recursos, sob o argumento de que como se trata de ação civil pública decorrente de responsabilidade civil do Estado por suposto ilícito extracontratual praticado por concessionária de serviço público, a competência para apreciação das apelações seria de uma das Câmaras da Subseção de Direito Público do Tribunal de Justiça de São Paulo.

Em razão disso, as apelações foram redistribuídas para a 8ª Câmara de Direito Público. O relator designado para tratar do caso foi o Desembargador Antônio Celso Faria.

O feito, finalmente, foi julgado em segunda instância no dia 10/05/2023. O acórdão proferido pela 8ª Câmara possui a seguinte ementa:

> APELAÇÕES. Ação civil pública. Concessionária da Linha 4 do Metrô de São Paulo S.A. (Via Quatro) que opera, por meio das "Portas Interativas Digitais" dos trens da linha de metrô coletando diversos dados e informações dos consumidores usuários. Captação das imagens que eram utilizadas para fins publicitários e comerciais, tendo-se em vista que se buscava detectar as principais características dos indivíduos que circulavam em determinados locais e horários. Ausência de prévia autorização para captação das imagens que demonstra conduta muito reprovável caracterizando dano moral coletivo, principalmente considerando o incalculável número de passageiros que transitam pela plataforma da ré todos os dias. Entendimento do C. STJ de que o dano moral coletivo é aferível "in re ipsa", de forma que a sua constatação decorre da apuração da prática ilícita que viole direitos da coletividade, de conteúdo extrapatrimonial. Conquanto inexista fórmula matemática para a apuração do "quantum" devido a título de danos morais coletivos, cediço que deve guardar correspondência com a gravidade do fato, condição de vulnerabilidade dos consumidores usuários e a conduta da causadora do dano, evitando-se, assim, a reiteração da prática ilícita. Necessidade de condenação da ré ao pagamento de indenização no valor de R$ 500.000,00 (quinhentos mil reais), que se mostra suficiente para reparar o dano moral coletivo e prevenir a prática do mesmo tipo de ilícito. RECURSOS DO MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO, DO IDEC INSTITUTO BRASILEIRO DE DEFESA AO CONSUMIDOR E DA DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO PROVIDOS EM PARTE APENAS PARA MAJORAR O VALOR DO DANO MORAL COLETIVO E NEGADO PROVIMENTO AO RECURSO DA CONCESSIONÁRIA DA LINHA 4 DO METRÔ DE SÃO PAULO S.A. (VIA QUATRO).

Analisando o acórdão proferido pela 8ª Câmara de Direito Público, observa-se que o relator responsável pelo caso, simplesmente, reiterou a maior parte dos fatos e dos argumentos trazidos pela sentença. Aliás, com base no art. 252 do Regimento Interno do Tribunal de Justiça de São Paulo[22], o relator admitiu que estava se limitando a ratificar os fundamentos da decisão recorrida (sentença), entendendo que, nesta situação, seria inútil repetir a matéria.

[22] Art. 252 do Regimento Interno do Tribunal de Justiça de São Paulo "Nos recursos em geral, o relator poderá limitar-se a ratificar os fundamentos da decisão recorrida, quando, suficientemente motivada, houver de mantê-la".

Em síntese, no mesmo sentido da magistrada, os desembargadores que participaram do julgamento concluíram que restou incontroverso que ocorreu a captação de imagens (englobando, portanto, as emoções e reações) para fins comerciais, sem comunicação dos usuários do metrô, que, por sua vez, eram os titulares dos dados pessoais coletados.

Após as considerações a respeito da sentença, o Desembargador relator optou por majorar o valor que havia sido atribuído à título de danos morais coletivos, para constar que deveria ser pago pela Ré o montante de R$500.000,00 (quinhentos mil reais), pois, a seu ver, este valor seria uma forma de prevenir a prática do mesmo tipo de ilícito, ou seja, um caráter didático, bem como de proteger a coletividade de futuras coletas indevidas de seus dados.

A ViaQuatro, o IDEC e a Defensoria opuseram embargos de declaração, com o intuito de esclarecer alguns vícios, consistentes em omissões e contradições, do Acórdão, requerendo, ainda, o prequestionamento dos artigos referidos nas minutas. Em resumo, as partes apontaram questões que, a seu ver, não teriam sido apreciadas pelo Tribunal.

O Ministério Público, por sua vez, interpôs diretamente recurso especial, expondo violações atreladas ao Código de Defesa do Consumidor, especificamente aos artigos 6º, incisos VI e VII, e 95 do CDC. Isto porque, segundo o ente, a ViaQuatro deveria ser condenada por danos individuais homogêneos, de forma cumulada com danos morais coletivos. Disse que, com a conduta da Ré, houve violação dos direitos da personalidade de diferentes indivíduos, sobretudo da imagem e da intimidade, tratando-se de situação que ultrapassa o mero dissabor cotidiano.

Assim, até a data em que esta pesquisa foi efetuada (11/07/2023), os recursos ainda não haviam sido julgados pelo Tribunal, estando pendente a manifestação das partes.

Embora o atual quadro legislativo, em especial a LGPD, não forneça diretrizes claras e específicas a respeito do uso de tecnologias de reconhecimento facial, analisando as circunstâncias do caso em tela, a conclusão é no sentido de que, tanto constitucionalmente, quanto infraconstitucionalmente, houve violação à privacidade e à proteção de dados pessoais pela ViaQuatro.

O principal fundamento para se justificar referida violação é o fato de que os usuários do metrô, além de não consentirem com o tratamento de seus dados pessoais pela concessionária, sequer tinham conhecimento de que referida coleta estava ocorrendo. A gravidade da situação é ainda maior ao constatarmos que a controladora também tinha acesso às emoções e as reações dos indivíduos, com o objetivo de utilizá-las como material de estudo para a criação de propagandas publicitárias.

Como vimos no tópico três desta pesquisa, o direito à proteção de dados já reconhecido como fundamental e, portanto, que merece proteção inerente.

Sob o ponto de vista constitucional, observamos que houve a violação à privacidade em seu sentido amplo, atingindo não apenas a imagem do titular, mas sua própria intimidade (emoções e reações) e sua vida privada.

Do mesmo modo, na esfera infraconstitucional, percebemos que houve violação ao conjunto de facetas da vida da pessoa e de sua personalidade.

Além disso, é evidente que houve violação em relação à atual dimensão positiva do direito à privacidade, como direito à proteção dos dados pessoais, no sentido de que, hoje, a privacidade também implica no direito de o seu titular ter o controle sobre suas informações e de determinar a maneira pela qual irá construir seu espaço particular. Isto porque a ViaQuatro não permitiu que o usuário tivesse conhecimento das formas de tratamento, da finalidade e do destino de seus dados que foram coletados.

Referida conduta da concessionária também viola frontalmente o que dispõe o §3º do art. 11 da LGPD:

> A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

Assim, por qualquer ângulo que se observe a questão, é evidente que o caso das Portas Digitais Interativas representa uma hipótese de violação ao direito à privacidade, em seu sentido amplo.

4.2 Do tratamento de dados pessoais biométricos pela Concessionária ViaQuatro

Nos dias de hoje, o avanço das tecnologias da informação e da comunicação têm alterado as formas de interação na sociedade, principalmente as estratégias do mercado de consumo. Há uma crescente coleta de dados pessoais dos usuários para se estabelecer formas de marketing, a fim de influenciar cada vez mais diretamente os consumidores.

No caso em tela, a captura e o uso das imagens- consideradas dados pessoais sensíveis- dos usuários do metrô correspondem a um tratamento de dados pessoais que tinha a finalidade de extrair informações sobre a reação das pessoas às propagandas disponibilizadas e, posteriormente, produzir novos anúncios de publicidade de acordo com os interesses dos usuários.

O tratamento de dados pessoais da forma que ocorreu no caso analisado foi possível, sobretudo, pelo uso de algoritmos de Inteligência Artificial da AdMobilize, agregados ao funcionamento das câmaras de filmagens locais, tecnologia que permitiu a coleta do rosto dos milhares de usuários que passavam pelo metrô de forma rápida e a um baixo custo (TEÓFILO *et al.*, 2021, online).

Como visto, a coleta tinha o intuito de extrair informações a respeito da reação e da emoção dos indivíduos quanto às publicidades apresentadas e, desta forma, conduzir futuras estratégias de marketing, de acordo com as vontades e as demandas dos usuários da linha de metrô.

No caso estudado, o uso da tecnologia de reconhecimento facial pode configurar violação à proteção de dados biométricos, os quais, como vimos, são considerados dados sensíveis, que, por sua vez, exigem uma proteção mais especial.

Com a coleta de imagem dos passageiros do metrô, foi possível identificar o gênero, a faixa etária, entre outras características físicas do indivíduo, assim como suas emoções, as quais são obtidas por meio de uma análise pelo algoritmo de Inteligência Artificial de alguns aspectos do rosto, como o sorriso, a posição das sobrancelhas. Ou seja, o algoritmo consegue identificar a emoção do usuário apenas com aquela coleta de imagem.

Conforme explanamos nas subseções 2 e 3, os dados sensíveis são aquelas informações que, em razão de suas características, ao serem submetidas a tratamento, podem oferecer conteúdo de vulnerabilidade e uma potencial discriminação de seu titular. Por este motivo, o tratamento de dados sensíveis pode apresentar maiores riscos aos direitos da privacidade e da proteção de dados e à personalidade do titular do que outros tipos de informação.

Por esse motivo, a LGPD propõe uma proteção normativa ainda mais especial sobre estes dados, assegurando, de forma expressa, que eles apenas poderão ser tratados se houver consentimento de seu titular, o proprietário da característica captada; ou, para estrito cumprimento de obrigação legal ou regulatória; para execução de políticas públicas pela administração pública; realização de estudos por órgão de pesquisa; proteção da vida ou da incolumidade física do titular ou de terceiros; ou, por fim, para tutela da saúde (art. 11, II).

Inclusive, é por esta razão que a orientação jurídica fornecida para as empresas que coletam e tratam dados pessoais biométricos é no sentido de que implementem um procedimento cauteloso, em que seja possível a coleta de autorização específica do titular, em um documento próprio para tanto e, ainda. que a empresa forneça todas as informações possíveis e cabíveis a respeito do tratamento (PECK PINHEIRO, 2013, p. 92).

Além disso, o tempo de armazenamento dos dados biométricos deve ser sempre determinado. Passado o período, aqueles deverão ser eliminados, exceto se existir alguma situação que justifique sua guarda por tempo maior. Afinal, eles envolvem a personalidade de seu titular, merecendo maior cuidado e proteção.

4.3 Análise do caso à luz dos princípios da LGPD

Como vimos, a LGPD é uma norma principiológica, trazendo algumas diretrizes, em forma de princípios, para a tutela do titular de dados. Estes princípios, comuns a muitos ordenamentos jurídicos, formam um núcleo orientador das questões envolvendo proteção de dados, para que o legislador, o Poder Judiciário, os titulares e os agentes de tratamento possam seguir ao se depararem com problemas envolvendo o tema.

Para a compreensão de princípios, adota-se, aqui, o conceito formulado pelo jurista Robert Alexy, que formulou sua teoria dos direitos fundamentais em 1979. Segundo o jurista, princípios são normas que "ordenam que algo deva ser realizado na maior medida possível, para dentro das possibilidades jurídicas e fáticas existentes" (2008, p. 90).

Para Alexy, os princípios consistem em mandamentos de otimização, que incorporam conteúdos morais do ordenamento em que estão inseridos e trazem algumas premissas básicas do dever ou da proibição. Em razão destas características, possuem uma conotação axiológica.

Além disso, ele explica que os princípios podem ser satisfeitos em diferentes graus, dependendo das possibilidades do caso concreto, isto é, se o fato de se adequar ou não à norma, e das limitações jurídicas, as quais podem ser compreendidas como eventuais colisões entre diferentes princípios.

Com isso, diferencia os princípios das regras, as quais, ao seu ver, trazem direitos e deveres definitivos, cuja aplicação depende da subsunção, ou seja, elas podem ser ou não satisfeitas, não havendo um meio-termo entre mais de uma regra.

A partir desta perspectiva, Alexy sugere que haja uma vinculação entre a textura aberta da norma jurídica e aquele sujeito que era interpretá-la ou aplicá-la. Ou seja, cabe ao intérprete decidir dentro das limitações sugeridas pelos princípios. Ainda, em caso de conflito, deverá ser aplicada uma técnica de ponderação entre os princípios, a fim de que prevaleça aquele que tenha mais peso sobre a situação, segundo critérios de proporcionalidade, adequação e necessidade.

Os princípios, portanto, colaboram na interpretação da Lei Geral de Proteção de Dados Pessoais, que, como visto anteriormente, se diferencia por ser uma legislação mais "aberta" e

ampla. Eles são o cerne dessa norma jurídica, são fatores determinantes para a própria tutela dos dados pessoais e dos direitos fundamentais do indivíduo.

