UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE NACIONAL DE DIREITO

A APLICAÇÃO DA TUTELA DA PROTEÇÃO DE DADOS PESSOAIS NO CASO DAS PORTAS INTERATIVAS DIGITAIS DO METRÔ DE SÃO PAULO

JÚLIA TUPYNAMBÁ DUARTE

Rio de Janeiro

2019/1

JÚLIA TUPYNAMBÁ DUARTE

A APLICAÇÃO DA TUTELA DA PROTEÇÃO DE DADOS PESSOAIS NO CASO DAS PORTAS INTERATIVAS DIGITAIS DO METRÔ DE SÃO PAULO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Flávio Alves Martins.**

Rio de Janeiro

2019/1

CIP - Catalogação na Publicação

D812a

Duarte, Júlia Tupynambá
A aplicação da tutela da proteção de dados pessoais no caso das Portas Interativas Digitais do metrô de São Paulo / Júlia Tupynambá Duarte. -- Rio de Janeiro, 2019.
66 f.

Orientador: Flávio Alves Martins.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2019.

1. Privacidade. 2. Dados pessoais. 3. Reconhecimento facial. 4. Legislação. I. Martins, Flávio Alves, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

JÚLIA TUPYNAMBÁ DUARTE

A APLICAÇÃO DA TUTELA DA PROTEÇÃO DE DADOS PESSOAIS NO CASO DAS PORTAS INTERATIVAS DIGITAIS DO METRÔ DE SÃO PAULO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Flávio Alves Martins.**

Data da Aprovação: __/__/____.

Banca Examinadora:

_____

Orientador

_____

Membro da Banca

_____

Membro da Banca

Rio de Janeiro

2019/1

RESUMO

O direito à privacidade e o direito à proteção de dados pessoais vêm cada vez mais sendo impactados pela crescente utilização de reconhecimento facial. Com efeito, a disponibilidade de dispositivos conectados, sensores e recursos de informática cria oportunidades para produzir, captar e processar uma enorme variedade de bancos de dados. Dentre essas tecnologias, destaca-se o uso do reconhecimento facial por utilizar dados biométricos, permitir identificar o indivíduo, além de rastrear sua localização, tudo isso de modo imperceptível pelo titular de dados. Nessa linha, chama a atenção o caso das Portas Interativas Digitais instaladas na linha amarela do metrô de São Paulo em 2018, sistema que realizava o reconhecimento facial dos usuários do transporte sem qualquer aviso prévio e sem o consentimento deles enquanto veiculava anúncios publicitários com a finalidade de captar a reação das pessoas aos estímulos que lhe eram exibidos. Assim, o presente trabalho, baseando-se no estudo de caso das Portas Interativas, busca compreender as necessidades que a proteção de dados possui hoje e verificar a efetividade da proteção conferida pelo ordenamento jurídico brasileiro aos titulares de dados em casos como esse.

Palavras-chaves: Privacidade. Dados pessoais. Reconhecimento facial. Legislação.

ABSTRACT

The right to privacy and the right to personal data protection are increasingly being impacted by the increasing use of facial recognition. Indeed, the availability of connected devices, sensors, and computing resources creates opportunities to produce, capture, and process a wide variety of databases. Among these technologies, it is important to note the use of facial recognition for using biometric data, allowing the identification of the individual, and tracking their location, all imperceptibly by the data subject. In this way, it highlights the case of the Digital Interactive Doors installed in the yellow line of the subway of São Paulo in 2018 the system that realized the facial recognition of the users of the transport without any previous notice and without their consent while it published announcements for the purpose to capture the reaction of the people to the stimuli that were shown to them. Thus, the present work, based on the case study of the Interactive Doors, seeks to understand the needs that data protection has today and to verify the effectiveness of the protection conferred by the brazilian legal order to data holders in cases such as this.

Keywords: Privacy. Personal data. Facial recognition. Legislation

SUMÁRIO

INTRODUÇÃO

A tecnologia é algo que acompanha a própria história da humanidade e impulsiona alterações no modo que a sociedade tem de se relacionar. A transição do século XX para o século XXI é marcada pela acentuação dessa presença, em especial das tecnologias de informação. Principalmente após o avanço das redes sociais, as pessoas passaram a compartilhar verdadeira biografia digital de suas vidas. Posteriormente, a Internet espraiou-se para os sensores, aparelhos, eletrodomésticos entre outros objetos com a chamada Internet das Coisas. Com efeito, a inovação tecnológica possibilitou não só o acesso a uma enorme quantidade e diversidade de informação, como também seu compartilhamento de maneira instantânea, revolucionando a forma de organizá-la e de comunicá-la.

A ascensão da informação ao papel protagonista do atual modelo econômico, marcou a formação da denominada Sociedade de Informação, onde os dados são o novo petróleo. Com todo esse arsenal de dados que gerados, por meio de algoritmos e do cruzamento de dados, é possível identificar pessoas e traçar perfis pessoais, o que é altamente interessante para que governos possam estruturar políticas públicas e que empresas possam canalizar suas publicidades para eventuais consumidores de maneira mais eficaz. Não obstante, diferente do petróleo, os dados pessoais não são um recurso natural aguardando para ser descoberto, mas são o registro da personalidade do indivíduo e expressão da sua dignidade humana. Nesse sentido, entre as diversas ponderações sobre os riscos associados ao uso da informação, a garantia da privacidade merece destaque.

A famosa série Black Mirror já há algum tempo convida o público a refletir sobre os contornos que a tecnologia assume na vida das pessoas, sobretudo quanto às interferências na privacidade. Em “*Shut up and dance*”, há o acionamento remoto das câmeras de computadores pessoais, objetivando o acesso a informações comprometedoras para serem usadas como chantagem. Já nos episódios “*Nosedive*” e “*Hated in the nation*”, as redes sociais permitem que usuários avaliem uns aos outros, de modo que essa avaliação determina o preço de aluguéis residenciais, o acesso a serviços de transporte, e até a condenação à

morte. Apesar da série se passar no futuro, as narrativas expostas não se distanciam muito do que a sociedade já vive hoje.

Nesse sentido, frisa-se a crescente utilização de reconhecimento facial para a coleta de dados praticada por governos e empresas. Apesar de sua potencial utilidade como instrumento de segurança pública, sua utilização em larga escala pode ser altamente danosa à privacidade do indivíduo, haja vista que o reconhecimento facial permite identificar individualmente determinada pessoa, além de rastrear sua localização. Com efeito, George Orwell, em sua obra “1984”, já prenunciava a vigilância que hoje a tecnologia permite com o tratamento de dados. Nessa linha, exemplo dos contornos que o reconhecimento facial pode assumir verifica-se na China, onde câmeras são usadas para monitorar atos e movimentações de cidadãos com o intuito de avaliar cada pessoa por notas, que podem ser usadas para finalidades diversas, como, por exemplo, diferenciar acesso a serviços ou, até mesmo, gerar sanções.

No Brasil, caso emblemático dessa nova realidade exemplifica-se com a instalação de painéis nas portas do metrô na cidade de São Paulo, que realizavam o reconhecimento facial dos usuários do transporte sem o conhecimento desses enquanto veiculava anúncios publicitários com a finalidade de captar a reação das pessoas aos estímulos que lhe eram exibidos. Esse caso revela, ainda, especial gravidade, uma vez que os cidadãos sequer precisavam acessar a rede para terem seus dados coletados, pelo contrário, o tiveram enquanto se locomoviam pela cidade.

Assim, tendo em vista que a captação de dados biométricos por câmeras pode ocorrer de modo imperceptível àquele que tem a imagem captada, e permite sua identificação de maneira específica, necessário repensar a tutela da privacidade à luz das demandas do meio digital, em especial, das tecnologias que realizam leitura facial. Além disso, verifica-se a necessidade de controlar o tratamento desses dados, para garantir a privacidade dos indivíduos.

Na verdade, desde que o ex-agente da Agência Nacional de Segurança dos Estados Unidos, Edward Sonowden, revelou informações a respeito do esquema de espionagem que o governo norte-americano empreendia sobre governos do mundo todo, inclusive brasileiro, a necessidade da regulação do tratamento de dados pessoais ganhou destaque. Com efeito, hoje, o Brasil possui uma lei específica sobre o tema, a Lei n° 13.709/2018. Além disso, o ordenamento jurídico nacional conta com um compilado de leis que tutelam a proteção de dados, formado pelo Código de Defesa do Consumidor, o Marco Civil da Internet, a Lei de Acesso à Informação e a Lei do Cadastro Positivo. Ainda, a privacidade é direito fundamental consagrado pela Constituição da República e direito da personalidade garantido pelo Código Civil.

Tendo isso em vista, o presente trabalho realiza o estudo do caso das Portas Interativas do metrô de São Paulo, de modo a evidenciar a importância que a proteção de dados pessoais ocupa na sociedade hoje e averiguar de que modo o direito protege o titular de dados pessoais, sobretudo em casos como o em foco, em que há desafios contundentes à proteção de dados, como a utilização de sensores automatizados, dispositivos de captura de imagem camuflados e coleta de dados sensíveis, levando em consideração, ainda, a enorme quantidade e variedade de bancos de dados existentes hoje e a possibilidade de cruzamento de informações entre eles. Com isso, espera-se que a presente pesquisa possa evidenciar possíveis lacunas ou insuficiências presentes na legislação aplicável, para contribuir no debate acerca de uma construção efetiva da proteção de dados pessoais.

Para isso, optou-se por dividir o presente estudo em três etapas: em um primeiro momento se construirá o raciocínio necessário para compreender a lógica por trás da proteção de dados pessoais, discorrendo sobre a evolução da concepção de direito à privacidade até a formulação do direito à proteção de dados. Depois, através de uma análise dogmática, se averiguará como o direito brasileiro tutela a proteção de dados pessoais, levantando-se as principais normas das legislações citadas anteriormente. Finalmente, após esclarecer os aspectos necessários para se compreender as peculiaridades a respeito da prática de

reconhecimento facial, se examinará o caso das Portas Interativas Digitais, considerando, especialmente a possibilidade de a tecnologia empreendia identificar os passageiros e os aspectos que caracterizam a ilegalidade do tratamento de dados pessoais.

1 A TUTELA DA PRIVACIDADE

1.1 Da origem à Sociedade de Informação

A origem da proteção da privacidade remonta ao "*right to be alone*"[1] formulado por Cooley em 1888, cuja essência encerrava-se na busca pela tranquilidade. Com efeito, um direito de ser deixado só representava uma espécie de imunidade do indivíduo perante terceiros, isto é, uma garantia de ausência de comunicação com os outros. Desse modo, tal concepção de privacidade estava fadada a um individualismo exacerbado, reflexo de um cenário no qual a vida em sociedade era representada por um forte isolamento entre os sujeitos.