Assim sendo, o art. 6º traz, tanto no caput, quanto em seus incisos, alguns princípios pelos quais as atividades de tratamento de dados pessoais previstas na LGPD deverão ser orientadas: boa-fé, finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas. Abaixo, destacamos alguns de relevância para a análise desta pesquisa. A presença destes princípios pode ser identificada em todo o teor da lei, ao longo de seus dispositivos, reforçando a ideia de ser um sistema único e coerente.

Em primeiro lugar, logo no caput do art. 6º, há referência ao princípio da boa-fé objetiva, o qual atua como uma cláusula geral, uma diretriz, a ser seguida não apenas por aqueles que realizam atividades de tratamento de dados, mas por todo o ordenamento jurídico brasileiro.

Doutrinariamente, são apresentadas diversas definições a respeito deste princípio. Optamos por utilizar o conceito de Nunes (2010, p. 15), segundo o qual "a boa-fé objetiva consiste em um corolário do Direito e exige dos sujeitos das relações jurídicas uma postura leal, honesta e em conformidade com os padrões éticos vigentes". Nesta perspectiva, portanto, a boa-fé objetiva está atrelada às noções de lealdade e de confiança entre as partes, as quais deverão ser observadas no caso concreto.

A partir desta compreensão, em uma atividade que envolve tratamento de dados pessoais, é mister que aquele que realiza o tratamento o faça de forma a não ensejar qualquer tipo de abuso ou de lesão aos direitos fundamentais do titular de dados. O controlador e o operador devem agir com transparência, nos limites da eticidade.

Em relação ao princípio da finalidade (inc. I), este exige que a realização do tratamento de dados pessoais seja orientada para propósitos legítimos, específicos, explícitos e informados ao titular.

Um propósito legítimo é aquele que tem correspondência com uma das bases legais previstas na LGPD. Ele é específico quando é precisamente identificado. E, por fim, é explícito quando é claramente revelado ou expresso ao titular. Estes requisitos visam garantir que todos os envolvidos tenham o mesmo entendimento inequívoco sobre a finalidade de determinado tratamento (MALDONADO; BLUM, 2020, p. 129).

Assim, a finalidade é justamente o motivo pelo qual o agente está tratando determinado dado. É ela quem traz as fronteiras de legalidade para determinado tratamento, delimitando seus propósitos. Por isso, a finalidade deve ficar clara para o titular, que, por sua vez, tem que efetivamente compreender o porquê daquele seu dado estar sendo tratado, bem como por quanto

tempo, quem terá acesso aos dados, se estes dados serão transmitidos a terceiros, entre outras informações e detalhes que se fizerem necessários para que o titular, de forma livre e consciente, possa compreender o tratamento e, se o caso, autorizá-lo.

A utilização dos dados pessoais, portanto, deverá corresponder à finalidade previamente informada ao titular. Qualquer tratamento realizado fora deste âmbito ou incompatível com a finalidade previamente anunciada implicará em uma abusividade por parte do agente de tratamento. Ademais, qualquer uso secundário dos dados somente poderá ser realizado quando for compatível com a finalidade original, ou seja, quando existir um elo entre elas, dentro das expectativas razoáveis do titular a respeito do tratamento.

Atrelado ao princípio da finalidade, está o da adequação (inc. II), segundo o qual deve haver compatibilidade lógica entre o tratamento e as finalidades previamente informadas ao titular, dentro do contexto do tratamento, bem como da necessidade (inc. III), de acordo com o qual o tratamento deverá corresponder ao mínimo necessário para a realização das finalidades anunciadas.

Cabe ao titular questionar se o tratamento que está sendo feito é realmente necessário para atingir a finalidade que lhe foi anteriormente informada. Ou seja, se os dados coletados são realmente imprescindíveis para se atingir determinado objetivo, e não são excessivos. Sendo assim, em resumo, somente podem ser coletados os dados necessários para a finalidade previamente estabelecida.

No caso analisado, como já destacado, a coleta de dados pessoais dos usuários do metrô teve como principal objetivo o direcionamento de campanhas publicitárias. Para tanto, se fez uso de dados biométricos, considerados como dados pessoais sensíveis.

Referida atividade de tratamento de dados pessoais, consistente na coleta da imagem ou rosto do usuário para fins publicitários, por si só, envolve riscos aos direitos dos usuários, sobretudo ao direito de privacidade e da proteção de dados pessoais, tendo em vista que tal tratamento vai além das finalidades que se espera do uso do metrô, já que sua atividade-fim é tão somente permitir a locomoção de seus usuários, e não a realização de pesquisas de mercado e de direcionamento de mensagens publicitárias, ainda mais da forma que foi feita, sem consentimento e sem conhecimento dos próprios usuários do serviço.

Assim sendo, examinando a situação sob o aspecto do princípio da finalidade, verifica-se que o tratamento de dados realizado não corresponde às finalidades esperadas para o caso, isto é, para o uso do metrô. No caso, para uso do serviço bastaria informações cadastrais para a compra dos tickets e consequente identificação do usuário, nada além disso.

Além disso, observa-se que referida finalidade sequer foi informada para os titulares de dados, que nunca tiveram conhecimento de que seus dados estavam sendo coletados e utilizados como forma de direcionamento de campanhas publicitárias.

Assim, não houve, na coleta de dados pela ViaQuatro, a demonstração da relação necessária entre o tratamento de dados pessoais realizado e o fim buscado, o que seria essencial para se comprovar a adequação do tratamento. Com isso, os princípios da necessidade e da adequação não foram atendidos e sequer puderam ser efetivamente avaliados, ante a falta de elementos comprobatórios.

Neste diapasão, importante destacar que não foi apresentada qualquer razão legítima para que terceiros tenham acesso a estes dados sensíveis. A esse respeito, não se afigura legítimo que a concessionária transfira tais dados com a finalidade de atender a interesses meramente privados e comerciais. As informações eventualmente coletadas pelo metrô somente deveriam ser utilizadas para as específicas finalidades do serviço executado. É fundamental que haja uma justificativa adequada, pautada em lei, para a coleta e, principalmente, para o compartilhamento de tais dados.

Ressalta-se, mais uma vez, que é direito do cidadão ser devidamente informado a respeito da finalidade para a qual seus dados estão sendo coletados.

Do mesmo modo, é importante o tratamento se orientar pelo princípio da proporcionalidade, embora este não esteja expressamente previsto na LGPD, segundo o qual deve haver uma compatibilidade entre os dados tratados, a operação envolvida e os resultados almejados com os eventuais riscos aos direitos fundamentais do titular (MALDONADO; BLUM, 2020, p. 134).

Sob a perspectiva deste princípio, a coleta de dados biométricos para fins publicitários tem como consequência uma violação ao direito à proteção de dados pessoais em um âmbito muito maior do que se esperaria naquela situação, já que, com o compartilhamento dos dados referentes à sua imagem, foi possível aos terceiros, receptores dos dados, conhecer também suas emoções e interesses em relação à publicidade que era veiculada. Ou seja, os danos ao titular são proporcionalmente maiores à necessidade da coleta.

O livre acesso ao titular (inc. IV), de forma simples e gratuita, aos seus dados que foram tratados pela concessionária também não foi respeitado. Esse princípio implica que o titular tenha acesso a todas as informações sobre o tratamento de seus dados, para que possa controlar o fluxo informacional que lhe diga respeito, inclusive, se for de seu interesse, requerer a

correção de dados utilizados de forma incorreta ou, até mesmo, o descarte de dados coletados de forma excessiva ou ilícita.

No caso, o usuário, em nenhum momento, teve a oportunidade de consultar os dados que estavam sendo tratados, já que sequer sabia do tratamento. Pelo contrário, a situação retratada correspondia a uma coleta totalmente obrigatória de dados, já que os titulares, simplesmente por passarem naquela região, tinham suas informações pessoais coletadas, não podendo exercer qualquer tipo de consentimento.

O princípio do livre acesso também exige que os titulares tenham acesso ao banco de dados onde suas informações estão armazenadas e, ainda que, de forma ampla, possam corrigi-las, atualizá-las e até eliminá-las.

Em relação à qualidade dos dados (inc. V), tendo em vista que os titulares dos dados sequer sabiam da coleta e do tratamento que estava sendo realizado, não resta dúvidas de que referido princípio não foi respeitado, uma vez que em nenhum momento foram prestadas, pela controladora, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento. O princípio da qualidade está diretamente relacionado à proteção da personalidade do titular, uma vez que qualquer imprecisão ou equívoco no dado poderá afetar a construção do perfil do titular e, assim, intervir de forma catastrófica em sua vida.

Como decorrência deste princípio, exige-se também a atualização constante dos dados pessoais do titular, justamente para que não haja qualquer tratamento equivocado.

Também houve infração ao princípio da transparência (inc. VI), uma vez que os usuários não receberam informações claras, precisas e facilmente acessíveis sobre o que estava sendo objeto de coleta e de tratamento. O titular não soube como os dados estavam sendo utilizados, nem por quanto tempo ficariam armazenados.

O princípio da transparência implica que o controlador apresente de forma clara e concisa qual a finalidade, adequação e necessidade do uso do dado solicitado, bem como seja especificado quais os dados serão utilizados, para quem serão repassados e por qual motivo. Em síntese, ele exige que o agente de tratamento exponha ao titular todas as circunstâncias que envolvem o uso de seus dados, para que o usuário possa exercer o direito de autodeterminação informativa.

O titular jamais pode ser “pego de surpresa” com determinado tratamento, sem ter ciência de que seus dados estão sendo utilizados em determinada situação. Sob essa perspectiva, no caso em tela, sem dúvida, houve infração deste princípio.

Outro ponto a se destacar é que em nenhum momento foi apresentado pela concessionária qualquer mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, violando diretamente os princípios da segurança (inc. VII), que exige justamente do agente de tratamento a utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de violações dolosas e acidentais;

Atrelado ao princípio da segurança, o princípio da prevenção (inc. VIII) obriga os agentes a adotarem medidas para mitigar riscos e prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. Aqui, é obrigação do agente de tratamento formular regras de boas práticas e de governança, com as devidas normas de organização e com a disposição de obrigações para aqueles que, eventualmente, forem ter acesso aos dados.

A ausência de medidas de proteção, antes, durante e após o tratamento, é perigosíssima ao titular que, em eventual violação de dados, poderá sofrer danos irreparáveis em seus direitos fundamentais. Assim, houve falha da ViaQuatro em determinar os padrões de segurança do tratamento.

Neste mesmo sentido, o princípio da responsabilização e da prestação de contas (inc. X) exige que o agente de tratamento demonstre que aplicou todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas, vez que ele é o responsável pela fiel observância da LGPD, sob pena de ter que reparar os danos causados ao titular. Essa responsabilidade envolve todo o ciclo do tratamento e depende do cumprimento dos demais princípios previstos em lei.

É justamente esse o debate central da ação estudada nesta dissertação, pois nela discute-se se a conduta da ViaQuatro foi a causadora de danos aos titulares dos dados por ela coletados e, em caso positivo, quais as implicações para a concessionária.

Por fim, aqui, importante trazer uma ressalva em relação ao princípio da discriminação (inc. IX): esta não será analisado detalhadamente neste tópico, pois apenas com os elementos juntados aos autos, os quais foram objeto deste estudo de caso na pesquisa, não foi possível verificar se o tratamento era utilizado para fins discriminatórios ilícitos ou abusivos, seja criando estereótipos dos usuários do metrô, por exemplo, seja limitando direitos a estes usuários (segregação).

De qualquer forma, ressalta-se que a observância do princípio da não discriminação se mostra fundamental, com o intuito de se estabelecer limites no processamento de dados, principalmente naqueles realizados por meio de decisões automatizadas. Neste diapasão, cabe

ao controlador desenvolver medidas técnicas e administrativas que inviabilizem o tratamento discriminatório de dados.

A tutela da privacidade e da proteção de dados pessoais, portanto, depende da observação dos princípios previstos na LGPD, que atuam como cláusula mais geral, orientadora das práticas dos agentes de tratamento. Somente desta maneira é que se criará um ambiente no qual o titular possa exercer plenamente os seus direitos.

O uso de informações pelas empresas, voltadas para fins desconhecidos e que sequer trariam benefícios ao titular, como ocorreu no caso, não pode prejudicar o espaço de liberdade e de controle dos cidadãos, que deve ter seu direito garantido e protegido.

Neste aspecto, o tratamento de dados pessoais pela concessionária vai de encontro aos princípios tutelados em lei, ferindo, por consequência, os direitos da privacidade em sentido amplo e da proteção de dados pessoais, bem como o livre desenvolvimento da personalidade e a dignidade da pessoa humana.

4.4 Contribuições da legislação Europeia sobre o tema

Embora nos últimos anos tenhamos tido muito avanço nos estudos envolvendo a privacidade e a proteção de dados pessoais, algumas questões mais específicas, como a que é objeto desta pesquisa - coleta de dados pessoais biométricos por meio de tecnologias de reconhecimento facial- ainda não possuem tanta regulamentação no ordenamento jurídico do Brasil, sobretudo em relação a problemáticas mais práticas. Aliás, sequer existem mecanismos de controle e de prestação de contas voltados para tais sistemas.

Por esta razão, nesta parte do trabalho, optou-se por trazer alguns apontamentos oriundos de estudos realizados no âmbito da legislação europeia, principalmente do Reino Unido, e do GDPR que possam trazer paradigmas para orientar a melhor forma de se tutelar o direito à proteção dos dados pessoais quando nos deparamos com o tratamento de dados biométricos por particulares. Naquele ordenamento, inclusive, é muito comum a construção de pareceres objetivos sobre temas importantes.

Assim, nesta parte da pesquisa, foram consultados o “Guidelines 3/2019 on processing of personal data through video devices” desenvolvido pelo Conselho Europeu de Proteção de Dados, o “EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Councillaying down harmonised rules on artificial intelligence (Artificial Intelligence Act)”, elaborado em conjunto pelo Parlamento Europeu e pelo Conselho, o “Guide

to Data Protection - Guidance on video surveillance" desenvolvido pelo Information Commissioner's Office (ICO), autoridade do Reino Unido e, por fim, o "Guidelines on Facial Recognition" (Convenção 108) do Conselho da Europa.

Referidos estudos foram desenvolvidos com o intuito de trazer recomendações para as organizações, tanto do setor público, quanto do privado, que usam tecnologias de coleta de dados pessoais biométricos, como imagens de vídeo, para estas se adequarem aos princípios de proteção de dados.

A conformidade com a lei é fundamental para a implantação de um sistema eficiente. Além disso, sabendo que as medidas de cautela estão sendo tomadas, os cidadãos passam a sentir maior confiança no tratamento de seus dados pelos controladores e pelos operadores. Por fim, também evita que os agentes de tratamento sofram penalidades.

Os pareceres alertam que a quantidade de dados pessoais gerados pela coleta de imagens de vídeo, combinados com ferramentas e técnicas da inteligência artificial aumentam não apenas os riscos de uso indevido ou secundário dos dados, ou seja, um tratamento que não está relacionados ao propósito original do sistema, mas também os riscos relacionados a possíveis preconceitos que aquela coleta pode induzir.

Isso porque o software pelo qual o algoritmo é programado para identificação facial varia de acordo com a idade, sexo, etnia, o que pode, dependendo das informações que formularam esse algoritmo, reforçar preconceitos existente na sociedade. Um dado aparentemente insignificante pode acabar revelando um conteúdo de natureza altamente pessoal ou, ainda, pode ser utilizado para inferir informações sensíveis daquele titular.

Outro ponto de especial relevância é que dependendo do espaço monitorado e do número de pessoas que frequentam este local, o risco potencial de uso indevido é maior. Assim, o uso de tecnologia de reconhecimento facial em espaços públicos pode ser ainda mais intrusivo, sobretudo se a coleta de dados ocorrer sem o conhecimento de seu titular.

Por esta razão, antes de optar pelo tratamento, é fundamental que o controlador analise o nível de risco e/ou de dano que determinada tecnologia poderá gerar aos indivíduos. Cabe àquele ainda avaliar se o uso da tecnologia é realmente a forma necessária e proporcional de lidar com determinada situação. A tecnologia não deve ser usada simplesmente porque é "nova" ou é "mais rápida", enfim, ela deve ser utilizada com fundamento em justificativas plausíveis, que demonstrem que, naquelas circunstâncias, o uso de reconhecimento facial é a melhor maneira de resolver determinada situação e de se atingir a finalidade buscada.

Assim, antes de se realizar qualquer tratamento de imagem facial, os pareceres recomendam que sejam considerados métodos alternativos e menos invasivos da privacidade - como utilizar uma senha, um crachá- e que, caso não haja esta escolha, se justifique porque tais métodos não foram considerados adequados para a finalidade pretendida. Ou seja, o controlador não pode, simplesmente, realizar a coleta da imagem para atingir determinado objetivo. Cabe a ele justificar o porquê do tratamento de dados pessoais biométricos, em detrimento dos demais.

Especificamente em relação ao caso estudado, por exemplo, milhares de pessoas frequentam diariamente o espaço do metrô, de maneira que muitos dados são coletados a cada instante, agrupados de inúmeras maneiras. Assim, é mister verificar se não existe qualquer irregularidade que possa prejudicar os direitos do titular e se a coleta de dados biométricos era realmente a forma mais adequada de se atingir o objetivo dos agentes de tratamento.

Um dos documentos, ao analisar especificamente os sistemas de reconhecimento facial, traz uma diferenciação nos cuidados de acordo com o setor que o estiver utilizando: se for público (autoridade público), a justificação deverá estar prevista em lei ou, ainda, fundamentada em propósitos legítimos; agora, se for privado, exige-se a obtenção do consentimento dos titulares, de forma explícita, específica, livre e informada, independentemente se a coleta for para fins de autenticação ou de verificação.

Cabe ao agente de tratamento, posteriormente, ter meios adequados para comprovar que o consentimento ocorreu. Em razão disso, o reconhecimento facial só pode ser utilizado em um ambiente no qual se possa ter esse controle dos usuários.

Os pareceres estudados também recomendam que os propósitos da coleta de dados biométricos sejam documentos por escrito, a fim de deixar claro todo o procedimento realizado pelo agente de tratamento, desde o estágio inicial de determinado projeto, até a fase de término do tratamento.

Tais registros devem conter, por exemplo, a finalidade do tratamento, o tempo, as formas de exclusão dos dados, eventuais compartilhamentos de informações com terceiros, possibilidades de riscos e como saná-los, etc., ou seja, todos os detalhes possíveis sobre a operação para que caso, futuramente, o controlador receba alguma notificação ou punição, ele possa demonstrar sua preocupação com a regularidade do tratamento e com os direitos do titular.

Isso colabora com o atendimento do princípio da responsabilidade, segundo o qual o agente é responsável por tudo aquilo que faz com os dados por ele coletados. Ainda, garante a obediência aos princípios orientadores da proteção de dados pessoais, referidos no GDPR, que

trazem a obrigação de os agentes implementarem medidas técnicas e organizacionais apropriadas ao tratamento.

Tal mandamento aparece na LGPD, razão pela qual, no âmbito brasileiro, também é importante que os agentes sigam as orientações abaixo para demonstrar sua conformidade com a matéria.

É importante que se analise todo o contexto envolvido naquele tratamento, desde qual informação é coletada, qual a extensão espacial em que a coleta ocorre, quantos titulares estarão envolvidos, qual o escopo do tratamento, se este está dentro das expectativas razoáveis dos titulares cujos dados são processados e, principalmente, quais os possíveis impactos do tratamento nos direitos e liberdade dos indivíduos.

Além disso, a finalidade, que deve ser lícita e justa, também deve ser especificada. Os dados pessoais tratados devem ser adequados, relevantes e limitados ao que for necessário para determinado objetivo. Assim sendo, o uso de captura de imagem de reconhecimento facial deve atingir a finalidade previamente estabelecida pelo controlador.

O GDPR, em seu artigo 6º[23], atendendo ao princípio da legalidade, também traz a obrigação de fundamentar o tratamento realizado em uma base legal adequada, identificando-a no momento da coleta. O processamento de dados deverá ser necessário e proporcional à base legal e à finalidade escolhidas. No que se refere especificamente aos dados pessoais biométricos, por se tratar de dados de categoria especial, as hipóteses de base legal, como vimos, são ainda mais limitadas.

Todos aqueles que eventualmente irão operar o sistema, deverão ter conhecimento da finalidade escolhida e da base legal utilizada para fundamentar o tratamento. Outra recomendação importante dos guias é no sentido de que as pessoas que operam tais sistemas devem ser devidamente treinadas para utilizar a tecnologia de forma adequada. As imagens coletadas devem ficar restritas a pessoas autorizadas a tratá-las, por meio de um procedimento seguro, que evite o vazamento de informações.

. Os dados pessoais coletados somente poderão ser utilizados em uma nova finalidade se esta for compatível com a original e, ainda, se for atrelada a uma obrigação estabelecida em lei. Caso contrário, deverá se obter novo consentimento, se esta for a base justificadora do tratamento.

[23] Art.6º Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (...).

Por outro lado, o titular deverá saber quem é o responsável por tomar as decisões referentes aos seus dados e quem deve contatar caso necessite exercer algum de seus direitos. Assim, a equipe do controlador deverá ser capacitada para responder demandas de acesso, exclusão ou correção de dados de forma rápida e eficiente, principalmente no tratamento de dados para fins de publicidade, ocasião em que, a qualquer momento, o titular poderá se opor.

No GDPR, inclusive, o direito de oposição ao marketing direto, ainda que feito de forma ampla, é absoluto e seu exercício deve ser possibilitado pelos controladores.

Ainda, os titulares precisam ter conhecimento, por meio de uma sinalização adequada, visível e legível, de onde e porquê - qual a finalidade- está ocorrendo a coleta de seus dados. Ou seja, todos os pontos em que haverá a coleta de imagem por reconhecimento facial deverão estar separados e delimitados, a fim de que o titular possa reconhecer com facilidade as circunstâncias do tratamento, bem como para que não se capture dados de pessoas que não consentiram com aquele.

As informações devem ser fornecidas em um local que fique antes da área em que a coleta está correndo, justamente para evitar que os indivíduos sejam monitorados sem saber.

No caso da coleta de dados por reconhecimento facial, cada câmera que eventualmente realizar a coleta deverá ser mencionada, para total conhecimento dos titulares acerca do processamento. Isto reflete o teor dos artigos 5º[24] e 13[25] do GDPR. Além disso, os próprios outdoors ou sistemas de reconhecimento facial utilizados devem informar o titular sobre a captura dos dados biométricos.

Outra sugestão dos guias analisados é que as mídias sociais da plataforma que faz a coleta de imagem informem previamente que em determinada área de sua operação, ocorrerá o tratamento de dados pessoais biométricos.

No que diz respeito ao uso de dados pessoais biométricos para fins de marketing, os pareceres analisados entendem que deverá ser utilizada a base legal do consentimento, o qual deverá ser obtido de forma explícita e válida de todos os titulares cujos dados serão tratados.

A escolha dada aos indivíduos deve ser totalmente informada e dada de forma livre, para que o titular possa escolher estar ou não sujeito ao processamento de seus dados. Além disso, é fundamental que a obtenção do consentimento seja devidamente comprovada pelo controlador - é evidente que, na prática, é difícil obter consentimento dos indivíduos para coleta de seus dados em espaços públicos.

[24] Art.5º Principles relating to processing of personal data (...);
[25] Art. 13 Information to be provided where personal data are collected from the data subject (...);

Outra preocupação que deve ser observada pelos controladores é que os dados extraídos não sejam excessivos, de modo que deverão ser coletadas apenas as informações minimamente necessárias para a finalidade anteriormente especificada ao titular, evitando, desta maneira, qualquer novo tratamento posterior.

Os dados pessoais biométricos que eventualmente forem armazenados, deverão ser incluídos em uma base de dados segura, protegida, por exemplo, por criptografia com uma chave de segredo que fica restrita a um grupo mínimo de pessoas, impedindo, assim, qualquer acesso não autorizado.

É tarefa do controlador tomar todas as medidas necessárias para preservar a disponibilidade, a integridade e a confidencialidade dos dados tratados. Além disso, se o armazenamento envolver algum provedor de nuvem de terceiro, é tarefa daquele que o contratou verificar se o provedor oferece medidas técnicas de segurança ao tratamento de dados.

O tempo deste armazenamento também deverá ser previamente informado e definido individualmente para a finalidade almejada, devendo ser o mais curto possível. Dados pessoais armazenados por muito tempo serão considerados desnecessários. O sistema deverá ser constantemente monitorado, a fim de verificar se o período de armazenamento está sendo cumprido.

Caso mais de um controlador esteja envolvido no processo ou, ainda, caso haja compartilhamento dos dados coletados com terceiros, é importante esclarecer as obrigações e as responsabilidades de cada um, por meio de um documento escrito, que deixe claro aquilo que foi acordado entre as partes.

Após o uso, os dados deverão ser eliminados de forma eficaz, a fim de que não sejam utilizados indevidamente por terceiros. Assim, antes de iniciar o tratamento, o agente já deve desenvolver medidas que, futuramente, garantirão a eliminação permanente e segura dos dados coletados.

Por fim, cabe aos controladores avaliar o impacto do tratamento de dados pessoais nos direitos e liberdades fundamentais do indivíduo, buscando um equilíbrio entre a finalidade por ele buscada e mecanismos que sejam menos intrusivos para se alcançar tal propósito. Além disso, os controladores devem garantir que o titular possa exercer todos os direitos relativos à tutela de seus dados pessoais.