Já em seu artigo "*The right to privacy*"[2], Warren e Brandeis apresentam a proteção da privacidade desvinculada do direito de propriedade. Embora a *privacy* inove ao arraigar na personalidade seu fundamento, não há ruptura definitiva com a definição egoística do *right to be alone*, ao contrário, a doutrina majoritária entende que teriam o fortalecido ainda mais[3]. Tampouco, há a definição de um conceito do que seria efetivamente o direito à privacidade. Feitas as ressalvas necessárias, fato é que o destaque dado ao tema por Warren e Brandeis serviu para impulsionar e

---

1 O right to be let alone foi mencionado pelo magistrado Thomas McIntyre Cooley em 1888 no seu Treatise of the law of torts. v. 4, capítulo 3.2.

2 WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, Cambridge, 15 dez. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 20 maio 2019.

3 "De modo emblemático, o artigo intitulado The Right to Privacy, de autoria de Warren e Brandeis, na Harvard Law Review, no ano de 1890, representou um marco para o debate jurídico sobre o tema da privacidade. No texto, os autores analisam o contexto das invenções recentes da época e os novos métodos de negócio para chamar a atenção, surgindo a necessidade de instrumentos jurídicos de proteção da pessoa, de modo a assegurar o que Cooley denominou, anos antes, 'o direito de ser deixado em paz', ou originalmente "the right to be let alone" (WARREN; BRANDEIS, 1890, p. 1-10). [...] O direito à privacidade, contudo, garante a proteção aos âmbitos mais imateriais, aos interesses espirituais da pessoa, configurando-se como um direito autônomo que adquire substantividade própria. Por essa razão, Warren e Brandeis fundamentaram diretamente o denominado right to privacy no direito de desfrutar a vida, rechaçando expressamente qualquer conexão ou associação com os direitos de liberdade ou propriedade. Eles situaram o direito à privacidade em uma categoria geral do direito individual de ser deixado em paz ou de, simplesmente, não ser incomodado – right to be let alone (SALDAÑA, 2012, p. 195-240)". Cf. FORTES, Vinícius Borges. Os direitos de privacidade na internet e a proteção de dados pessoais: uma compreensão conceitual para os direitos fundamentais. In Reia, Jhessica et al. (Org.). **Horizonte presente**: tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito; FGV – Fundação Getúlio Vargas, 2019.

valorizar a concepção de um direito à privacidade de forma autônoma e positivada, o que seria primordial para seu posterior desenvolvimento como direito fundamental.

Desde então, a definição do direito à privacidade vem sendo discutida com mais afinco, já lhe tendo sido atribuído desde o sentido de um resguardo contra interferências alheias até de um direito ao sigilo. No entanto, somente a partir da década de 1950, que a privacidade passa a ser associada também a proteção de dados. De fato, a insurgência do modelo do Welfare State assinalou substancial diferença na relação entre cidadão e Estado, ao mesmo tempo, o desenvolvimento tecnológico, impulsionou o crescimento do fluxo informacional. Com a possibilidade de obtenção das informações pessoais, o Estado viu uma grande oportunidade em se apropriar desses dados. DONEDA (2006)[4] sugere dois fatores para justificar este marco – o controle e a eficiência:

> "Os motivos são razoavelmente implícitos: basta verificar que um pressuposto para uma administração pública eficiente é o conhecimento tão acurado quanto possível da população, do que decorre, por exemplo, a realização de censos e pesquisas e o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais à administração pública, visando maior eficiência. Em relação ao controle, basta acenar às várias formas de controle social que podem ser desempenhadas pelo Estado e que seriam potencializadas com a maior disponibilidade de informações sobre os cidadãos, aumentando seu poder de controle sobre os indivíduos".

A princípio, só o Estado utilizava essas informações, pois era o único que tinha condições para arcar com o alto custo que a prática requeria. Contudo com o desenvolvimento da tecnologia de informação, a utilização de dados passou a ser menos onerosa, o que atraiu a iniciativa privada. Desse modo, a importância dos dados na sociedade acentuava-se progressivamente.

Isso posto, à medida que as tecnologias que viabilizam o tratamento de dados se desenvolvem, suas características estampam-se no complexo sócio-político-econômico, "de modo a penetrarem nas instâncias da vida cotidiana, moldando-a em uma lógica que preza por aquilo que seria justamente as suas vantagens - eficiência, rapidez ou infalibilidade" (DONEDA, 2006). Forma-se, portanto, a

---

[4] DONEDA, Danilo. **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Saraiva, 2006.

chamada Sociedade de Informação, na qual a principal moeda são os dados pessoais, isto é, onde a informação tem natureza de bem econômico e consiste em elemento estruturante das relações sociais (BIONI, 2014)[5].

Não obstante, se por um lado as inovações tecnológicas representavam avanços no desenvolvimento político-econômico e inclusive em aspectos da vida em sociedade, representados pela praticidade, aproximação de pessoas e rompimento das distâncias físicas, em contrapartida nem sempre estariam associadas ao bem-estar social. Por conseguinte, o desenvolvimento da privacidade como um direito fundamental levou a necessidade de funcionalizá-la. Assim, era necessário o desdobramento da tutela geral da privacidade em direitos específicos voltados a tutelar as situações cotidianas. Nesse sentido, DONEDA (2006) esclarece:

> "A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Neste papel, a vemos como pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos."

Desse modo, o desenvolvimento tecnológico evidenciou a limitação que um conceito de privacidade encarnado na concepção de uma liberdade negativa tinha para lidar com o surgimento de novas situações, como a necessidade de proteção de dados pessoais. Nesse sentido, a privacidade exige, nas palavras de RODOTÁ (2008)[6], "um tipo de proteção dinâmica, que segue o dado em todos os seus movimentos", como resultado

> "de um longo processo evolutivo experimentado pelo conceito de privacidade - de uma definição original como o direito de ser deixado em paz, até o direito de controle sobre as informações de cada um e de determinar como a esfera privada deve ser construída".

---

[5] BIONI, Bruno. A produção normativa no cenário transfronteiriço. In: CONPENDI/UFSC (org.). **Direito e novas tecnologias**: XXIII Encontro Nacional do CONPEDI. Florianópolis: CONPENDI, 2014. Disponível em: http://www.publicadireito.com.br/artigos/?cod=575dc1140c7f1254. Acesso em: 17 ago 2018.

[6] RODOTÁ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Organização, seleção e apresentação de: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro, RJ: Editora Renovar, 2008.

Tal necessidade é constatada ao se analisar a evolução que a proteção da privacidade teve no direito internacional. Nesse sentido, em 1948, a Declaração Americana dos Direitos do Homem, no artigo V, estabeleceu que, “toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar”. Ainda no mesmo ano, a Declaração Universal dos Direitos Humanos acrescenta a proteção contra ataques e interferências nas correspondências de cada pessoa[7]. Finalmente, a Carta de Direitos Fundamentais da União Europeia de 1950, reconhece a complexidade dos interesses relacionados à privacidade, ao positivar, ao mesmo tempo, o direito ao respeito pela vida privada e familiar[8], e a proteção dos dados pessoais[9], sem fracionar sua fundamentação, que é a dignidade do ser humano.

Com isso, a privacidade transcende a esfera doméstica para alcançar qualquer ambiente onde circulem dados pessoais do seu titular, como suas características físicas, seu código genético, seu estado de saúde, sua crença religiosa e qualquer outra informação pertinente à pessoa. Com efeito, a necessidade de funcionalização da proteção da privacidade fez com que dela defluísse uma disciplina de proteção de dados pessoais que, embora compreenda a privacidade como seu núcleo, assume feições próprias inerentes a suas peculiaridades. Conforme anuncia DONEDA (2006):

> “Nesta mudança, a proteção da privacidade identifica-se e acompanha a consolidação da própria teoria dos direitos da personalidade e, com seus mais recentes desenvolvimentos, contribui para afastar a leitura segundo a qual sua utilização em nome de um individualismo exacerbado alimentou o medo de que eles se tornassem o "direito dos egoísmos privados". Algo paradoxalmente, a proteção da privacidade na sociedade da informação , tomada na sua forma de proteção de dados pessoais, avança sobre terrenos outrora impropo níveis e nos induz a pensá-la como um elemento que, antes de garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e

---

7 Artigo 12 do Código Civil (Lei n° 10.406/2002): “Ninguém será sujeito a interferência na sua vida, privada, na sua família, no seu lar, ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências e ataques”.

8 Artigo 7º da Carta de Direitos Fundamentais da União Europeia: “Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.”

9 Artigo 8° da Carta de Direitos Fundamentais da União Europeia: “1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, 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 respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”

> consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade.”

Desse modo, chegou-se ao ponto em que hoje se encontra o direito contemporâneo, isto é, do reconhecimento da necessidade de um espaço de coexistência das novas tecnologias com os vários interesses e o respeito aos direitos fundamentais. E dentre todas as tentativas de construí-lo, as mais interessantes não são propriamente "revolucionárias", mas as que privilegiam uma abordagem mais pragmática. Assim, importante assimilar que não houve efetiva ruptura com a privacidade de outras épocas, mas sim um reposicionamento de seu centro de gravidade em função da multiplicidade de interesses envolvidos e da sua importância na tutela da pessoa humana.

1.2 O desenvolvimento do direito à proteção de dados pessoais

Como visto, a proteção da privacidade em concreto depende de uma valoração complexa na qual sejam sopesadas situações concretas de sua aplicabilidade, o que dificulta a sua conceituação e sua estruturação como direito subjetivo (DONEDA, 2006). Isso porque a demanda por uma proteção de dados exige necessariamente que o titular tenha direito ao controle sobre suas informações, isto é, de determinar como, quando, aonde e a quem seus dados podem ser comunicados. De acordo com RODOTÁ (2008, p. 36), o cidadão não pode ser visto como simples fornecedor de dados, ele tem que ter poder de controle sobre esses dados, para se estabelecer o equilíbrio na concentração de poder. Na verdade,

> “[...] A obrigação de fornecer dados não pode ser simplesmente considerada como contrapartida dos benefícios sociais que, direta ou indiretamente, o cidadão pode chegar a aproveitar. As informações coletadas não somente tornam as organizações públicas e privadas capazes de planejar e executar os seus programas, mas permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes: consequentemente, os cidadãos têm o direito de pretender exercer um controle direto sobre aqueles sujeitos aos quais as informações fornecidas atribuirão um crescente plus-poder.” (RODOTÁ, 2008, p. 36-37)

Em outras palavras, os efeitos produzidos pela garantia à privacidade ultrapassam a imposição de um dever geral de abstenção, pois necessitam de obrigações de caráter positivo, como o dever de solicitar autorização para a inclusão do nome de certa pessoa em um cadastro de dados ou o dever de possibilitar a correção de dados do mesmo cadastro pelo seu titular a qualquer tempo.