Frente a este contexto, na União Europeia, já existe uma proposta de legislação desenvolvida pelo Parlamento Europeu, na qual se propõe que os programas de reconhecimento facial e de identificação biométrica só sejam utilizados se possuírem um nível de segurança

adequado e se preencherem os requisitos de conformidade previamente estipulados na legislação, tais como: gestão de risco, mecanismos de supervisão do sistema e das pessoas que têm acesso às informações.

Se ainda com todos estes cuidados houver qualquer uso inadequado ou excessivo dos dados, cabe ao agente de tratamento notificar a autoridade de proteção de dados pessoais, responsável pela matéria em seu país, a fim de informar o ocorrido e, de forma conjunta, buscar a melhor solução para a tutela do titular.

4.5 Algumas hipóteses legítimas de tratamento de dados pessoais biométricos por câmeras de vídeo

O estudo de caso apresentado, por se tratar de matéria recente e nova na temática de proteção de dados pessoais, carrega ainda alguns questionamentos sobre as eventuais situações nas quais o tratamento de dados pessoais biométricos, por meio de reconhecimento facial, seria possível.

A pesquisa não pretende se estender em todas as hipóteses aplicáveis ao caso, mas tão somente destacar aquelas que levantam mais dúvidas na sociedade e que comumente são acionadas pelos controladores e operadores.

A primeira delas é a coleta de dados biométricos quando houver consentimento do titular. Como vimos, a LGPD, em seu art. 5º, inc. XII, define o consentimento como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada".

Em complemento, o inc. I do art. 11 da mesma lei permite que haja o tratamento de dados sensíveis quando o seu titular (ou responsável) consentir para as finalidades que lhe tiverem sido previamente informadas:

> 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;

Neste sentido, no caso estudado, é possível que seja empregada a base legal do consentimento como forma de fundamentar o tratamento de dados realizado pela ViaQuatro, a fim de que os titulares não apenas tenham conhecimento sobre a captação de sua imagem pelas Portas Interativas, mas consintam com ele.

Para tanto, a empresa deveria fornecer ao titular o acesso a um documento que esclareça tudo aquilo que for relevante sobre o tratamento que está sendo realizado com seus dados.

Frente a esta problemática, uma alternativa seria a de instalar cabines ou totens em espaços na área de passagem, onde deveriam ser disponibilizadas informações claras e adequadas sobre o tratamento, a fim de que o usuário entendesse a operação realizada e, após, manifestasse expressamente sua vontade em contribuir- ou não- para a pesquisa de opinião.

Contudo, trata-se de base legal de difícil aplicação prática, uma vez que, diariamente, milhares de pessoas frequentam o espaço em que as câmeras estão instaladas, para utilizarem o metrô. Assim, elaborar os termos e obter o consentimento destes usuários seria uma diligência demasiadamente trabalhosa, que prejudicaria o fluxo de pessoas naquele ambiente.

Além disso, trata-se de prática que, dificilmente, poderia ser comprovada, tendo em vista que a controladora não consegue enumerar precisamente a quantidade de usuários que passam pelas câmeras e, desta forma, indicar se todos efetivamente preencheram os termos de consentimento permitindo a captura de sua imagem.

Outra hipótese em que se verifica a coleta da imagem por câmeras é a dos controladores que utilizam o reconhecimento facial em seus sistemas de segurança.

Tal situação, embora adote a mesma sistemática do caso estudado, se diferencia justamente pela finalidade que define o tratamento de dados pessoais.

Enquanto nas Portas Digitais Interativas a finalidade da coleta era de cunho comercial (coletar as emoções dos usuários e, com base nelas, direcionar as propagandas publicitárias que seriam veiculadas no equipamento), as imagens coletadas por câmeras de segurança têm o intuito de identificar e/ ou autenticar usuários para proteger determinada propriedade ou as pessoas que frequentam determinado espaço.

Assim, caso a ViaQuatro tivesse informado que a finalidade da coleta de imagem era para manter a proteção e/ou segurança dos usuários, por exemplo, tal captura seria possível, tendo em vista que uma das obrigações da concessionária de serviço público é justamente zelar pela segurança de seus usuários, dentro de suas áreas de dependência, de acordo com os termos da Lei Federal nº 6.149/1974:

> Art. 1º A segurança do transporte metroviário incumbe a pessoa jurídica que o execute, observado o disposto nesta Lei, no regulamento do serviço e nas instruções de operações de tráfego.

A base legal, nesta hipótese, está prevista na alínea “g” do inc. II do art. 11 da LGPD:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> (...)
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> (...)
> 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.

Aqui, mais uma vez, a preocupação do legislador é com o próprio titular de dados.

Em relação à primeira possibilidade (fraude), nota-se que o objetivo desta proteção é impedir que alguém obtenha vantagem indevida sobre aquele titular, como, por exemplo, se apropriando ilegalmente de seus dados pessoais. O uso de dados biométricos, nesta situação, é uma alternativa para autenticar o verdadeiro titular dos dados.

Em relação à segunda hipótese (segurança), entendemos que pode ser compreendida de forma ampla, englobando tanto a segurança física do titular, como, por exemplo, evitar acesso de pessoas não autorizadas, quanto a segurança da própria informação, a fim de impedir incidentes de segurança, como vazamento de dados.

Assim, nestas situações, o reconhecimento facial por meio da coleta de dados biométricos seria uma maneira de identificar com precisão o titular dos dados e, assim, evitar situações que possam comprometer sua segurança.

É evidente que, ainda nesta hipótese da alínea "g" a controladora deve informar aos usuários do serviço as finalidades da coleta, bem como o tempo de armazenamento dos dados e demais obrigações previstas na LGPD. Em síntese, deve ser demonstrado que o uso da ferramenta (câmeras) é uma medida adequada e eficaz para garantir ao titular sua própria segurança.

Ainda nesta situação, é fundamental que se busquem medidas técnicas aptas a proteger o direito à proteção de dados do titular, bem como seus demais direitos e liberdades fundamentais- ressalva que, inclusive, consta ao final da alínea “g”. Ou seja, deve haver uma compatibilidade entre o objetivo perseguido (segurança) e o direito tutelado.

Importante, neste ponto, informar que durante a elaboração da presente pesquisa, em 03/03/2.022, o IDEC ajuizou uma nova ação civil pública em face da ViaQuatro (processo nº 1010667-97.2022.8.26.0053), questionando justamente o tratamento de dados pessoais biométricos em um sistema de monitoramento e de segurança a ser implementado no metrô.

De acordo com o narrado pelo próprio IDEC, esse novo sistema pretende, por meio de software de reconhecimento facial, captar dados para fins de autenticação e identificação de usuário. Para o Instituto, esta prática configuraria abuso de direito na prestação de serviços e na execução de serviços públicos, razão pela qual requereu o impedimento da execução desse sistema de tratamento de dados.

A ViaQuatro, por sua vez, defendeu que esse programa seria utilizado para modernização do sistema de vigilância, com um monitoramento digital dos passageiros. E, ainda, acrescentou que o sistema seria utilizado para situações específicas, como, por exemplo, busca de pessoas desaparecidas, identificação de usuários que, eventualmente, tenham cometido infrações penais ou, por fim, busca após determinações judiciais.

Embora a liminar requerida pelo IDEC tenha sido parcialmente deferida pela magistrada em primeiro grau, determinando-se a suspensão da execução do sistema, posteriormente, em 13/10/2.022, foi proferida decisão nos autos do Agravo de Instrumento nº 2079077-58.2022.8.26.000, na qual o Tribunal de Justiça de São Paulo entendeu ser prematura qualquer decisão determinando a suspensão do sistema, tendo em vista que ele sequer havia sido instalado, dependendo, naquele momento, de diversas etapas para que fosse efetivamente implantado.

O Relator designado, o Desembargador Fermino Magnani Filho, entendeu que seria essencial ouvir a parte contrária para analisar a necessidade da medida almejada, até porque, se o contrato fosse suspenso, poderia gera uma oneração dos cofres públicos, os quais não poderiam ficar à mercê do inefável tempo processual.

Um dos argumentos utilizados foi de que o art. 4º, inc. III, alíneas "a" e "d", da Lei Federal nº 13.709/2018, excepciona sua abrangência nos casos de tratamento de dados pessoais realizados para fins exclusivos de segurança pública e atividades de investigação e repressão de infrações penais e que o metrô, no âmbito de suas instalações, possui o poder de polícia, nos termos do artigo 2º da Lei Federal nº 6.149/1974[26], a qual dispõe, justamente, sobre a segurança do transporte metroviário, além de dar outras providências.

O tema é bastante complexo, tanto que, no próprio Tribunal, a decisão não foi unânime, tendo o voto vencido, proferido pela Desembargadora Maria concluído que:

[26] Art. 2º Para os fins desta Lei, incluem-se na segurança do transporte metroviário a preservação do patrimônio vinculado a ele, as medidas de natureza técnica, administrativa, policial e educativa que visem a regularidade do tráfego, a incolumidade e comodidade dos usuários, à prevenção de acidentes, a higiene e a manutenção da ordem em suas instalações.

> A instalação do sistema de monitoramento e reconhecimento facial parece estar sendo feito à revelia de uma avaliação prévia de impacto da proteção dos dados, especialmente considerando que o tratamento das referidas informações pode resultar em elevado risco para os direitos e liberdades das pessoas (...) o Metrô, em nenhum momento, forneceu explicações e/ou documentos a respeito das regras, condições, formas, prazos, entre outros, em que se dará o tratamento e, mais importante, o compartilhamento com outros órgãos, públicos ou privados — dos dados biométricos coletados de seus usuários.

No tocante à tramitação do processo em sua origem, o processo se encontra em fase de produção de provas, dentre as quais foi determinada a realização de prova pericial. Um dos pontos que, para a magistrada Cynthia Thome, é essencial neste caso, em que os dados pessoais, supostamente, são utilizados para fins de segurança, é verificar se existe transparência no tratamento dos dados, bem como se existem medidas para avaliar o impacto e mitigar os riscos inerentes à tecnologia de reconhecimento facial.

Até o presente momento, a perícia não foi realizada, estando, ainda, sendo elaborados e validados os quesitos a serem respondidos pelo perito.

De qualquer modo, frente à problemática apresentada nesta pesquisa, nota-se que a prova pericial é uma das mais importantes, tendo em vista que ela permite que sejam apreciadas questões técnicas envolvendo o sistema de captação e de monitoramento de imagens da ViaQuatro.

Assim, tal prova irá colaborar na compreensão das funcionalidades do sistema como um todo e, consequentemente, poderá trazer subsídios para se apreciar possíveis violações dos direitos do titular, sobretudo do direito à privacidade e à proteção de dados pessoais.

Pela análise das decisões proferidas até o presente momento no caso, é possível perceber que, ainda que a base legal utilizada seja a segurança do titular, alguns cuidados devem ser tomados pela parte controladora. É importante que todas as informações a respeito do tratamento de dados sejam fornecidas de forma clara, contendo, por exemplo, as condições do sistema de reconhecimento facial utilizado, isto é, como ele opera.

Além disso, é essencial esclarecer como os dados pessoais serão armazenados neste sistema e por quanto tempo. Também é fundamental informar a respeito de eventual compartilhamento dos dados coletados com outros bancos de dados.

Assim sendo, embora se reconheça que o Estado deva, em nome do interesse público, promover a segurança dos indivíduos, essa prerrogativa jamais deve ser utilizada como justificativa para um tratamento ilimitado de dados e, ainda, que violem os demais direitos e fundamentos defendidos pelo Estado Democrático de Direito.

Uma terceira hipótese da utilização das câmeras que, inclusive, foi utilizada na defesa da ViaQuatro, é a coleta de dados pessoais para fins estatísticos, de estudos por órgãos de pesquisa, nos termos da alínea "c" do inc. II do art. 11 da LGPD:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> (...)
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> (...)
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

Nesta situação, é obrigação do controlador demonstrar cabalmente que os dados biométricos coletados serão utilizados para tal finalidade e, ainda, que os dados coletados são anonimizados, com o intuito de não identificar o usuário ao qual o dado corresponde. Não basta, simplesmente, alegar que não há reconhecimento facial.

Assim sendo, a base legal acima deve ser utilizada com cuidado, tendo em vista que, havendo qualquer tipo de questionamento pelo titular, ou pela própria ANPD, caberá ao agente de tratamento produzir as provas competentes, a fim de demonstrar que o tratamento está ocorrendo de acordo com o que foi previamente informado - e não está exercendo referida finalidade.

Não basta, simplesmente, que a parte alegue que esteja efetuando o tratamento para fins de pesquisa. Cabe a ela comprovar tal assertiva, por meio de relatórios técnicos, como, por exemplo, o Relatório de Impacto à Proteção de Dados Pessoais, (RIPDP), que é a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco", conforme o disposto no art. 5º, XVII, da LGPD.

Nesta situação, também é importante que o agente de tratamento faça a anonimização dos dados pessoais tratados, com o intuito de garantir a segurança do titular. Isto porque, com a anonimização, os dados deixam de estar vinculados a um único sujeito, tornando impossível sua identificação.

No caso, foi justamente com base nesta argumentação que a sentença rejeitou a tese de defesa da ViaQuatro, tendo em vista que a requerida não trouxe qualquer prova a respeito de suas alegações, sequer solicitando a produção de prova pericial.

Outras hipóteses, embora não tão comuns na prática, e que poderiam justificar o tratamento de dados pessoais biométricos seriam as previstas nas alíneas “e” e “f” do art. 11:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> (...)
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> (...)
> 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;

Tais hipóteses estão relacionadas diretamente à proteção da saúde e da vida do titular como um todo, como, por exemplo, em situações de urgência médica- identificar o titular por meio do reconhecimento facial e, a partir deste reconhecimento, tomar conhecimento de suas condições de saúde-, nas quais a obtenção do consentimento poderia atrasar determinado procedimento e, com isso, gerar prejuízos e danos irreparáveis ao titular.

5 CONSIDERAÇÕES SOBRE A POLÍTICA DE PRIVACIDADE DA VIAQUATRO DE ACORDO COM AS DIRETRIZES DA LGPD

Finalmente, nesta última etapa da pesquisa, tendo como base teórica toda a leitura realizada até o presente momento, pretende-se realizar uma análise crítica sobre a política de privacidade da ViaQuatro, à luz dos princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais.

A ideia de elaborar uma política de privacidade surge justamente por conta da responsabilidade dos agentes, sejam eles controladores ou operadores, informarem o titular de dados, de forma transparente, tudo aquilo que envolve o tratamento de seus dados pessoais. Assim, nesta parte da pesquisa, objetiva-se verificar se a política de privacidade da empresa ViaQuatro garante uma proteção de dados pessoais de maneira eficiente.

Esclarece-se que o documento a ser analisado é a Política de Privacidade que foi disponibilizada pela própria ViaQuatro, em seu sítio eletrônico[27], isto é, aquela que é direcionada para pessoas externas à organização, com o intuito de esclarecer aos usuários do serviço todos os trâmites envolvendo a coleta e o uso de dados pela empresa, bem como as finalidades para as quais estes são tratados

É importante, aqui, efetuar esta distinção, pois algumas organizações possuem também uma política de privacidade interna, voltada para as regras e diretrizes aplicadas dentro da pessoa jurídica, que, portanto, não será objeto deste trabalho.

As Políticas de Privacidade, na situação estudada, têm o intuito de informar aos usuários de determinado serviço quais as informações que são por ele coletadas, bem como a forma do tratamento, a finalidade e, ainda, alguns aspectos mais particulares daquele serviço, como, por exemplo, se as informações são compartilhadas com terceiro, se há alguma transferência internacional, entre outros (KLAFKE *et al*, 2020, p. 11). Ou seja, ela deverá descrever todos os procedimentos adotados no tratamento de dados pessoais realizado por aquele serviço.

A partir da leitura da Política de Privacidade, o usuário, titular de dados, consegue ter uma breve noção do que esperar da utilização de determinado serviço e quais as consequências deste uso no tocante à proteção de sua privacidade e de seus dados pessoais. É fundamental que o titular tenha conhecimento de qualquer restrição que possa ser feita em seus direitos quando ele opta por usufruir de determinado serviço.

---

[27] Política de Privacidade da Concessionária da Linha 4 do Metrô de São Paulo S/A. Disponível em: <https://www.viaquatro.com.br/politica-de-privacidade>. Acesso em 11 jul. 2023

Ademais, a Política deve apresentar de forma clara a maneira pela qual o usuário poderá, eventualmente, se manifestar sobre o tratamento de seus dados.

Por estas razões, é mister que o documento seja claro e objetivo, editado em linguagem acessível e simples. Além disso, ele deverá ser exposto em local de fácil acesso e visualização, sendo constantemente atualizado.

Sobre esta problemática, como vimos, a LGPD traz de forma expressa alguns princípios que devem ser seguidos para garantir a privacidade dos dados pessoais coletados pelos agentes de tratamento. Isto posto, cabe, aqui, reproduzir novamente o artigo 6º da lei, em que constam tais princípios, para possibilitar uma melhor compreensão do leitor.

Com base nos estudos teóricos realizados neste trabalho e, ainda, levando em consideração os princípios acima, aliados à experiência prática da autora da pesquisa na área de proteção de dados pessoais, inclusive na elaboração de termos e políticas da área, buscou-se desenvolver algumas perguntas objetivas para analisar de forma crítica se a Política de Privacidade da ViaQuatro garante de forma efetiva o direito à privacidade e à proteção de dados pessoais de seus usuários.

Além disso, outro material de apoio para esta investigação é o "Guia de Elaboração do Termo de Uso e Política de Privacidade para serviços públicos" elaborado pela Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, desenvolvido justamente para orientar os agentes de tratamento sobre a melhor forma de adequar suas políticas de privacidade à Lei Geral de Proteção de Dados Pessoais.

Isto posto, abaixo, responderemos a cada uma das perguntas de acordo com a última versão da Política de Privacidade disponibilizada pela empresa. Assim, as respostas trazidas abaixo foram retiradas diretamente do site da Via Quatro. Importante esclarecer que no site consta que a Política foi atualizada em abril de 2023.

Além disso, durante a realização da presente pesquisa, entre os anos de 2022 e 2023, foi possível perceber que houve atualizações da Política de Privacidade da Via Quatro, o que demonstra que a empresa tem, aparentemente, se preocupado em manter sua política sempre atualizada, de acordo com os procedimentos desenvolvidos.

Com o intuito de tornar a leitura mais dinâmica e objetiva e, ainda, de facilitar a análise das informações coletadas, optou-se por desenvolver um quadro (abaixo apresentado) formado por duas colunas, sendo a primeira as questões objeto de análise, formuladas pela pesquisadora,

e a segunda coluna as respostas encontradas no site da Concessionária. Destacamos ainda que as respostas foram copiadas exatamente da forma que se encontram no site.

PERGUNTAS PARA ANÁLISE DA POLÍTICA DE PRIVACIDADE - FORMULADAS PELA PESQUISADORA	RESPOSTAS LOCALIZADAS NO TEXTO DA POLÍTICA DE PRIVACIDADE DA VIAQUATRO
1- A Política informa quais são os dados coletados, mencionando, ainda, se há tratamento de dados pessoais sensíveis?	A empresa informa que coleta dados cadastrais, como nome, CPF, e-mail, gênero, telefone para contato, CEP e endereço completo; bem como dados de identificação digital, como endereço IP, porta lógica de origem. dispositivo (versão do sistema operacional), geolocalização, registros de data e horário de cada ação que o usuário realizar, telas que o usuário acessou, ID da sessão e cookies. Ademais, a empresa informa que os dados poderão ser coletados quando o próprio usuário os submete ou quando o usuário interage na plataforma. Ela alerta que caso o usuário opte por não fornecer alguns desses dados, alguns serviços poderão ficar impossibilitados de serem prestados total ou parcialmente pela empresa. Por fim, não consta qualquer referência específica sobre o tratamento de dados pessoais sensíveis. Dentre os dados tratados pela empresa, informados na Política e reproduzidos acima, não há dados sensíveis.

2- A Política fundamenta o tratamento de dados por ela realizado em alguma base legal?	Cumprir as obrigações legais e regulatórias da empresa.
3- As finalidades da coleta e do uso dos dados pessoais são informadas com clareza?	Sim. A empresa traz expressamente as finalidades da coleta, sendo que os dados cadastrais são coletados para identificar o usuário; cumprir as obrigações decorrentes do uso dos serviços da empresa; ampliar o relacionamento com a empresa, informando sobre novidades, funcionalidades, conteúdos, notícias e demais eventos que consideramos relevantes para; enriquecer a experiência do usuário com a empresa e promover seus produtos e serviços; e, por fim, cumprir obrigações legais e regulatórias. Já os dados de identificação digital são coletados para identificar o usuário; cumprir com obrigações legais de manutenção de registros estabelecidas pelo Marco Civil da Internet - Lei 12.965/2014; e cumprir obrigações legais e regulatórias.
4- A forma e o tempo de armazenamento dos dados pessoais são informados?	Há um tópico específico informando que os dados Pessoais coletados e os registros de atividades são armazenados em ambiente seguro e controlado nos servidores locais da empresa. Informa também que os dados coletados serão armazenados nos servidores da empresa localizados no Brasil, bem como em ambiente de uso de recursos ou servidores na nuvem (cloud computing), o que poderá

	exigir uma transferência e/ou processamento destes Dados fora do Brasil. A empresa diz ainda que a base de dados formada é de sua propriedade e está sob sua responsabilidade, sendo que o uso, acesso e compartilhamento desta base de dados, quando necessários, serão feitos dentro dos limites e propósitos dos negócios descritos na Política de Privacidade. Sobre o tempo de armazenamento, a empresa informa que os dados são armazenados pelo período necessário ao cumprimento das finalidades elencadas na Política de Privacidade, incluindo para o cumprimento de obrigações legais e contratuais no âmbito de contratos de concessão, permissão ou autorização. Informa, ainda que, para informações específicas sobre períodos de retenção de dados, o usuário pode entrar em contato com a empresa através do nosso canal de comunicação com o encarregado para a proteção de dados pessoais enviando um e-mail para: encarregado.dadospessoais@grupoccr.com.br. Além disso, a empresa informa que alguns dados são armazenados por períodos maiores para fins de auditoria, segurança, controle de fraudes, proteção ao crédito e preservação de direitos, de maneira que poderá permanecer com o histórico de registro dos Dados pessoais do usuário por prazo maior nas

	hipóteses que a lei ou norma regulatória assim estabelecer ou para preservação de direitos. Por fim, a empresa alerta que caso o titular solicite a exclusão de seus dados, pode ocorrer que estes precisem ser mantidos por período superior ao pedido de exclusão, nos termos do artigo 16 da Lei Geral de Proteção de Dados Pessoais, para (i) cumprimento de obrigação legal ou regulatória, (ii) estudo por órgão de pesquisa, e (iii) transferência a terceiro (respeitados os requisitos de tratamento de dados dispostos na mesma Lei). Somente findos o prazo de manutenção e a necessidade legal, os Dados Pessoais serão excluídos com uso de métodos de descarte seguro, ou utilizados de forma anonimizada para fins estatísticos.
5- Os direitos do titular dos dados são garantidos?	Sim. Existe um tópico específico sobre os direitos básicos do titular. A empresa informa que os direitos do titular são aqueles previstos na LGPD, quais sejam (i) confirmação da existência de tratamento dos seus dados pessoais; (ii) acesso aos seus dados pessoais; (iii) correção de dados pessoais incompletos, inexatos ou desatualizados; (iv) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, se aplicável; (v) portabilidade dos dados pessoais para outro fornecedor, sujeito