Diante da positivação do direito de proteção de dados a partir da década de 1960, MAYER-SCHÖNBERGER (1997)[10] divide as legislações sobre a temática em quatro gerações. Como visto, primeiramente, a utilização de dados pessoais foi prática originada pelo Estado. Assim, a principal preocupação das primeiras leis era evitar o uso indiscriminado dessas informações pelo Poder Público, para tanto, a saída encontrada foi a submissão do tratamento de dados à prévia autorização do titular e a princípios gerais e abstratos[11]. Contudo, com o início da utilização de dados pelos entes privados e a consequente multiplicação dos centros de processamento de dados, o acompanhamento do regime de autorizações tornou-se insustentável.

Por conseguinte, no final da década de 1970, a proteção de dados na segunda geração de leis é representada por intermédio de instrumentos que permitiam que o próprio cidadão pudesse acompanhar o tratamento de seus dados, e caso verificado o uso indevido, poderia então requerer sua tutela[12]. Assim, a responsabilidade pela proteção de dados passava a recair sobre os titulares.

Não obstante, tal abordagem ignorava que o exercício dessa liberdade não tinha aplicabilidade diante dos moldes sociais. Com efeito, conforme atenta

---

[10] MAYER-SCHÖNBERGER, Viktor. General devepoment of data protection in Europe. In: **Technology and privacy: the new landscape**. AGRE, Philip; ROTENBERG, Marc (org.). Cambridge: MIT Press, 1997, p. 219-242.

[11] Dentre as legislações inseridas no contexto da primeira geração da proteção de dados pessoais estão: o norte-americano Fair Credit Reporting Act de 1970; a lei do Land alemão de Hessen de 1970; o Estatuto para banco de dados da Suécia de 1973; e o norte-americano Privacy Act 1974.

[12] Representam a segunda geração de diplomas sobre proteção de dados a Datenschutzgesetz (Lei n° 565/1978 da Áustria), a Constituição de Portugal e a Constituição da Espanha, promulgadas em 1976 e 1978, respectivamente.

DONEDA (2019)[13], o fornecimento de dados pessoais pelos cidadãos tinha se tornado requisito indispensável para a sua efetiva participação na vida social, sendo assim a interrupção ou o simples questionamento do fluxo de informações pelo cidadão já implicava sua exclusão em algum aspecto da vida social. Em síntese, o titular de dados possuía um direito de grande importância, mas com um ônus que o tornava muito improvável de ser exercido.

Tendo isso em vista, as leis da década de 1980 consagraram a terceira geração de diplomas a respeito da proteção de dados ao estipularem meios capazes de tornar efetiva a autodeterminação informativa. Para isso estabeleciam recursos para as ocasiões em que a liberdade do titular em decidir livremente acerca da autorização para o tratamento de dados lhe era tolhida por eventuais condicionantes, bem como o dever de informação dos operadores dedados (DONEDA, 2019). Apesar do grande avanço que representaram as leis da terceira geração por permitirem um controle sobre todas as etapas do tratamento de dados e não apenas no momento da autorização como nas primeiras leis, elas estavam marcadas por um caráter eminentemente exclusivista. Isso porque a demanda pela proteção dos dados pessoais não é sentida de forma uniforme pela população, pois varia conforme o padrão médio de consumo, educação e a acesso à tecnologia no cotidiano. Assim, nem todos teriam condições de arcar com os custos econômico e pessoais que requeria a autodeterminação informativa assim entendida.

Na verdade, com o avanço da tecnologia aliado ao aumento da velocidade das redes e à melhoria dos mecanismos de busca, tornou-se possível não apenas a formação de diversos tipos de grandes bancos de dados, como também o cruzamento de informações entre eles, possibilitando que a informação tornasse-se tão organizada a ponto de permitir a criação de perfis sobre cada indivíduo e, em última análise, a sua identificação. Tais “perfis” guiam decisões, ações e estratégias de entidades privadas e públicas.

---

[13] DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In MARTINS, Guilherme Magalhães (coord.); LONGHI, João Victor Rozatti (coord.). **Direito digital:** direito privado e internet. 2 ed. Indaiatuba, SP: Editora Foco, 2019.

De acordo com RODOTÁ (2008), esses obstáculos refletiam a necessidade de que o controle sobre os dados pessoais assegurasse ao cidadão não apenas a exatidão e o uso correto das informações a ele relacionadas (caráter individual), mas, sobretudo, um instrumento para estabelecer o equilíbrio na nova distribuição do poder (caráter coletivo). Nesse sentido, o autor observa uma tendência à identificação de sujeitos coletivos, minorias (ou mesmo maiorias) de diversas ordens, como entes prejudicados pela violação da privacidade, chegando mesmo a afirmar uma tendência à mudança dos sujeitos que demandam pela privacidade, com uma predominância da coletividade. Nesses termos,

> "É evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em "controle". Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejoso de esquivar-se de novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo do qual somente poderá sair sem perdedor.
>
> A atenção, consequentemente, deve deslocar-se dos meios de reação individual para instrumentos de controle social: e poderá ocorrer que, seguindo esse caminho, alguns meios que estavam tradicionalmente à disposição do indivíduo venham a ser perdidos; perda, no entanto, que pode ser compensada pela criação, em nível coletivo, de um aparato de controle globalmente mais incisivo e vigilante do que o atual." (RODOTÁ, 2008)

Dessa dimensão coletiva surge, enfim, a conotação contemporânea da proteção da privacidade, representada pela quarta geração de leis, as quais reconhecem o desequilíbrio que marcam as relações entre titular e operador de dados. Sendo assim, elas deixam de dar vazão somente a um imperativo de ordem individualista, e passam a ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana. Nesse sentido, as leis atuais reservam algumas matérias ao mais alto grau de proteção, como é o caso do tratamento dos dados sensíveis que será analisado mais a frente, além de preverem a atuação de autoridades independentes para fiscalizarem sua correta aplicação.

Por todo o exposto, conforme se pode observar, por trás da proteção de dados pessoais está presente a concepção de autodeterminação informativa. Ocorre que, em um primeiro momento, ela ainda não se fazia notar de forma

efetiva, proporcionando quase nenhum poder ao cidadão diretamente. Sem embargo, ao decorrer da história da tutela das informações pessoais, mais precisamente, com a terceira geração de leis, a autodeterminação se concretiza através de instrumentos a permitirem o efetivo controle das informações pelos seus titulares. Até que se chega ao direito contemporâneo, quando então se percebe que a verdadeira efetividade da autodeterminação informativa só poderia se dar com uma tutela coletiva da proteção de dados. Como sintetiza DONEDA (2006):

> “A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva para a tutela da pessoa quanto a sua adequação às novas tecnologias de informação. Não basta pensar na privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma "predileção" individual, associada basicamente ao conforto e comodidade. A própria visão da privacidade como algo de que um cidadão respeitável poderia tranquilamente abrir mão (ou que ao menos se esperasse isto de um cidadão honesto e de bons costumes), a presumida "transparência de quem não tem nada a temer", deixa de fazer sentido dada a crescente complexidade da matéria . Uma esfera privada, na qual a pessoa tenha condições de desenvolvimento da própria personalidade, livre de ingerências externas, ganha hoje ainda mais em importância; passa a ser pressuposto para que não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada (para tocar em um conceito caro ao direito privado) e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade.”

Desse modo, o desenvolvimento jurídico da privacidade levou-a um lugar de destaque dentro da proteção da dignidade humana. Para tanto, foi necessário que, em paralelo ao direito autônomo da privacidade, existissem diversos outros direitos para lidar com os problemas que surgiam na sociedade, dentre eles a proteção de dados. Posteriormente, a própria proteção de dados precisou trilhar caminho semelhante até se perceber que ela não poderia limitar-se a mero princípio geral ou direito individual. Ademais, importante destacar que, embora se observe essa diversificação normativa, todos os direitos criados a partir da privacidade encontram nela seu fundamento, o que a faz ser compreendida hoje como um direito “guarda-chuva” que protege esses outros direitos. Assim, o caminho percorrido pela privacidade até aqui, fez com que sua disciplina passasse a definir todo um estatuto que perpassa as relações da própria personalidade com o mundo exterior, para garantir o pleno exercício da cidadania e democratização das tecnologias de informação.

2 A PROTEÇÃO DE DADOS PESSOAIS NO ORDENAMENTO JURÍDICO BRASILEIRO

2.1 Interpretação sistemática

A proteção de dados pessoais configura-se a partir da interpretação conjunta da Constituição Federal, do Código Civil, do Código de Defesa do Consumidor (Lei nº 8.078/1990), da Lei de Acesso à Informação (Lei nº 12.527/2011), do Marco Civil da Internet (Lei nº 12.965/2014) e da Lei do Cadastro Positivo (Lei nº 12.414/2011). Nesse sentido, a proteção de dados é respaldada por uma sistematização jurídica baseada nos direitos básicos de transparência, na proteção das pessoas naturais e na evolução da ideia de autodeterminação informativa, ante a previsão de mecanismos de controle do indivíduo sobre os seus dados pelo ordenamento.

Como visto no capítulo anterior, a tutela da proteção de dados pessoais é uma das manifestações do amplo espectro de direitos decorrentes do direito fundamental à privacidade, que é expressão da proteção da dignidade a da pessoa humana, fundamento da República Federativa do Brasil, conforme o inciso III do artigo 1º da Carta Política brasileira. Assim sendo, a privacidade tem sua inviolabilidade resguardada no art. 5º, X da Constituição e ainda recebe tutela constitucional específica, ao se resguardar a interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), bem como com a possibilidade da ação de habeas data (art. 5º, LXXII), que teve seus contornos definidos na Lei n° 9.507/97.