	à regulamentação da Autoridade Nacional (ANPD); (vi) solicitação de apagamento ou anonimização dos dados pessoais tratados com base no seu consentimento, exceto quando a lei autorizar a manutenção destes dados por outro fundamento; (vii) informações sobre as entidades públicas e privadas com as quais Nós tenhamos realizado o uso compartilhado dos seus dados pessoais; (viii) informações sobre a possibilidade de não consentir com o tratamento dos seus dados pessoais e as consequências de tal ação; e (ix) revogação de seu consentimento.
6- Existe informação sobre quem terá acesso aos dados coletados?	Sim. A empresa informa que os Dados Pessoais coletados são acessados somente por profissionais devidamente autorizados, respeitando os princípios de proporcionalidade, necessidade e relevância para os objetivos do nosso negócio, além do compromisso de confidencialidade e preservação da sua privacidade nos termos desta Política.
7- Existe informação sobre a transferência internacional de dados?	Sim. A empresa informa que como utiliza servidores na nuvem (cloud computing), tal situação poderá exigir uma transferência e/ou processamento destes Dados fora do Brasil.
8- Existe informação sobre eventual compartilhamento de dados com terceiros?	A empresa informa que não compartilha os dados pessoais coletados com terceiros, exceto nos seguintes casos: “i. Quando tivermos obtido o seu consentimento para o

	compartilhamento de seus dados pessoais; ii. Com empresas afiliadas dentro do grupo do VIAQUATRO; iii. Com prestadores de serviço e parceiros de negócio do VIAQUATRO, que realizem o tratamento de dados pessoais em nome do VIAQUATRO; iv. Com prestadores de serviço e parceiros de negócio da VIAQUATRO, no contexto do contrato de concessão, além de outras condutas ilícitas com risco de dano elevado, no interesse da VIAQUATRO e da proteção de terceiros; v. Com a Administração Pública, em cumprimento a obrigações legais e contratuais, inclusive no contexto de contratos de concessão, permissão ou autorização; vi. Com autoridades policiais conforme requerido pela lei ou quando razoavelmente necessário para proteger os direitos, a propriedade e/ou a segurança do Usuário, de terceiros e/ou do VIAQUATRO; vii. Com autoridades judiciais, administrativas ou governamentais competentes, sempre que houver determinação legal, requerimento, requisição ou ordem judicial; viii. Quando necessário às atividades comerciais e aos serviços prestados por nós por meio do https://www.viaquatro.com.br/; ix. De forma automática, em caso de movimentações societárias, como fusão, aquisição e incorporação. Informa ainda que, existe a possibilidade de compartilhamento para fins de pesquisas de

	inteligência de mercado, divulgação de dados à imprensa e realização de propagandas e que, nestes casos, os dados serão compartilhados de forma anonimizada. Por fim, também consta na Política que caso empresas terceirizadas realizem o tratamento de dados em nome da ViaQuatro, elas respeitarão as condições estipuladas na Política de Privacidade e as normas de segurança da informação.
9- São previstas medidas técnicas e administrativas visando à proteção e à segurança dos dados coletados?	A empresa não especifica as medidas por ela adotadas. Apenas informa que, na qualidade de agente controlador, tem como responsabilidade (i) registrar as atividades de tratamento; (ii) adotar medidas de segurança técnicas e administrativas; (iii) garantir a segurança da informação; (iv) atender aos direitos dos titulares; (v) cooperar com a Autoridade Nacional de Proteção de Dados; e (vi) garantir o atendimento aos princípios e bases legais da LGPD.
10- Existe informação sobre o término do tratamento? Ou sobre a revogação de consentimento pelo usuário?	Sim, no mesmo tópico que dispõe sobre o armazenamento. Sobre o tempo de armazenamento, a empresa informa que os dados são armazenados pelo período necessário ao cumprimento das finalidades elencadas na Política de Privacidade, incluindo para o cumprimento de obrigações legais e contratuais no âmbito de contratos de concessão, permissão ou autorização.

	Informa, ainda que, para informações específicas sobre períodos de retenção de dados, o usuário pode entrar em contato com a empresa através do nosso canal de comunicação com o encarregado para a proteção de dados pessoais enviando um e-mail para: encarregado.dadospessoais@grupoccr.com.br. Além disso, a empresa informa que alguns dados são armazenados por períodos maiores para fins de auditoria, segurança, controle de fraudes, proteção ao crédito e preservação de direitos, de maneira que poderá permanecer com o histórico de registro dos Dados pessoais do usuário por prazo maior nas hipóteses que a lei ou norma regulatória assim estabelecer ou para preservação de direitos. Por fim, a empresa alerta que caso o titular solicite a exclusão de seus dados, pode ocorrer que estes precisem ser mantidos por período superior ao pedido de exclusão, nos termos do artigo 16 da Lei Geral de Proteção de Dados Pessoais, para (i) cumprimento de obrigação legal ou regulatória, (ii) estudo por órgão de pesquisa, e (iii) transferência a terceiro (respeitados os requisitos de tratamento de dados dispostos na mesma Lei). Somente findos o prazo de manutenção e a necessidade legal, os Dados Pessoais serão excluídos com uso de métodos de

	descarte seguro, ou utilizados de forma anonimizada para fins estatísticos.

Diante do exposto, observou-se que a Política de Privacidade da ViaQuatro foi disponibilizada em local de destaque em seu site, facilitando seu acesso pelo usuário do serviço.

A ViaQuatro esclarece que atua como controladora dos dados pessoais do usuário, destacando que, por exercer este papel, possui algumas responsabilidades, tais como: (i) registrar as atividades de tratamento; (ii) adotar medidas de segurança técnicas e administrativas; (iii) garantir a segurança da informação; (iv) atender aos direitos dos titulares; (v) cooperar com a Autoridade Nacional de Proteção de Dados; e (vi) garantir o atendimento aos princípios e bases legais da LGPD.

Os direitos do titular de dados, tópico essencial em uma política de privacidade, também foram informados de forma clara e adequada, atendendo às diretrizes da LGPD.

A Política esclarece que eventuais controvérsias que envolvam o documento deverão ser resolvidas no foro da Comarca de São Paulo.

Um ponto relevante na Política analisada é que, logo no início, ela traz um aviso para que os menores de 16 anos não se registrem na plataforma e que caso tenham entre 16 e 18 anos, deverão ser assistidos pelos pais ou representantes legais.

Outro item importante é que a empresa disponibiliza um e-mail indicando quem é o Encarregado que facilitará a comunicação com o titular em caso de dúvidas com relação às disposições contidas na Política de Privacidade e de Tratamento de Dados.

Seria interessante a empresa ter incluído um endereço para eventuais envios de correspondências pelo titular, e um telefone para contato, ampliando as formas pelas quais o titular poderá exercer seus direitos. Além disso, faltou incluir o horário disponível para o atendimento.

Por fim, ela também traz um glossário contendo algumas definições e descrições para colaborar na compreensão da Política. Observamos que a presença deste glossário é muito importante para a leitura do documento, pois explica termos técnicos e legais referidos no texto, que poderiam ser desconhecidos pelo usuário. A linguagem utilizada foi bastante compreensível e se baseou em definições da própria lei.

A partir das análises realizadas é possível concluir que a Política de Privacidade analisada se mostra bastante preocupada em se adequar às diretrizes e comandos da Lei Geral

de Proteção de Dados Pessoais, buscando apontar de forma clara tudo aquilo que envolve o tratamento de dados pela plataforma.

A empresa esclareceu, logo no início do documento, quais dados são tratados por ela. Porém, como vimos na pergunta de número 1, ela nada menciona sobre a existência de tratamento de dados pessoais sensíveis, os quais, como vimos no estudo de caso analisado nos tópicos anteriores, são também tratados pela empresa.

Isto posto, era fundamental que a ViaQuatro expusesse de forma clara que realiza referido tratamento, pontuando, especificamente, as situações nas quais este tratamento ocorre, como, no exemplo estudado, a coleta de dado pessoal biométrico (imagem) pelo reconhecimento facial de seus usuários do metrô.

Na situação do metrô, inclusive, houve tratamento de dados pessoais sensíveis de crianças e de adolescentes. Assim, era imprescindível que a ViaQuatro trouxesse em sua Política de Privacidade um tópico em destaque sobre esta coleta de dados de crianças e de adolescentes, sobretudo por conta da vulnerabilidade desses sujeitos, para que os usuários tivessem conhecimento e pudessem manifestar seu consentimento.

Ademais, nesta situação, cabe à ViaQuatro se comprometer a realizar o máximo de esforço para proteger tais dados, indicando as medidas escolhidas para tanto.

Outrossim, nota-se um grande equívoco no material que é a ausência de menção expressa à base legal utilizada para o tratamento de dados pessoais pela empresa em outras situações além do cumprimento das obrigações legais e regulatórias, já que, como visto nesta pesquisa, esse tratamento de dados também existe. Somente com a referência à base legal é que seria possível constatar se o tratamento de dados realizado é ou não permitido pela lei. Em síntese, cabia à ViaQuatro informar ao titular a previsão legal (uma ou mais bases legais) de todos os tratamentos que está efetuando.

Outro ponto que, infelizmente, deixa a desejar maior aprofundamento no documento é quando a Política menciona, apenas de forma superficial, a possibilidade de coleta de dados para a realização de propagandas. Consta ainda que, nestes casos, os dados serão compartilhados de forma anonimizada.

No caso, a finalidade foi apresentada de forma genérica, sem esclarecer ao titular quais propagandas poderiam ser realizadas. Isto posto, questiona-se: (1) a propaganda está relacionada ao serviço ofertado?; (2) existe a possibilidade de o titular não concordar com o uso de seus dados para esta finalidade?; (3) existe alguma forma de controle sobre quem são esses terceiros que poderão receber os dados coletados?; (4) quais dos dados coletados serão

direcionados para este fim?. A resposta a referidos questionamentos é essencial para que o titular possa ter seu direito à privacidade e à proteção de dados devidamente protegidos.

Além disso, analisando o documento disponibilizado pela empresa, verifica-se que faltou esclarecer o procedimento de descarte e de exclusão dos dados pessoais, requisito fundamental para que o titular possa exercer um controle efetivo sobre seus dados.

Por fim, embora conste a data de atualização da Política de Privacidade, a empresa não se preocupou em mostrar o número de sua versão. Isso é importante para que, havendo pedido do usuário para exercer algum de seus direitos em relação a seus dados, ele saiba exatamente qual versão da Política regia determinada operação de tratamento.

CONCLUSÃO

Com esta pesquisa, pudemos observar de forma profunda o quanto as novas tecnologias de informação e de comunicação alteraram nossa sociedade e a maneira pela qual esta se desenvolve nos aspectos econômicos e sociais. Vimos que, hoje, a informação, compreendida como um consolidado de dados pessoais, é a principal fonte de poder e de controle.

Neste sentido, pudemos perceber que as tecnologias alteraram o próprio funcionamento do mercado e da prospecção de clientes, trazendo novos caminhos de se abordar o usuário/consumidor. Um destes caminhos foi justamente o uso de dados pessoais.

Nesta pesquisa, foi possível verificar a utilização de dados pessoais como fonte de propagandas publicitárias, as quais passaram a ser produzidas de forma cada vez mais direcionada e específica ao interesse daquele que irá adquirir determinado serviço ou produto.

Ademais, constatou-se que, muitas vezes, a coleta desses dados é feita de maneira singela, sendo que o titular sequer tem conhecimento de que ela está sendo realizada.

Todo este contexto refletiu no Direito, que precisou buscar novas respostas para as demandas atuais da população, a fim de regular o tratamento de dados pessoais e de proteger de forma ampla o indivíduo, não mais com base exclusivamente em seu direito à privacidade.

Isto porque, embora, por um lado, a era dos dados e das tecnologias digitais tenha contribuído para facilitar o acesso e a troca de informações em uma intensidade e uma velocidade antes inimagináveis; por outro lado, possibilitou que o titular sofresse violações cada vez mais íntimas, em seu aspecto mais particular, que é sua personalidade.

Vimos que os dados são representações do indivíduo, revelando suas características, seus interesses e emoções, motivo pelo qual merecem especial atenção e proteção.

Importante registrar que a coleta e a utilização de dados pessoais, por si só, não é um problema e jamais deve ser visto como algo negativo. Pelo contrário, o tratamento de dados facilita a realização de inúmeras atividades cotidianas, bem como inova as estratégias de mercado, e traz impactos positivos em diversas outras áreas.

Do mesmo modo, em relação às tecnologias que se valem de dados pessoais biométricos, tais como, aquelas de reconhecimento facial, é evidente que adentram um espaço ainda mais sensível e único do titular. Em razão disso, os cuidados com sua manipulação deverão ser ainda maiores.

O que se deve ter em consideração, em qualquer atividade de tratamento de dados pessoais realizada, é que esta deverá ser acompanhada por instrumentos que possam garantir parâmetros mínimos de proteção à pessoa humana e a seus direitos fundamentais.

Neste sentido, com essa pesquisa, percebemos que é fundamental que o Direito estruture mecanismos jurídicos para proteger o titular dos dados de eventuais violações e, ainda, garantir que o titular tenha um efetivo controle sobre a circulação e sobre o tratamento de suas informações, sem que isso inviabilize os avanços tecnológicos.

Frente a esta problemática, a Lei Geral de Proteção de Dados Pessoais, no ordenamento jurídico brasileiro, atua como principal referência na busca pela tutela efetiva dos dados pessoais, ao estruturar parâmetros legais mínimos para a regulação de atividades que tratam dados, bem como ao propor a proteção dos direitos fundamentais dos titulares, como o direito à autodeterminação, à privacidade e à própria proteção de dados.

A referida Lei trouxe uma série de transformações significativas na maneira pela qual os dados pessoais são tratados no nosso país.

Uma das consequências da LGPD foi justamente a obrigação de os agentes de tratamento (controlador e operador) passarem a esclarecer e expor ao titular tudo aquilo que envolve o tratamento de seus dados, desde a finalidade da coleta, o fundamento utilizado para tanto (base legal), as formas de armazenamento, períodos de retenção, entre outros, respeitando, ainda, todos os princípios definidos em lei.

Hoje, uma das soluções trazidas pela própria Lei Geral de Proteção de Dados Pessoais para mitigar as questões envolvendo coleta de dados biométricos, como imagens de vídeo, é a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais, medida esta, inclusive, já é aplicada nos países da União Europeia.