O *habeas data* é uma ação constitucional por meio da qual o cidadão pode acessar e retificar seus dados pessoais em bancos de dados de entidades governamentais ou de caráter público, aqui também compreendidos os bancos de dados referentes a consumidores, mesmo que administrados por entes privados. Apesar disso, algumas de suas limitações fazem com que sua aplicação seja escassa e pouco abrangente, não somente pelo fato de que os bancos de dados privados e de uso interno estarem exclusos do seu âmbito de aplicação, como também em virtude de seu perfil estar demasiadamente associado à proteção de

liberdades negativas, como a necessidade de sua interposição através de advogado, além da necessidade da prova da recusa da administração pública em fornecer a informação, e da ausência da possibilidade expressa de que informações indevidamente coletadas ou armazenadas sejam eliminadas do banco de dados. Nesse sentido, BARROSO (1998, p. 212) afirma se tratar de "um remédio de valia, no fundo, essencialmente simbólica"[14].

Replicando limitadamente o espírito constitucional, o Código Civil1516 estabelece a vida privada da pessoa natural como um direito da personalidade humana, considerada, por conseguinte, intransmissível e irrenunciável. Além disso, segundo o enunciado do art. 21, "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". Contudo, como já analisado no capítulo anterior, de acordo com as lições de RODOTÁ (2008), a proteção de dados pessoais não pode ser pensada nos parâmetros clássicos do direito à privacidade enquanto pessoa-informação-sigilo, mas sim no quadrinômio pessoa-informação-circulação-controle.

Considerando o tratamento dispensando pelo Código Civil de 2002 à privacidade, Anderson Schereiber[17] adverte:

> "A verdade é que o Código Civil brasileiro deu à privacidade um tratamento inadequado. Em primeiro lugar, dedicou um único artigo à matéria, cuja importância se renova a cada dia na sociedade contemporânea. Nesse dispositivo solitário, o legislador limitou-se, como se verá mais adiante, a um enunciado genérico, que não acrescenta rigorosamente nada ao que já se encontrava previsto na Constituição. Perdeu, assim, a oportunidade de oferecer parâmetros para a solução de diversos conflitos concretos ligados à tutela da privacidade.
>
> Não bastasse isso, empregou a expressão vida privada, revelando certa indiferença à recente evolução do conceito de privacidade, que abandonou uma concepção mais restrita, limitada ao círculo da intimidade da pessoa

---

[14] BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: Wambier (coord.). **Habeas data**. São Paulo: Revista dos tribunais, 1998, p. 212

[15] Art. 11 do Código Civil de 2002: Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

[16] Art. 20 do Código Civil de 2002: Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

[17] SCHEREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

> humana, para abarcar a proteção aos dados e informações pessoais. Sobre esse último aspecto, a codificação não trouxe uma palavra sequer. Não é exagero dizer que o Código Civil ignorou a vasta amplitude do tema, cuja compreensão é essencial para perceber o importante papel reservado à tutela da privacidade no século XXI.” (SCHEREIBER, 2014, p. 134)

Na omissão do Código Civil, o Código de Defesa do Consumidor, visando proteger o consumidor da utilização abusiva de seus dados, marcou importante modernização do ordenamento civil brasileiro, suprindo muitas das lacunas deixadas pela ausência de um marco normativo específico sobre dados pessoais. Desse modo, a doutrina entende pela extensão da aplicação do art. 43 do CDC a outros setores da vida em sociedade, já que a proteção à privacidade transcende as relações consumeristas, como se verifica a seguir:

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

Com isso, o ordenamento brasileiro passa a prever um direito do titular de dados de tomar conhecimento de quando alguém estoca informações a seu respeito sem sua provocação ou aprovação. Trata-se de verdadeiro dever de comunicação, o qual é corolário do direito à retificação disposto no art. 43, §3º, CDC, que abre ao consumidor a possibilidade de retificar ou ratificar o registro de

seus dados a qualquer momento. Ainda trouxe o CDC a previsão de alguns deveres para os gestores de bancos de dados, dentre eles o estabelecimento de prazo para manutenção dos dados em arquivo, determinando a exclusão de informações relativas a débitos prescritos dos registros.

A Lei de Acesso à Informação (Lei nº 12.527/2011), que regulamenta o direito constitucional de acesso às informações públicas[18], também trouxe importantes avanços no que tange à proteção de dados. Para além das questões pontuadas, o art. 4º, IV da LAI define como informação pessoal "aquela relacionada à pessoa natural identificada ou identificável". Já o art. 31 dispõe que o tratamento de informações pessoais deve ser feito de forma transparente, e qualquer transferência a terceiros apenas pode ser realizada caso estipulada por previsão legal ou com consentimento expresso do titular dos dados.

Outrossim, a Lei nº 12.965/2014, conhecida como Marco Civil da Internet, ao disciplinar o uso da internet no Brasil adota a proteção da privacidade e dos dados pessoais como princípios (art. 3º, II e III), bem como prevê a nulidade das cláusulas contratuais que os ofenderem ou violarem as comunicações privadas pela internet (parágrafo único do art. 3º). Além disso, o art. 7º garante importantes direitos aos usuários da Internet no que toca à proteção de dados pessoais, como os constantes nos incisos VII a X:

> VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

[18] Art. 5º, XXXIII da Constituição da República Federativa do Brasil de 1988: todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta lei;

Verifica-se, portanto, a imposição de um dever de transparência por parte dos operadores de dados, sobretudo, quanto a delimitação da finalidade específica do tratamento. Além disso, o princípio do consentimento, enquanto elemento basilar da proteção de dados pessoais, também está consagrado no MCI, o qual, nos termos do art. 7º, VII e IX, deve ser livre, informado, expresso e constar em cláusula destacada das demais do contrato. Quanto a este princípio, MENDES (2016, p. 5)[19] desenvolve importantes considerações:

> "A autorização pelo consumidor, como regra geral, é um pressuposto essencial para o tratamento de dados pessoais nas relações de consumo, inclusive aquelas desenvolvidas no ambiente virtual. Afinal, se os dados pessoais referem-se ao seu titular e o representam, afetando a sua personalidade, somente ele pode decidir a respeito do fluxo desses dados, salvo em casos excepcionais ou expressa previsão legal. Tal conceito, que já podia ser extraído do Código de Defesa do Consumidor, tornou-se requisito expresso a partir da promulgação do Marco Civil. Trata-se da concretização do princípio da liberdade de escolha do consumidor (art. 6º, II, CDC). A regra do consentimento está prevista no art. 7º, VII e IX, do Marco Civil da Internet. Enquanto o inc. VII condiciona o fornecimento a terceiros dos dados pessoais ao consentimento livre, expresso e informado do usuário, salvo em caso de previsão legal, o inc. IX estabelece norma geral acerca do consentimento em caso de coleta, uso, armazenamento e tratamento de dados pessoais, prevendo ainda que o consentimento deve constar de cláusula destacada. Essa regra básica para a legitimidade do tratamento de dados pessoais também está presente na Lei federal de proteção de dados alemã, que determina que a coleta, o processamento e a utilização de dados pessoais somente são permitidos se autorizados por lei ou consentidos pelo titular (§1º, 1, BDSG). Para que o tratamento constitua a real manifestação de vontade do consumidor de submeter os seus dados pessoais a tratamento, ele tem que atender a determinados requisitos. Assim, entende-se que o consentimento somente é válido se for expresso, livre, específico e informado. (...) Além do consentimento ou outro fundamento legítimo para o tratamento de dados, a análise da legitimidade do tratamento de dados deve levar em conta a boa-fé objetiva, as expectativas legítimas do consumidor, bem como os impactos e os riscos de tratamento de dados pessoais para o consumidor".

[19] MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, n. 106, julho/agosto, 2016.

Ainda sobre a questão do consentimento, a Lei do Cadastro Positivo (Lei nº 14.414/2011) originalmente trazia a previsão da liberdade de escolha do titular de dados, condicionando a abertura de cadastro à autorização prévia do potencial cadastrado mediante consentimento expresso e informado[20]. Contudo a Lei Complementar nº 166/2019, afastou o modelo *opt-in*[21] e instituiu o modelo *opt-out*,[22] por meio do qual, a abertura de cadastro se dará automaticamente pelo gestor, a menos que o consumidor exerça o seu direito de oposição, fazendo cessar o compartilhamento de seus dados[23].

Com as alterações introduzidas pela LC 166/19, os consumidores devem ser informados da abertura de cadastros em seu nome no prazo de até trinta dias, bem como têm direito de receber informações claras e objetivas sobre os canais disponíveis para cancelamento de seu cadastro. Além disso, o art. 5º garante algumas prerrogativas ao consumidor como o acesso gratuito às informações sobre

---

[20] Art. 4º da Lei n° 14.414/2011 com a redação dada pela LC166/2019: A abertura de cadastro requer autorização prévia do potencial cadastrado mediante consentimento informado por meio de assinatura em instrumento específico ou em cláusula apartada. § 1º Após a abertura do cadastro, a anotação de informação em banco de dados independe de autorização e de comunicação ao cadastrado. § 2º Atendido o disposto no caput, as fontes ficam autorizadas, nas condições estabelecidas nesta Lei, a fornecer aos bancos de dados as informações necessárias à formação do histórico das pessoas cadastradas.

[21] O *opt-in* consiste em manifestação ativa do titular de dados consentido com a criação do banco de dados, afastando-se a presunção de aceite pelo silêncio.

[22] O *opt-out* configura-se na possibilidade que o titular tem de requerer a retirada de suas informações do banco de dados. Nesse sentido, o *opt-out* rem aplicabilidade nas hipóteses em que o *opt-in* é dispensado, isto é, o cadastro de dados que é criado independente de seu aceite. Assim, ao tomar ciência da existência do cadastro e não querendo que a prática seja continuada pode, então, exercer o *opt-out*.

[23] Art. 4 da Lei nº 14.414/2011 com a redação dada pela LC166/2019: O gestor está autorizado, nas condições estabelecidas nesta Lei, a: I - abrir cadastro em banco de dados com informações de adimplemento de pessoas naturais e jurídicas; II - fazer anotações no cadastro de que trata o inciso I do caput deste artigo; III - compartilhar as informações cadastrais e de adimplemento armazenadas com outros bancos de dados; e IV - disponibilizar a consulentes: a) a nota ou pontuação de crédito elaborada com base nas informações de adimplemento armazenadas; e b) o histórico de crédito, mediante prévia autorização específica do cadastrado. (...) § 4º A comunicação ao cadastrado deve: I - ocorrer em até 30 (trinta) dias após a abertura do cadastro no banco de dados, sem custo para o cadastrado; II - ser realizada pelo gestor, diretamente ou por intermédio de fontes; e III - informar de maneira clara e objetiva os canais disponíveis para o cancelamento do cadastro no banco de dados. § 5º Fica dispensada a comunicação de que trata o § 4º deste artigo caso o cadastrado já tenha cadastro aberto em outro banco de dados. § 6º Para o envio da comunicação de que trata o § 4º deste artigo, devem ser utilizados os dados pessoais, como endereço residencial, comercial, eletrônico, fornecidos pelo cadastrado à fonte. § 7º As informações do cadastrado somente poderão ser disponibilizadas a consulentes 60 (sessenta) dias após a abertura do cadastro, observado o disposto no § 8º deste artigo e no art. 15 desta Lei. § 8º É obrigação do gestor manter procedimentos adequados para comprovar a autenticidade e a validade da autorização de que trata a alínea b do inciso IV do caput deste artigo.

ele existentes; impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados, e sua respectiva correção ou cancelamento em até dez dias; conhecimento dos principais elementos e critérios considerados para a análise de risco; ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; e a revisão de decisões automatizadas. Outro ponto importante instituído pela lei é a vedação de anotações no cadastro de informações não vinculadas à análise de risco de crédito ao consumidor, e dados sensíveis, isto é, pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas (art. 3°).