Neste Relatório, é possível descrever todos os processos que envolvem o tratamento de dados, as finalidades buscadas, a base legal que o justifica, e, de forma paralela, trazer mecanismos para prevenir os riscos e gerir os danos que esse tratamento poderá gerar aos direitos dos titulares de dados. Tal prática indica a boa-fé do agente de tratamento.

Uma das formas de se adequar à Lei Geral de Proteção de Dados Pessoais analisada nesta pesquisa, foi justamente a adequação das Políticas de Privacidade, instrumento essencial para fornecer informação clara e objetiva ao titular.

Desde antes de a LGPD entrar em vigor, quando a mesma ainda era um projeto em discussão, os tribunais brasileiros têm sido acionados para interpretar e, principalmente, se

posicionar a respeito das possíveis violações ao direito à privacidade e à proteção de dados pessoais.

O caso da linha amarela do metrô de São Paulo, administrado pela empresa Via Quatro, utilizado aqui como estudo de caso, foi um deles, já que foi interposto antes da LGPD entrar em vigor e foi diretamente influenciado pelos avanços da lei, da doutrina e dos pesquisadores.

Este caso também se destaca pelo imenso número de usuários envolvidos e que tiveram seus dados pessoais coletados de maneira indevida, o que levou a uma grande discussão midiática.

Além disso, este caso foi uma das primeiras situações em que foram judicializadas questões referentes à temática da proteção de dados pessoais, a fim de buscar respostas do Poder Judiciário sobre quais as consequências geradas aos agentes de tratamento quando estes incorrem em violações ao direito à proteção de dados pessoais. Aliás, foi o primeiro caso envolvendo especificamente o reconhecimento facial de usuários em transportes públicos.

Certamente, a decisão final proferida neste caso – que, recorde-se, ainda não tramitou pelo Superior Tribunal de Justiça ou pelo Supremo Tribunal Federal – estabelecerá um precedente para o ordenamento jurídico brasileiro e atuará como paradigma orientador de outros conflitos que envolvam a matéria.

Do que se observou até o presente momento, evidente que existe uma preocupação do Poder Judiciário em ampliar a proteção concedida aos titulares do direito à proteção de dados pessoais, a fim de garantir o desenvolvimento de sua personalidade de forma livre e, principalmente, estando consciente a respeito de eventuais interferências em sua esfera individual.

Por outro lado, pudemos perceber que existe uma cobrança cada vez maior por parte do Poder Judiciário para que haja uma adequação dos agentes de tratamento às diretrizes da lei. Ou seja, cabe aos controladores e aos operadores das operações envolvendo dados pessoais adotarem medidas técnicas, administrativas e de segurança, voltadas a proteger os dados do titular.

Outra medida de suma importância é a implementação de políticas de privacidade, as quais têm o intuito de esclarecer ao usuário, titular dos dados pessoais, todas as operações que envolvem o tratamento de seus dados, assim como todos os cuidados que são adotados pelo agente de tratamento. A disponibilização das políticas de privacidade também proporciona maior confiança ao titular, que percebe que aquele sujeito para o qual está fornecendo seus dados, está preocupado em atender à LGPD.

Além disso, com este estudo de caso, foi possível perceber que, ainda que seja em local público, a coleta de dados pessoais jamais deve ser realizada sem conhecimento dos titulares e, principalmente, sem uma base legal que a justifique.

Especificamente em relação aos dados pessoais discutidos nesta pesquisa, quais sejam, os dados pessoais biométricos, a LGPD traz algumas hipóteses de tratamento destes que poderiam ser aplicadas no caso (consentimento do titular; segurança do titular; realização de estudos por órgão de pesquisa), a depender das circunstâncias nas quais o tratamento foi realizado.

A situação torna-se ainda mais problemática quando nos deparamos com o tratamento de dados pessoais para fins exclusivamente comerciais, como ocorreu pela Via Quatro, tendo em vista que referida finalidade não está compreendida nos objetivos de uma concessionária de serviço público. Ali, cabia à Via Quatro apenas e tão somente definir as condições referentes ao transporte de passageiros, e não trazer propagandas publicitárias, totalmente manipuladas por algoritmos.

Frente a uma violação como esta, é direito do titular exigir que a coleta de seus dados cesse e, ainda, que as informações sejam eliminadas.

Isto posto, o estudo de caso aqui realizado reforçou que, nos dias atuais, já existe uma orientação jurisprudencial no sentido de que, constatada a violação ao direito à proteção de dados pessoais, deve ocorrer a responsabilização dos agentes de tratamento, tanto voltada para a reparação dos danos materiais e morais causados ao titular, quanto para a prevenção de futuras violações – acessos não autorizados, perdas, alterações indevidas, entre inúmeros outros tratamentos inadequados ou ilícitos.

Importante, por fim, pontuar que durante a realização dessa pesquisa, percebeu-se uma atuação cada vez mais ativa por parte da Autoridade Nacional de Proteção de Dados, seja por meio da instauração de processos de fiscalização em face de agentes que estariam violando disposições da LGPD, seja, até mesmo, pela primeira ocorrência de imposição de sanção.

A esse respeito, o próprio Poder Judiciário tem reforçado e reconhecido a competência da autoridade para aplicar as sanções previstas na LGPD, enquanto ao judiciário caberia, prioritariamente, o arbitramento de indenizações nos casos de violações. Assim, sua atuação seria paralela e complementar.

Conclui-se que a LGPD, juntamente com o Poder Judiciário e a ANPD, atuam como elementos extremamente importantes na proteção do titular, e sua atuação cada vez mais ativa

tem contribuído significativamente para ampliar o conhecimento acerca do direito à proteção de dados e, sobretudo, a incentivar a sua aplicação nas relações entre diferentes sujeitos.

REFERÊNCIAS

ABADE, André da Silva; ALVES, Josilene Dália. Política de privacidade e dados pessoais: a caracterização da consciência de uso e o valor da informação armazenados na nuvem. **Revista Facisa on-line**. Barra do Garças – MT, vol.6, n.1, p. 123- 144, jan.- jul. 2017.

ALEXY, Robert. **Teoria dos Direitos fundamentais.** Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ALEXY, Robert; RAZ, Joséph et BULYGIN, Eugenio. **Uma discussão sobre teoria do Direito**. São Paulo: Marcial Pons, 2013.

AMARAL, Fernando. **Introdução a ciência de dados: mineração de dados e Big Data.** Rio de Janeiro: Alta Books, 2016.

ANPD. Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado.v. 2. 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 14 ago. 2022.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**. Curitiba, vol. 4, n. 3, p. 167-200, set./dez. 2017.

BAEZ, Narciso Leandro Xavier Baez; LIMA, Germano Alves. Os limites da autonomia privada em face da perspectiva civil-constitucional. **Direitos Fundamentais & Justiça**. Belo Horizonte, ano 10, n. 34, p. 115-131, jan./jun. 2016. p. 03.

BARROSO, Luís Roberto Barroso; BARCELLOS, Ana Paula. O começo da história. a nova interpretação constitucional e o papel dos princípios no direito brasileiro. *In* **Revista Direito Administrativo**. Rio de Janeiro, 232: 141-176. Abr./ jun. 2003. p.23/24

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. *In* **Cadernos Jurídicos.** v. 1. n. 53. São Paulo: Escola Paulista da Magistratura. Jan-mar 2020

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**- A Função e os Limites do Consentimento. 3.ed. Rio de Janeiro: Grupo GEN, 2021.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade.** 8. ed., rev., aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015.

BLUM, Renato Opice; SCHUCH, Samara. Compartilhamento e comercialização de dados pessoais em ambiente online. *In* BERGAMINI, Adolpho *et al*. (coord.). **Contraponto jurídico: posicionamentos divergentes sobre grandes temas do Direito.** São Paulo: Revista dos Tribunais, 2018. p. 451-466. Localização: SEN, MJU, STF, TJDFT, TST

BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. *In* **Seqüência** (Florianópolis), n. 68, p. 109-127, jun. 2014.

BRASIL. Câmara dos Deputados. Projeto de Lei PL 3514/2015.Altera a Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), para aperfeiçoar as disposições gerais do Capítulo I do Título I e dispor sobre o comércio eletrônico, e o art. 9º do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro), para aperfeiçoar a disciplina dos contratos internacionais comerciais e de consumo e dispor sobre as obrigações extracontratuais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2052488. Acesso em: 19 nov. 2022.

BRASIL. **Código Civil: Lei n. 10.406, de 10 de janeiro de 2002.** 4. ed. Barueri: Manole, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 14 jul. 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 07 jul. 2022.

BRASIL. Emenda Constitucional nº15. **Diário Oficial da União**. Brasília, DF, ano 2022, n. 30, 11 fev. 2022. Seção I, p.2.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 jul. 2022.

BRASIL. Lei 13.853, de 8 de julho de 2019**.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 25 jul. 2022.

BRASIL. Medida Provisória nº 1.124, de 13 de junho de 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Mpv/mpv1124.htm#:~:text=MEDIDA%20PROVIS%C3%93RIA%20N%C2%BA%201.124%2C%20DE%2013%20DE%20JUNHO%20DE%202022&text=Altera%20a%20Lei%20n%C2%BA%2013.709,e%20transforma%20cargos%20em%20comiss%C3%A3o. Acesso em: 07 jul. 2022.

BRASIL. Supremo Tribunal Federal. **ADI 6387.** Rel. Min. Rosa Weber, Decisão Monocrática, j. 24.04.2020, DJe 28.04.2020. p. 12.

CAMARA, Maria Amália Oliveira de Arruda; RODRIGUES, Walter de Macedo. A gestão de dados pessoais por grandes empresas: considerações geopolíticas e jurídicas**.** *In* **Cadernos Adenauer**- Proteção de dados pessoais: privacidade versus avanço tecnológico. n. 3. Rio de Janeiro: Fundação Konrad Adenauer, out. 2019.

CANARIS, Claus-Wilhelm**. Direitos fundamentais e direito privado**. Trad. Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra: Almedina, 2003, p. 10

CLARKE, Roger. Human identification in information Systems: Management challenges and public policy issues. **Information Technology & People**, v. 7, n. 4, p. 6-37, 1994, p.4. Disponível em: https://openresearch-repository.anu.edu.au/bitstream/1885/46248/27/03Paper02.pdf . Acesso em 29 jan. 2023.

COLOMBO, Cristiano; GOULART, Guilherme Damasio. Ética algorítmica e proteção de dados pessoais sensíveis: classificação de dados de geolocalização em aplicativos de combate à pandemia e hipóteses de tratamento. *In* BARBOSA, Mafalda Miranda; NETTO, Felipe Braga [*et al*]. (Coord.). **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa.** Indaiatuba: Foco, 2021, p. 271-287.

COUNCIL OF EUROPE. **Guidelines on Facial Recognition** CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CONVENTION 108. 2021. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 29 jan. 2023

DONEDA, Danilo. A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados. *In:* BIONI, Bruno [*et al*]. (org.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021. p. 459-469.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**. Joaçaba. v. 12. n. 2. jul/ dez. 2011, p. 91-108.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados.** 2. ed. São Paulo: Thomson Reuters Brasil, 2020

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. *In* BIONI, Bruno [*et al*]. (org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 03-20.

DONEDA, Danilo; MONTEIRO, Marília Aguiar. **Proteção de dados pessoais enquanto direito fundamental e o direito fundamental à saúde –privacidade e e-Health**. *In* Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. (Temas em saúde coletiva, 18). Org. Tânia Margarete Mezzomo Keinert [*et al*]. São Paulo: Instituto de Saúde, 2015.

EUROPEAN DATA PROTECTION BOARD; EUROPEAN DATA PROTECTION SUPERVISOR. **EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Councillaying down harmonised rules on artificial intelligence (Artificial Intelligence Act).** v. 1. 18 jun. 2021. Disponível em: https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf . Acesso em: 25 mai. 2022

EUROPEAN DATA PROTECTION BOARD. **Guidelines 3/2019 on processing of personal data through video devices**. v. 2. 29 jan. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf . Acesso em: 25 mai. 2022

EUROPEAN PARLIAMENTARY RESEARCH SERVICE. **Regulating facial recognition in the EU**. set. 2021. Disponível em: https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf. Acesso em: 16 nov. 2022

FEFERBAUM, Marina; QUEIROZ, Rafael Mafei Rabelo. **Metodologia da pesquisa em direito: técnicas e abordagens para elaboração de monografias, dissertações e teses.** 2. ed. São Paulo: Saraiva, 2019.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

GRUPO DE TRABALHO DE PROTECÇÃO DE DADOS DO ARTIGO 29.º. Parecer 4/2007 sobre o conceito de dados pessoais. 20 de junho de 2007. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pt.pdf . Acesso em: 19 nov. 2022.