Não obstante todo o arcabouço legal observado até então, o avanço social-tecnológico exige um tratamento mais complexo sobre o tema. O cenário vem se transformando cada vez mais rapidamente, provocando profundas mudanças nas relações sociais. Nesse sentido, o Direito corre atrás do fato social, tentando respaldar os acontecimentos com as regulamentações do plano normativo, contudo é evidente o descompasso nessa jornada.

Da análise do instrumental disponível para possibilitar a concreta atuação de tais direitos, sucede uma proteção que, embora devesse corresponder a uma proteção integrada e dirigida pela tábua axiológica constitucional, atua de forma fracionada, em focos de atuação determinados que tendem a orientar-se mais pela lógica de seus específicos campos do que por uma estratégia baseada na tutela integral da personalidade através da proteção dos dados pessoais.

Por mais que o Marco Civil tenha representado um importante avanço rumo a proteção de dados pessoais, ele ainda é insuficiente, pois seu âmbito de regulação limita-se a ambientes online, enquanto grande parte dos abusos que ocorrem com a utilização de dados pessoais estão presentes no ambiente *off-line*. Além disso, o MCI não traz definições importantes, como de dado pessoal e de tratamento de dados, por exemplo. Tendo isso em vista, há situações específicas que demandam previsão direta e assertiva por parte da lei, como a proteção específica de dados sensíveis, deveres de segurança digital, uma autoridade independente que garanta

efetividade aos deveres e garantias, entre outros. Por essa razão surgem as novas legislações sobre proteção de dados pessoais como uma tentativa de sanar essa carência de sincronismo ao lidar com a temática da privacidade na era digital.

Ainda, soma-se, a esse panorama, a entrada em vigor do Regulamento Geral de Proteção de Dados Europeu (*General Data Protection Regulation* - GDPR)[24] em 25 de maio de 2018, tornou ainda mais urgente a necessidade de uma legislação específica sobre proteção de dados pessoais brasileira, uma vez que, como ele, um fator ganha ainda mais peso, a pressão político-econômica internacional. Isso porque, com o GDPR, os responsáveis pelo tratamento de dados só podem realizar transferência de dados para países ou organizações internacionais que apresentam leis que confiram grau de proteção compatível ao do Regulamento europeu. Em decorrência, o Brasil, por não possuir uma legislação específica de proteção de dados pessoais, em princípio, não poderia realizar troca de dados com a Europa, o que geraria dificuldades para as empresas aqui instaladas realizarem suas transações, bem como o enfraquecimento da competitividade e da inovação na economia nacional.

Antes disso, a necessidade de uma lei geral de proteção de dados brasileira já se salientava com as revelações do ex-analista da Agência Nacional de Segurança dos Estados Unidos, Edward Snowden, de que o governo brasileiro teria sido alvo de espionagem do governo americano[25], quando então uma

---

[24] O General Data Protection Regulation - GDPR, conjunto de normas da União Europeia que tratam da proteção e do processamento de dados dos cidadãos do bloco foi aprovado no Parlamento da União Europeia em 14 de abril de 2016, e passou a ter vigência em 25 de maio de 2018, substituindo a Diretiva 95/46, que regulava a questão até então. A alteração de diretiva para regulamento tem um grande impacto, uma vez que agora os membros da UE no lugar de terem que internalizar os regramentos da diretiva por meio da legislação nacional, o que permitia distinções de um país para o outro, a regulação cria um regime jurídico único em todos os 28 países membros, conferindo uma maior segurança jurídica. Além disso, a nova regulação europeia diferencia-se da antiga não apenas por assegurar mais direitos aos usuários e obrigações aos responsáveis pelo tratamento de dados (*data controllers*), como também por possuir abrangência global

[25] "O Brasil, com extensas redes públicas e privadas digitalizadas, operadas por grandes companhias de telecomunicações e de internet, aparece destacado em mapas da agência americana como alvo prioritário no tráfego de telefonia e dados (origem e destino), ao lado de nações como China, Rússia, Irã e Paquistão. É incerto o número de pessoas e empresas espionadas no Brasil. Mas há evidências de que o volume de dados capturados pelo sistema de filtragem nas redes locais de telefonia e internet é constante e em grande escala. [...] Companhias de telecomunicações no Brasil têm esta parceria que dá acesso à empresa americana. O que não fica claro é qual a empresa americana que tem sido usada pela NSA

Comissão de Inquérito Parlamentar deu iniciativa ao projeto de lei. Posteriormente, a importância de uma regulamentação foi evidenciada com o caso de vazamento de dados da *Cambridge Analytica*[26] e, por fim, em virtude da vigência do Regulamento Europeu de Proteção de Dados.

2.2 A Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018

Considerando todo o contexto exposto foi que, em 14 de agosto de 2018, o Presidente da República sancionou Projeto de Lei nº 53/2018, que deu origem à Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais – LGPD, que entrará em vigor a partir de fevereiro de 2020[27]. Com forte influência do modelo europeu e em evidente atenção a diversos princípios constitucionais, a Lei 13.709 tem como objetivo proteger os direitos fundamentais à liberdade e à privacidade e o livre desenvolvimento da personalidade da pessoa natural[28].

---

como uma espécie de "ponte". Também não está claro se as empresas brasileiras estão cientes de como a sua parceria com a empresa dos EUA vem sendo utilizada. Certo mesmo é que a NSA usa o programa Fairview para acessar diretamente o sistema brasileiro de telecomunicações. E é este acesso que lhe permite recolher registros detalhados de telefonemas e e-mails de milhões de pessoas, empresas e instituições." Cf. GREENWALD, Glenn; KAZ, Roberto; CASADO, José. EUA espionaram milhões de e-mails e ligações de brasileiros: país aparece como alvo na vigilância de dados e é o mais monitorado na América Latina: País aparece como alvo na vigilância de dados e é o mais monitorado na América Latina. **O Globo**. Rio de Janeiro, 6 jul. 2013. Disponível em: https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934. Acesso em: 10 jun. 2019.

[26] "Cerca de 270 mil pessoas acessaram um teste de personalidade no Facebook e aceitaram compartilhar informações de seus perfis, sem saber que, assim, estavam abrindo a porta para que o pesquisador criador do quiz acessasse também os dados de seus amigos. Foi ele que passou adiante. Dados de 87 milhões foram usados pela Cambridge Analytica, diz Facebook. a informação para a *Cambridge Analytica* — prática que o Facebook diz ser contra as regras da rede social." Cf. DADOS de 87 milhões de pessoas foram usados pela Cambridge Analytica diz Facebook: antes, informação era de que 50 milhões de usuários tinham sido afetados. **O Globo**. Rio de Janeiro, 4 abr. 2018. Disponível em: https://oglobo.globo.com/economia/dados-de-87-milhoes-foram-usados-pela-cambridge-analytica-diz-facebook-22556605. Acesso em: 10 jun. 2019

[27] A princípio a Lei n° 13.709/2018 entraria em vigor a partir de fevereiro de 2020, pois de acordo com seu art. 65 sua vigência estaria condicionada ao transcurso de 18 (dezoito) meses contados a partir da sua publicação oficial, o que ocorreu em 14 de agosto de 2018. No entanto, a Medida Provisória n° 869/2018 aprovada no Congresso alterou o *vacatio legis* para 24 (vinte e quatro) meses, o que, portanto, altera sua entrada em vigor para agosto de 2020, salvo os dispositivos referentes a Agência Nacional de Proteção de Dados - ANPD, que terão vigência imediata. O estabelecimento desse prazo possibilitará que a ANPD funcione de maneira consultiva e, dessa forma, seja útil no processo de adaptação das empresas que atuem no tratamento de dados pessoais aos dispositivos da nova lei.

[28] Art. 1º da Lei n° 13.709/2018: 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

Outrossim, entre os fundamentos em que se baseia estão: o respeito à privacidade; a inviolabilidade da intimidade, da honra e da imagem; a liberdade de informação; a autodeterminação informativa; a defesa do consumidor; os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º)[29]. Além disso, a lei se baseia nos seguintes princípios:

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

---

objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[29] Art. 2º da Lei 13.709/2018: A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

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

Diferente do Marco Civil da Internet, a chamada Lei Geral de Proteção de Dados, nos termos do art. 3º, aplica-se a qualquer operação de tratamento realizada no território nacional, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que objetivo da operação for a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional e que o titular dos dados objeto do tratamento se encontrasse em território nacional no momento da coleta. Ao mesmo tempo, a lei determina expressamente as hipóteses às quais ela não se aplica[30], dentre elas está a possibilidade de tratamento de dados pessoais para fins de segurança pública, o qual deverá ser regulado por lei específica.

A LGPD, embora só gere efeitos a partir de agosto de 2020, serve como referência na análise dos casos que envolvem o tratamento de dados pessoais já que prevê um regramento com questões específicas sobre a temática. Com efeito a lei harmoniza conceitos importantes até então trazidos em leis esparsas, dentre eles destaca-se:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

---

[30] Art. 4º da Lei n° 13.709/2018: 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; 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.

> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
>
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> VIII - encarregado: pessoa indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional; (redação alterada pela MP 689/18)[31]
>
> IX - agentes de tratamento: o controlador e o operador;
>
> 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;
>
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
>
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; [...]

Como visto, segundo a LGPD, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável. Isso significa dizer que não somente elementos óbvios como o nome, o número do RG ou número do CPF, são tidos como dados pessoais, mas também informações periféricas, as quais, muitas vezes parecem irrelevantes, porém se relacionadas a outras, podem ser utilizadas para a criação de perfis que levam à identificação de uma pessoa e, não raro, indicam os seus padrões de comportamento. Desse modo, tais interações identificáveis também são consideradas como dados pessoais. Isso posto, passa-se, agora, a análise dos elementos necessários para se proceder ao tratamento de dados pessoais, de acordo com a LGPD.