KAFKE, Guilherme Forma *et al*. **Direitos Humanos digitais: termos de uso e políticas de privacidade**. Apostila do curso “Termos de Uso e Políticas de Privacidade" ministrado na Fundação Getúlio Vargas. 2020. Online

KLEE Antonia Espíndola Longoni; PEREIRA NETO, Alexandre Nogueira Pereira. **A** Lei Geral de Proteção de Dados (LGPD): uma visão panorâmica. *In* **Cadernos Adenauer-** Proteção de dados pessoais: privacidade versus avanço tecnológico. n. 3. Rio de Janeiro: Fundação Konrad Adenauer, out. 2019.

LEONEL, Maria Eduarda. **Marketing jurídico digital: a evolução da publicidade do advogado e suas ferramentas**. Trabalho de Conclusão de Curso apresentado à Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, como pré-requisito para a obtenção do Título de Bacharel em Direito. Franca, 2022.

LIMA, Carolina Silva; SOUSA, Luana Pereira. A constitucionalização do direito civil como garantia de eficácia dos direitos fundamentais nas relações privadas. **Instituto Brasiliense de Direito Público** – IDP. p.17

LIMA, Cíntia Rosa Pereira de. A**utoridade Nacional de Proteção de Dados Pessoais e a Efetividade da Lei Geral de Proteção de Dados de acordo com a Lei Geral de Proteção de Dados (Lei n. 13/709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei n. 12.965/2014) e as sugestões de alteração do CDC (PL.3.514/2015).** 1. ed. São Paulo: Almedina, 2020.

LOPES, Fernanda Dutra Vieira. Processos Preliminares do Artigo 6º da LGPD: As novas perspectivas sobre proteção de dados entre o que se quer, o que de fato se precisa e como adequar os dados adquiridos com as permissões pessoais e as permissões legais. *In* PURKIT, Paulo (org.). **Comentários à Lei Geral de Proteção de Dados.** Comissão de Direito Digital, Tecnologia e Inteligência Artificial. OAB-SP 116ª Subseção Jabaquara - Saúde. Jan. 2020. Online.

MALGIERI, Gianclaudio; COMANDÉ, Giovanni. **Why a right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation**. International Data Privacy Law, vol. 7, Issue 4, November 2017. p. 258-259.

MARCONI, Marina de Andrade; LAKATOS Eva Maria. **Fundamentos de metodologia científica.** 5. ed.São Paulo: Atlas 2003.

MARTINS, Guilherme Magalhães; BASAN, Arthur Pinheiro. O Marketing algorítmico e o direito de sossego na internet: perspectivas para o aprimoramento da regulação publicitária. *In* BARBOSA, Mafalda Miranda; NETTO, Felipe Braga [*et al*]. (Coord.). **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa.** Indaiatuba: Foco, 2021, p. 339-362.

MARTINS, Leonardo. **Introdução à jurisprudência do Tribunal Constitucional Federal Alemão. Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Hennig *et al*. Montevidéu: Fundação Konrad Adenauer, 2005, p. 237.

MARTINS, Luciana Mabília. **O direito civil à privacidade e à intimidade.** *In:* MARTINS-COSTA, Judith (Org.) A reconstrução do Direito Privado. São Paulo, Revista dos Tribunais, 2002. p. 344.

MAYER-SCHONBERGER, Viktor; KENNETH, Cukier**. Big Data:** a revolution that will transform how we live, work and think. Nova Iorque: HMH, 2013. E-book.

MENDES, Laura Schertel. **A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis.** *In* SOUZA, Carlos Affonso [*et al*]. (org.) Lei Geral de Proteção de Dados - caderno especial. São Paulo: Revista dos Tribunais. nov. 2019

MENDES, Laura Schertel; DONEDA, Danilo. **Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da proteção de dados no Brasil**. Revista de Direito do Consumidor, São Paulo, v. 120, p. 555-570, 2018.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. **Proteção de dados para além do consentimento: tendências de materialização.** *In* Bioni, Bruno *Et Al* (coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN; 2020.

MENDES, Laura Schertel; JÚNIOR, Otavio Luiz Rodrigues; FONSECA, Gabriel Campos Soares da. **O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais: rumo a um direito fundamental autônomo.** *In*: BIONI, Bruno [*et al*]. (org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 61-71

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. STF reconhece direito fundamental à proteção de dados. Comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393. **Revista de Direito do Consumidor**. v. 130/2020. Jul.-Ago. 2020. p. 471 – 478.

MEZZAROBA, Orides; MONTEIRO, Cláudia Servilha. **Manual de metodologia da pesquisa no direito**. 7. ed. São Paulo: SaraivaJur, 2019

MORAES, Maria Celina Bodin; QUEIROZ, João Quinelato. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *In* **Cadernos Adenauer**- Proteção de dados pessoais: privacidade versus avanço tecnológico. n. 3. Rio de Janeiro: Fundação Konrad Adenauer, out. 2019.

MOURA, Marcel Brasil de Souza. **As Disposições Preliminares da LGPD.** In PURKIT, Paulo (org.). Comentários à Lei Geral de Proteção de Dados. Comissão de Direito Digital,

Tecnologia e Inteligência Artificial. OAB-SP 116ª Subseção Jabaquara - Saúde. Jan. 2020. Online

NUNES, Luis Antônio Rizzato. **Curso de direito do consumidor.** 5. ed. São Paulo: Editora Saraiva, 2010.

PAESANI, Liliana Minardi. **Direito e Internet : liberdade de informação, privacidade e responsabilidade civil**. 6. ed. São Paulo: Atlas. 2013.

PATZ, Stefani Reimann. O **uso de tecnologias de perfilamento no controle migratório: um estudo sobre o tratamento dos dados pessoais dos migrantes na sociedade da informação e da vigilância.** Dissertação de Mestrado em Direito apresentada à Universidade Regional Integrada do Alto Uruguai e das Missões (URI), Campus Santo Ângelo/RS, Departamento de Ciências Sociais Aplicadas, Programa de Pós-Graduação em Direito Stricto Sensu, Mestrado e Doutorado em Direito, para obtenção do título de Mestra em Direito. Santo Ângelo/RS, 2022.

PATZ, Stefani Reimann; PIAIA, Thami Covatti. **Os dados na sociedade contemporânea: histórico e aspectos fundamentais da Lei Geral de Proteção de Dados** (LGPD). *In* Inteligência artificial, proteção de dados e cidadania. v.2. organizadores: Eduardo Tomasevicius Filho, Stéfani Reimann Patz, Thami Covati Piaia. Cruz Alta: Ilustração, 2020.

PINHEIRO, Patrícia Peck. **Direito Digital.** 5. ed. rev. atual. e ampl. de acordo com as Leis n. 12.735 e 12.737 de 2012. São Paulo: Saraiva, 2013.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais.** 2. ed. São Paulo: Saraiva, 2020.

PINHEIRO, Patrícia Peck. **Segurança Digital - Proteção de Dados nas Empresas**. São Paulo: Atlas, 2021.

RAMOS, André de Carvalho. **Curso de direitos humanos**. São Paulo: Saraiva, 2014.

REIS, Abel. **Como as tecnologias digitais afetam quem somos e como vivemos**. Porto Alegre: Arquipélago Editorial, 2018.

RODOTA, Stefano. **A vida na sociedade da vigilância: a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada.** Belo Horizonte: Del Rey, 1998. p. 268.

SANTOS, Mariana Vieira; RAMOS, Taciana Cecília. **A criação da ANPD (Agência Nacional de Proteção de Dados) em um contexto de hiper presidencialismo no Brasil: uma ameaça à democracia?** *In* Inteligência artificial, proteção de dados e cidadania. org. FILHO, Eduardo Tomasevicius; PATZ, Stéfani Reimann Patz; PIAIA, Thami Covati. Cruz Alta: Ilustração, 2020.

SARLET, Gabrielle Bezerra Sales. **Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro**. *In*

LIMA, Cíntia Rosa Pereira de. Comentários à Lei Geral de Proteção de Dados- Lei n. 13.709/2018, com alteração da lei n. 13.853/2019. São Paulo: Grupo Almedina, 2020.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**- Uma teoria Geral dos Direitos Fundamentais na perspectiva constitucional. 11.ed. rev. Atual. Porto Alegre: Livraria do Advogado Editora, 2012. p.19.

SARLET, Ingo Wolfgang**. Direitos fundamentais e direito privado: Algumas considerações sobre a vinculação dos particulares aos direitos fundamentais.** *In* A Constituição concretizada: construindo pontes com o público e o privado. Porto Alegre: Livraria do Advogado, 2000.

SARLET, Ingo Wolfgang. **Fundamentos constitucionais: o direito fundamental à proteção de dados.** *In* Bioni, Bruno Et Al (coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN; 2020.

SARLET, Ingo Wolfgang; KEINERT, Tania Margarete Mezzomo. **O direito fundamental à privacidade e as informações em saúde: alguns desafios.** *In* Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. (Temas em saúde coletiva, 18). Org. Tânia Margarete Mezzomo Keinert [et al]. São Paulo: Instituto de Saúde, 2015.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. 2.ed. Rio de Janeiro: Lumen Juris, 2010.

SECRETARIA DE GOVERNO DIGITAL. **Guia de Elaboração do Termo de Uso e Política de Privacidade para serviços públicos.** v. 1.3. 2022. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_tupp.pdf. Acesso em 15 ago. 2022

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

SCHWABE, Jürgen. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal alemão.** Organização e introdução Leonardo Martins. Tradução de Beatriz Hennig *et al.* Montevidéu: Fundación Konrad Adenauer, 2005.

SILVA, José Afonso da. **Direito constitucional positivo**. 10. ed. São Paulo: Malheiros, 1994. p. 204.

SILVA, Vergilio Ricardo Britto; LUCIANA, Edimara Mezzomo; WIEDENHOFT, Guilherme. **Privacidade na internet: o que está por trás das Políticas de Privacidade.** *In* Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. (Temas em saúde coletiva, 18). Org. Tânia Margarete Mezzomo Keinert *[et al]*. São Paulo: Instituto de Saúde, 2015.

STEINMETZ, Wilson. **A vinculação dos particulares aos direitos fundamentais.** São Paulo: Malheiros Editores, 2004. p. 202

TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. *In* **CADERNOS JURÍDICOS**. v. 1. n. 53. São Paulo: Escola Paulista da Magistratura. Jan-mar, 2020.

TEPEDINO, Gustavo. **Do sujeito de direito à pessoa humana.** Editorial da Revista Trimestral de Direito Civil, n. 2, 2000, p. 06

TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odélio; VIEIRA, Victor Barbieri Rodrigues. **Parecer do IRIS na Ação civil Pública IDEC vs. ViaQuatro.** Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro). Setembro de 2019. Belo Horizonte: IRIS, 2019. Disponível em: https://irisbh.com.br/wp-content/uploads/2019/09/Acao-Civil-Publica-IDEC-vs.-ViaQuatro-Parecer-do-IRIS-1.pdf. Acesso em 18 mar. 2022

TOMASEVICIUS FILHO, Eduardo. **A Lei Geral de Proteção de Dados Brasileira**. São Paulo: Grupo Almedina, 2021.

TOMASEVICIUS FILHO, Eduardo. Reconhecimento facial e lesões aos direitos da personalidade. *In* BARBOSA, Mafalda Miranda; NETTO, Felipe Braga [*et al*]. (Coord.). **Direito Digital e Inteligência Artificial: diálogos entre Brasil e Europa.** Indaiatuba: Foco, 2021, p. 129-142.

TOMASEVICIUS FILHO, Eduardo; PATZ, Stéfani Reimann; PIAIA, Thami Covati. **Inteligência artificial, proteção de dados e cidadania**. v.2. Cruz Alta: Ilustração, 2020.

UNIÃO EUROPEIA. Carta dos Direitos Fundamentais da União Europeia. In: Jornal Oficial das Comunidades Europeias. 18 de dezembro de 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 18 set. 2022.

UNIÃO EUROPEIA. Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046. Acesso em: 18 set. 2022.

UNIÃO EUROPEIA. General Data Protection Regulation - GDPR- Regulation (EU) 2016/679. Disponível em: https://gdpr-info.eu/art-1-gdpr/>. Acesso em: 16 mar. 2022

UNITED KINGDOM. Information Commissioner's Office. **Guidance on video surveillance.** Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/video-surveillance/. Acesso em 31 jul. 2022.

UNITED KINGDOM. Information Commissioner's Office. **The use of live facial recognition technology in public places**. v.1. 18 jun. 2021. Disponível em: https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf. Acesso em 31 jul. 2022.

UNITED KINGDOM. Information Commissioner's Office. **What is special category data?**· Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/. Acesso em 31 jul. 2022.

VIOLA, Mario; TEFFE, Chiara Spadaccini. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11.** *In* Bioni, Bruno *Et Al* (coords.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Grupo GEN; 2020.

WIMMER, Miriam. **O regime jurídico do tratamento de dados pelo Poder Público.** *In:* BIONI, Bruno [*et al*]. (org.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 271- 288.