2.2.1 Requisitos para o tratamento de dados pessoais

[31] A Medida Provisória n° 689/2018 alterou o inciso VIII do art. 5°, que originalmente previa que o encarregado era a pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre o controlador e os titulares e a autoridade nacional. Com a alteração, restou afastado o termo “natural”, permitindo que a figura do encarregado seja pessoa física ou jurídica.

O tratamento de dados pessoais só é permitido nas hipóteses fixadas pela Lei 13.709[32], dentre elas, a principal situação está condicionada ao consentimento pelo titular de dados (inciso I do art. 7º). Como já verificado, o conceito de consentimento invocado pela lei no art. 5º, XII, é altamente qualificado, proporcionando carga participativa máxima ao cidadão já que ele deve exprimir uma manifestação de vontade (i) livre e inequívoca, (ii) formada mediante o conhecimento de todas as informações necessárias, e (iii) restrita às finalidades específicas informadas ao titular dos dados. Além disso, a autorização é vinculada ao controlador para o qual foi dada, fazendo com que toda transferência dos dados, nos termos do § 5º do art. 7º, submeta-se necessariamente a novo consentimento por parte do titular, dessa vez específico para aquela operação. Ademais, a demonstração desse consentimento é ônus do controlador (art. 8º, § 2º), e ele não será válido verificado qualquer vício de vontade (art. 8º, § 3º).

Em relação ao vício de vontade, a lei brasileira não faz menção explícita aos casos em que se verifica manifesto desequilíbrio entre o titular e o operador dos dados, como, por exemplo, no caso das relações consumeristas, em que a vulnerabilidade do consumidor é presumida. Porém, considerando que o consentimento é requisito *sine qua non* para o acesso a determinados serviços ou produtos, e que esses, por sua vez, dependem, na grande maioria das vezes, da concordância com contratos de adesão, o § 3º do art. 9º da LGPD estipula que “o

[32] Art. 7º da Lei n°13.709/2018: 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, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; 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.

titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18”[33].

Ante a necessidade de que autorização para o tratamento de dados seja dada para uma fim determinado, verifica-se que a validade do consentimento está intimamente relacionada ao princípio da finalidade, o qual, por sua vez, exige que os propósitos do tratamento de dados sejam legítimos, específicos, explícitos e informados ao titular (art. 6º, I). Nesses termos, a lei impede a possibilidade de que ocorra tratamento posterior de forma incompatível com essas finalidades declaradas no momento da autorização do titular dos dados. Ademais, o § 4º do art. 8º reforça a observância a esse princípio ao prever a nulidade de autorizações genéricas para o tratamento de dados pessoais.

Nesse sentido, o legislador garantiu ao titular, no artigo 9º, o direito ao acesso facilitado a informações claras, adequadas e ostensivas acerca do tratamento de seus dados, quanto a: (i) finalidade específica; (ii) forma e duração; (iii) identificação do controlador e seu contato; (iv) ao uso compartilhado de dados pelo controlador e a finalidade; (v) responsabilidades dos operadores; e (vi) direitos do titular, com menção explícita aos direitos contidos no art. 18 da lei.

Como se observa, o direito à informação está intrinsecamente relacionado ao princípio da transparência e prestação de contas. Com exceção do que pode ser considerado segredo comercial e industrial, todas as demais informações sobre o tratamento de dados devem ser prestadas ao titular, sem o que não restará observado o requisito do consentimento informado. E ainda a LGPD promove

[33] Art. 18 da Lei nº 13.709: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

importante proteção à eventual possibilidade de serem prestadas informações enganosas, abusivas ou que não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca, pois, nesses casos, de acordo com o §1º do art. 9º, o consentimento será considerado nulo.

Ademais, como o consentimento é vinculado às informações à que o titular foi cientificado, qualquer alteração nas circunstâncias que justificaram o consentimento deverá ser notificada a ele, o qual poderá revogar a autorização caso não concorde com as alterações feitas (art. 8º, §6º e art. 9º, §2º). Outro ponto importante é que o consentimento é temporário, podendo ser revogado a qualquer momento por procedimento gratuito e facilitado, conforme estabelece o §5º do art. 8º.

2.2.2 Tratamento de dados sensíveis

Ainda, um aspecto fundamental da Lei 13.709 é o tratamento especial reservado aos dados sensíveis, os quais definiu como “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”, nos termos do inciso II do artigo 5º.

Nesse sentido, a informação pessoal pode agrupar-se em categorias, às quais é atribuído grau de proteção diferenciado pelas normas de proteção de dados pessoais. Tendo isso em consideração, essas categorias podem ser assimiladas tendo como referência uma hipotética pirâmide normativa de dados, em cuja a base estariam as informações, assim definidas na Lei de Acesso à Informação como os dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato. Subindo para o meio da pirâmide, encontra-se os dados pessoais, que de acordo com a LGPD são os dados relacionados à pessoa natural identificada ou identificável. Finalmente, no topo, estariam localizados os dados pessoais sensíveis.

Os dados sensíveis permitem revelar dados a respeito de uma esfera mais íntima da pessoa humana, e que podem torná-la alvo de discriminações e de violações a direitos fundamentais. Assim, com fundamento no princípio da igualdade material, a categoria de dados sensíveis é fruto de uma necessidade pragmática de proteger o titular dos dados de eventuais discriminações ou lesões a direitos que o conhecimento ou processamento desses dados poderia ocasionar.

> "Na jurisprudência brasileira, a alegação de violação à privacidade surge com frequência em conflitos envolvendo quebra de sigilo bancário e fiscal. Se as cortes brasileiras têm reservado proteção às informações de cunho patrimonial, tutela mais intensa exigem os dados de natureza existencial, como decorrência da primazia que a Constituição assegura à dignidade humana. Com efeito, informações relacionadas à saúde, à ideologia política, à religião ou a outros aspectos íntimos da pessoa humana devem receber especial atenção da ordem jurídica." (SCHEREIBER, 2014, p.158/159)

Desse modo, considerando a necessidade de proteção especial pelo ordenamento jurídico desses dados, a Lei 13.709 os exclui de algumas das permissões estabelecidas art. 7º, como no caso de execução de contratos (art. 7º, V), de legítimo interesse do controlador (art. 7º, IX) e de proteção do crédito (art. 7º, X). Tanto que, no lugar da hipótese de legítimo interesse do controlador, o art. 11, II, "g", prevê hipótese bem mais restritiva, vinculada essencialmente aos interesses dos titulares de dados. Além disso, outra disposição relacionada ao tratamento de dados sensíveis está na própria vedação à discriminação, princípio consubstanciado no inciso IX do art. 6º. Com isso, a Lei 13.709 destaca a impossibilidade de realização do tratamento de dados para fins discriminatórios, ilícitos ou abusivos.

Não obstante, com as modernas técnicas estatísticas e de análise de dados, até mesmo informações pessoais que, em si, não são sensíveis podem causar tanto (i) um tratamento discriminatório em si, quanto (ii) a dedução ou inferência de dados sensíveis obtidos a partir de dados pessoais não-sensíveis. Em ambos os casos ocorre, efetivamente, justamente aquilo que se procura inibir com a criação de um regime especial para os dados sensíveis, que é a discriminação a partir do tratamento de dados pessoais. No entanto, essa situação não é amparada por proteção especial pela lei.

2.2.3 Dados anonimizados

Como verificado na conceituação do art. 5, III, dado anonimizado é aquele relativo à pessoa não identificada ou que não possa ser identificada considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. De acordo com o art. 12, os dados anonimizados não serão considerados dados pessoais, “salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido”.

Visando delimitar o que seriam “esforços razoáveis” o §1º do art.12 destaca que, quando da aplicação da norma, se deve levar em consideração fatores objetivos, como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. Ainda, o §2º assegura que, ainda que submetido ao processo de anonimização, serão considerados como dados pessoais “aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada”. Por fim, nos termos do §3º, “a autoridade nacional[34] poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais”.

Não obstante, esse é um ponto que merece cautela, pois, hoje, como se verá mais a frente o fenômeno do *big data*[35] e a tecnologia disponível hoje, é bastante comum a possibilidade de que a anonimização desses dados possa ser revertida. Desse modo, esses fragmentos aparentemente inócuos de informação pessoal não podem ser totalmente desconsiderados em uma regulação de proteção de dados. Além disso, por mais, que o parágrafo primeiro do art. 12 trace uma tentativa de definição do que seriam “esforços razoáveis” conforme a lei, o conceito permanece

[34] Cf. item 2.2.5
[35] Cf. Capítulo 3

demasiadamente aberto, permitindo sua reconfiguração de acordo com o caso concreto.

2.2.4 Requisitos de segurança e responsabilização

Preocupada com a segurança dos dados pessoais durante o tratamento, a lei determina que os equipamentos e serviços devem ter medidas visando proteger a privacidade e os dados pessoais dos cidadãos desde o momento da sua concepção. Nesse sentido, configurações de privacidade mais restritivas deverão ser o padrão e a implementação de métodos de anonimização serão incentivados[36].

Do princípio da prestação de contas decorre o dever dos agentes de tratamento de manterem registros de todas as operações de tratamento. Para o cumprimento dessa obrigação, as empresas deverão, portanto, elaborar relatórios de impacto à proteção de dados pessoais, contendo a descrição dos tipos de dados coletados, o fundamento da coleta e a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação as medidas, salvaguardas e mecanismos de mitigação de risco adotados, no que resulta na importância de se estruturar sistemas de segurança da informação confiáveis que permitam decisões automatizadas nos negócios.

Em caso de qualquer incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o controlador deve comunicar à autoridade nacional e ao titular o ocorrido em prazo razoável, conforme definido pela autoridade nacional, devendo descrever a natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; os riscos relacionados ao incidente; os motivos da demora, no caso de a comunicação não ter sido imediata; e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo[37].

---

[36] Cf. Arts. 46 e 47 da Lei n° 13.709/2018
[37] Cf. Art. 48 da Lei n° 13.709/2018

Por fim, quando o tratamento de dados pessoais causar dano patrimonial, moral, individual ou coletivo a outrem em violação à legislação de proteção de dados pessoais, o controlador ou o operador é obrigado a repará-lo. E as violações das normas previstas na lei, sujeitarão o infrator a multa simples ou diária, de até 2% (dois pontos percentuais) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração[38].

2.2.5 Autoridade Nacional de Proteção de Dados

O último aspecto a ser analisado é quanto a previsão de uma autoridade independente para estabelecer padrões técnicos, realizar a avaliação de cláusulas e jurisdições estrangeiras no que tange a proteção de dados, determinar a elaboração de Relatórios de Impacto, fiscalizar e aplicar sanções, atividades de difusão e educação sobre a lei, bem como demais atribuições que visam a correta aplicação da lei e os princípios da proteção de dados pessoais como um todo.

Na sanção da Lei 13.709, os dispositivos relacionados a tal entidade haviam sido vetados em razão de vício de iniciativa, eis que, de acordo com a lei, tal autoridade teria natureza de autarquia especial, o que seria de competência do Executivo e não do Legislativo nos termos do artigo 63, § 1º, II da Constituição Federal. Em decorrência, sobreveio a Medida Provisória n° 689/2018, já aprovada na Câmara dos Deputados e no Senado Federal para ser convertida em lei ordinária, que cria a Autoridade Nacional de Proteção de Dados - ANPD.

Contudo, diferente do que estabelecia texto original aprovado pelo Congresso, que previa a criação de uma autarquia autônoma ligada ao Ministério da Justiça, a MP 869/18 fundou a ANPD como órgão da administração pública federal, integrante da presidência da República e com autonomia técnica. Com isso, os especialistas temem que, do modo como foi arquitetada, a ANPD não goze

[38] Cf. Art. 52 da Lei n° 13.709/2018

de suficiente autonomia para que se tenha um ambiente de efetiva segurança jurídica, com capacidade de fomentar atividades econômicas baseadas em dados ao mesmo tempo em que assegura proteção aos titulares desses dados, especialmente quando se fala em tratamento de dados pessoais pelo Poder Público.

De todo o exposto, verifica-se que a Lei 13.709 estabelece de maneira sólida sua fundamentação nos direitos fundamentais e na proteção da pessoa humana ao, por exemplo, restringir sua aplicabilidade aos dados de pessoas naturais. Além disso, ela garante a autodeterminação informativa, ao mesmo tempo que fomenta o desenvolvimento econômico e tecnológico por meio de regras balanceadas para assegurar os interesses de todos os atores de uma economia e sociedade cada vez mais movida por dados, o que poderá ser utilizado pelas entidades privadas como diferencial competitivo e uma vantagem econômico. Por outro lado, há algumas normas que deixam a interpretação em aberto, como é o caso do tratamento dado aos dados anonimizados pela lei. Assim, muitas questões dependerão das diretrizes que a ANPD fixar.

3 RECONHECIMENTO FACIAL X PROTEÇÃO DE DADOS PESSOAIS: O CASO DAS PORTAS INTERATIVAS DIGITAIS DO METRÔ DE SÃO PAULO

O reconhecimento facial foi desenvolvido a partir da década de 1960 com fundamento nos conceitos básicos de inteligência artificial. Desde então essa tecnologia se propagou a passos largos de modo que, hoje, sistemas robustos de reconhecimento facial já são amplamente utilizados por empresas e governos. Trata-se de uma técnica que permite atribuir identidade à uma face, por intermédio da identificação positiva de um rosto em uma imagem de vídeo ou foto constante em um banco de dados pré-existente. Conforme esclarece o especialista em engenharia de produção e logística, DIANIN (20--)[39]:

> "Para o reconhecimento de face ser bem-sucedido pelo menos um rosto deve ser inserido no sistema, para criar o banco. Neste ponto, o software determina características faciais únicas de identificação, que é o que vai realmente armazenar no banco de dados. Mais tarde, quando as outras fotos são usadas para estabelecer a identidade, o software irá identificar as novas imagens com base em suas principais características e comparar estas características com as informações armazenadas no banco de dados. Se ele encontra uma correspondência, com um alto nível de confiança, ele vai ter 'reconhecido' a face particular em questão."

As tecnologias que realizam reconhecimento facial possuem grande utilidade para promover a segurança pública, tanto é assim que câmeras são usadas atualmente para a busca de suspeitos pela prática crimes em aeroportos, ruas e estádios. No carnaval de 2019, na cidade do Rio de Janeiro, câmeras foram instaladas no bairro de Copacabana visando identificar procurados pela Justiça[40]. Além disso, desde 2016 a Receita Federal começou a implantar em quatorze aeroportos brasileiros, uma tecnologia que cruza as imagens dos rostos de quem desembarca de voos internacionais com informações relativas a renda, profissão, natureza da viagem declarada, frequência de viagens, países visitados e listas de

---

39 DIANIN, Antonio Henrique. As diferenças entre detecção de rosto e reconhecimento de rosto. **Portal Educação**. [*s. l.*]. [20--]. Disponível em: https://www.portaleducacao.com.br/conteudo/artigos/informatica/as-diferencas-entre-deteccao-de-rosto-e-reconhecimento-de-rosto/67656. Acesso em: 18 maio 2019.

40 VETTORAZZO, Lucas; PITOMBO, João Pedro. Rio e Salvador terão sistema de reconhecimento facial no carnaval: capital baiana utilizará o mesmo sistema vigente na China, em que as próprias câmeras detectam rostos. **Folha de São Paulo**. Rio de Janeiro e Salvador, 27 fev. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/02/rio-e-salvador-terao-sistema-de-reconhecimento-facial-no-carnaval.shtml. Acesso em: 9 jun. 2019.

procurados por crimes como tráfico internacional de drogas e lavagem de dinheiro, por exemplo[41].

No entanto, não somente como medida de segurança pública é utilizada a prática de reconhecimento facial. Na verdade, com a inovação tecnológica, cada vez mais ela é incorporada em produtos e utilizada para diversas finalidades. O *iPhone* X, por exemplo, possibilita desbloquear a tela do celular e autenticar compras no iTunes Store, App Store e Book Store com a imagem de rosto[42]. Ademais, a rede social Facebook, por intermédio da tecnologia denominada Deepface, reconhece rostos em meio à enorme quantidade de fotos publicadas pelos usuários da rede social com 98% de precisão para sugerir a marcação de amigos nas fotos postadas[43]. No mais, com o desenvolvimento da publicidade comportamental, a tecnologia vem sendo utilizada por empresas para traçar perfis de consumo e, assim, direcionar suas campanhas publicitárias.

Embora o reconhecimento facial possa ser utilizado como um aliado para a segurança pública, proteção de dispositivos privados ou mesmo praticidade nas interações cotidianas, fato é que ele, viola sobremaneira a privacidade do titular de dados, permitindo que ocorra verdadeira vigilância. Isso porque ele permite não somente identificar individualmente o titular, com também rastrear sua localização, e, ainda, definir perfis comportamentais. Além de tudo, há dois agravantes que o tornam ainda mais danoso à privacidade: (i) muitas vezes, o reconhecimento facial ocorre sem a pessoa perceber, já que as câmeras podem estar em qualquer lugar, inclusive de forma camuflada; (ii) depois, a crescente disponibilidade de bancos de dados e dispositivos conectados potencializam a efetividade do reconhecimento facial.

---

41 ADUANA. Sistema de reconhecimento facial da Receita Federal é destaque em revista internacional. **Revista da Organização da Aviação Civil Internacional**. [*s. l.*], 1 nov. 2017. Disponível em: http://receita.economia.gov.br/noticias/ascom/2017/novembro/sistema-de-reconhecimento-facial-da-receita-federal-e-destaque-em-revista-internacional . Acesso em: 9jun. 2019.

42 APPLE INC. **Sobre a tecnologia avançada do Face ID**: saiba como o Face ID ajuda a proteger as informações no iPhone e no iPad Pro. [*s. l.*], 14 nov. 2018. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em: 11 jun. 2019.

43 SINGER, Natasha. Esforços de reconhecimento facial do Facebook geram preocupação sobre privacidade. Traduzido por Paulo Migliacci. **Folha de São Paulo**. São Paulo, 11 jun. 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/07/esforcos-de-reconhecimento-facial-do-facebook-geram-preocupacao-sobre-privacidade.shtml. Acesso em: 9 jun. 2019.

Considerando, ainda, a estratégia de usar a leitura facial para a geração de perfis comportamentais visando orientar campanhas de *marketing*, a invasão da vida privada é ainda mais grave, eis que a relação de consumo já pressupõe uma assimetria entre as partes, marcada eminentemente pela vulnerabilidade do consumidor. Desse modo, ante a possibilidade de produção desses bancos de dados, nos quais podem constar aspectos de natureza privada e de foro íntimo de cada pessoa, e a eventual comercialização dessas informações, o consumidor torna-se ainda mais vulnerável a práticas antiéticas.

Caso emblemático que ilustra os contornos de uma utilização abusiva do reconhecimento facial foi a implementação das Portas Interativas Digitais no metrô paulistano em abril de 2018. A Via Quatro, concessionária que opera a Linha amarela do sistema de trens metropolitanos de São Paulo, instalou painéis nas portas que liberam o fluxo de passageiros entre os vagões do metrô e as plataformas das estações Luz, Paulista e Pinheiros. Os painéis continham sensores capazes de reconhecer a presença humana e, através das expressões faciais e da estatura, identificar as emoções de raiva, alegria, surpresa e neutralidade, o gênero e a faixa etária das pessoas posicionadas em frente ao sistema, dados esses que, uma vez levantados, ficavam atrelados à localização e horário de captação.

Ao mesmo tempo, esses painéis veiculavam anúncios e publicidades para que a identificação da emoção ocorresse no momento em que o passageiro olhasse para eles, de modo a possibilitar captar os efeitos que produziam sobre a população em geral. Assim, segundo a empresa executora, por intermédio da identificação da reação das pessoas, as Portas Interativas tinham por finalidade categorizar os usuários do metrô para exibir propagandas mais eficientes.

A empresa responsável pela elaboração do *software* foi a AdMobilize, com sede em Miami, nos EUA, conhecida por realizar práticas como a chamada “custo por clique”, por meio da qual empresas pagam pelo número de visualizações dos

anúncios, o que é utilizado vastamente no *marketing* digital[44]. Tendo isso em vista, seria factível chegar à conclusão de que, combinando os dados levantados sobre os passageiros com suas reações às propagandas veiculadas, a AdMobilize e a Via Quatro teriam condições para construir um banco de dados de grande valor para o departamento de *marketing* de qualquer empresa.

Em decorrência, alegando que as Portas Digitais coletavam dados sem o consentimento dos passageiros e questionando uma possível venda das informações coletadas para potenciais anunciantes, o Instituto Brasileiro de Defesa do Consumidor (Idec) moveu a ação civil pública nº 1090663-42.2018.8.26.0100 em face da Via Quatro, na qual pleiteia o desligamento e a retirada das câmeras instaladas nos painéis do metrô em caráter de urgência, bem como o pagamento de indenização por danos coletivos em, no mínimo, de R$ 100 milhões, a ser destinado ao Fundo de Defesa de Direitos Difusos.

De acordo com a Promotoria de Justiça do Consumidor da Capital de São Paulo, (i) há elementos suficientes a corroborar a imputação de que a concessionária realizava coleta e tratamento de imagens e dados pessoais obtidos dos passageiros; (ii) restou comprovado a ausência de informação clara, prévia e adequada quanto à coleta e tratamento de dados ao usuário do metrô que assistia aos anúncios publicitários, ou simplesmente passava no raio de captação de imagens de câmera; e (iii) não havia qualquer garantia de que o tratamento dos dados e seu eventual armazenamento atendesse aos padrões de segurança digital. Tendo isso em vista, a decisão proferida pela juíza da 37ª Vara Cível de São Paulo deferiu a tutela de urgência para que para que a ré interrompesse, em 48 (quarenta e oito) horas, a utilização dos sensores de reconhecimento facial dos passageiros nas plataformas, sob pena de multa diária de R$ 50.000,00 (cinquenta mil reais). De acordo com a magistrada (grifos acrescidos):

> "Parece que a parte ré, ao introduzir câmeras nas portas de acesso aos trens do metrô, nas plataformas, com a captação da imagem e da expressão dos passageiros conforme apresentada publicidade nas telas, parece **violar o direito básico dos consumidores à informação**. Além disso, ao menos neste momento processual, **não está clara a exata**

[44] RINALDI, Camila. Entidades combatem câmeras do metrô de SP que leem emoções de passageiros para vender publicidade. **The Intercept Brasil**. 31 ago. 2018. Disponível em: https://theintercept.com/2018/08/31/metro-cameras-acao-civil/. Acesso em 11 abr. 2019.

> **finalidade da captação das imagens e a forma como os dados são tratados pela Via Quatro, o que, aliás, deveria ser objeto de ostensiva informação aos passageiros, inclusive diante da natureza pública do serviço prestado**".

A ação encontra-se em fase de conhecimento, por esse motivo ainda não se tem decisão definitiva a seu respeito. Contudo, tendo em vista a crescente utilização de reconhecimento facial, o caso é emblemático para a análise da tutela da proteção de dados pessoais no ordenamento jurídico brasileiro diante dos novos desafios à privacidade trazidos pela inovação tecnológica como o desenvolvimento de objetos inteligentes e a abundante quantidade de bancos de dados.

Desse modo, tendo em vista a importância da proteção de dados pessoais para garantir a privacidade do indivíduo debatida no primeiro capítulo, procura-se analisar, considerando a regulamentação brasileira relativa a temática examinada no capítulo anterior, a legalidade ou ilegalidade do tratamento de dados no caso das Portas Interativas Digitais e suas repercussões para a privacidade dos usuários do metrô. Nesse sentido, não vislumbrando esgotar as reflexões acerca do caso, a análise do caso compreenderá dois momentos: um primeiro em que se abordará a possibilidade de que a tecnologia identificasse as pessoas; e um segundo em que se avaliará a legalidade do tratamento dispendido aos dados.

3.1 Identificação dos passageiros

3.1.1 Tratamento de dados sensíveis

Como visto, a tecnologia utilizada nas Portas Interativas levantava dados a respeito da face dos passageiros. Para fins legais, a face humana é tida como um dado biométrico, que, por sua vez, é considerado como dado pessoal sensível desde 2011 pela Lei do Cadastro Positivo (Lei nº 14.414/2011), e assim permaneceu designado pela Lei nº 13.709/2018. Os dados sensíveis, como apontado no capítulo anterior, são potencialmente mais invasivos à privacidade do indivíduo, pois permitem identificar inequivocamente o sujeito, além de revelarem informações que, se má utilizadas, podem levar a práticas discriminatórias e

impedir o exercício de garantias e liberdades fundamentais. Sendo assim, o tratamento desses dados requer grau máximo de proteção.

De acordo com o Idec e as investigações jornalísticas sobre o caso, a tecnologia implementada no sistema das Portas inteligentes realizava reconhecimento facial dos passageiros. Como visto, tal técnica consiste na identificação da pessoa individualmente considerada através da imagem de seu rosto. Assim, uma primeira questão a ser definida é se as imagens coletadas pelas câmeras eram processadas e capazes de gerar identificadores únicos para cada avatar de expressão humana captada pelas câmeras instaladas no metrô, promovendo a identificação única e inequívoca de uma pessoa.

As poucas informações disponíveis sobre as Portas Digitais disponibilizadas pela Via Quatro, segundo as quais a tecnologia pode identificar a emoção exibida no rosto de uma pessoa e indicar seu gênero e sua faixa etária, sugerem que a empresa dilui o indivíduo e reconstrói a partir de seus dados uma figura em padrões de reconhecimento que são determinados por ela ou algum outro ator privado, o que, até o presente momento, é velado no processo.

Todavia, de acordo com a Via Quatro, a tecnologia empregada nas Portas Digitais realizava somente a detecção facial e não o reconhecimento, isto é, a tecnologia implementada apenas detectava pontos no rosto das pessoas, que eram convertidos em números binários sem, no entanto, armazenar qualquer imagem ou identificar o rosto de quem por ali passe. De acordo com DIANIN (20--):

> “A detecção de faces é o processo que o software de computador precisa percorrer para determinar se há realmente uma ou mais faces na imagem de uma foto ou vídeo. Ele não determina de quem são os rostos que estão na foto, apenas detecta se existem rostos na mesma. Portanto detecção facial por si só não se lembra ou armazena detalhes de rostos. Se o software detecta um rosto de uma pessoa em particular em uma imagem, e depois detecta o mesmo rosto em outra imagem, ele não reconhece que eles são a mesma pessoa, apenas reconhece que há um rosto de alguém em cada imagem. A detecção de rostos pode ser capaz de pegar algumas informações demográficas, por exemplo, a idade ou o sexo da pessoa em cada imagem, mas não muito mais do que isso. O software de detecção facial por si só não é capaz de reconhecer indivíduos.”

O reconhecimento facial por outro lado, atribui a face determinada identidade, através do cruzamento de informações com alguma base de dados. Assim, diante de uma imagem ou vídeo, ele é capaz de identificar as faces presentes, caracterizá-las matematicamente, compará-las com outras previamente cadastradas em um banco de dados e, havendo correspondência, informar à qual face do banco de dados aquela imagem condiz. Portanto, a detecção seria a primeira etapa do procedimento para se chegar ao reconhecimento facial.

Em sua defesa, a concessionária apresentou parecer técnico do Instituto Brasileiro de Peritos em Comércio Eletrônico e Telemática – IBP Brasil, segundo o qual: (i) não havia evidências que a tecnologia empregada nas Portas Digitais gerasse ou mantivesse uma base de dados prévia; (ii) tampouco foram identificadas evidências de coleta de pontos da imagem em tempo real suficientes para que se faça reconhecimento facial, ou que compare amostras com qualquer base de dados prévia nas condições acima; (iii) e ainda, as medições demográficas e de emoções necessitariam apenas de uma base de dados genérica, a qual seria insuficiente para fins de reconhecimento facial, eis que as características que definem essas medições são comuns a todas as pessoas. Ainda, conforme o parecer do IBP, as imagens dos passageiros nunca eram enviadas para o terminal controlador do sistema, portanto, nenhuma imagem seria armazenada e nenhum dado pessoal seria tratado ou gerado durante o uso do equipamento.

Com isso, a empresa argumenta que, por não ser capaz de identificar os passageiros, as Portas Interativas não coletavam dados pessoais, já que esses são definidos pela Lei 13.709 como as informações relativas à pessoa identificada ou identificável[45]. Segundo a defesa da Via Quatro, a tecnologia se limitava a contar a quantidade de pessoas que passavam em frente ao sistema de sensores, as visualizações, o tempo de permanência, o tempo de atenção, os gêneros, as faixas etárias, as emoções, o fator de visão, as horas de pico de visualizações e a distância de detecção. Assim, de acordo com a empresa, a tecnologia adotada no metrô gerava dados meramente estatísticos, sem coletar qualquer dado pessoal dos passageiros. Também destacou que todas as estimativas geradas a partir dos

[45] Cf. Art. 5°, I da Lei n° 13.709/2018 e art. 4º, IV da Lei n° 12.527/2011

dados estatísticos eram de baixa precisão, o que, segundo ela, ratifica a ausência de utilização de dados que possam tornar uma pessoa identificada ou identificável.

Não obstante, a distinção entre detecção e reconhecimento facial não encontra amparo nas legislações internacionais nem na Lei 13.709. De acordo com o Idec, “trata-se de uma distinção feita pelo próprio setor privado e por fóruns especializados em modelos de negócios para publicidade”[46]. Além disso, há inconsistência entre a defesa da Via Quatro e o projeto sobre as Portas Digitais enviado à Comissão de Monitoramento das Concessões e Permissões de Serviços Públicos dos Sistemas de Transportes de Passageiros acostado aos autos do processo, segundo o qual o sistema de painéis inteligentes realizaria reconhecimento facial.

Desse modo, a verificação de que a concessionária realizava ou não reconhecimento facial dependerá da produção de provas periciais ao longo do processo judicial. Mas, independentemente disso, fato é que as Portas Interativas coletavam dados biométricos dos usuários do metrô. Nessa ordem, destaca-se que a coleta e o tratamento de dados, e sua posterior alienação a terceiros, podem representar diversos riscos ao titular. Primeiro, porque pode levá-lo a ser alvo de discriminação por gênero ou raça, por exemplo, eis que o fornecedor pode classificar consumidores com base em perfis para atribuir vantagens a um determinado grupo em detrimento de outro. Há também, a possibilidade de ocorrerem falhas de segurança, o que pode ensejar a ocorrência de fraudes com seus dados e a exposição pública de sua imagem.

Conforme a definição de dados sensíveis, a lei não exige a vinculação dos dados à pessoa identificada ou identificável, mas tão somente que eles se refiram à pessoa natural, como é o caso em análise. Assim, o fato de haver coleta de dados biométricos, por si só, não somente enseja a aplicação da proteção de dados pessoais, mas também a observância ao tratamento especial reservado aos dados sensíveis.

---

[46] Cf. Petição inicial do Idec na ação civil pública n° 1090663-42.2018.8.26.0100.

3.1.2 Anonimização de dados

A despeito da discussão acerca da diferença entre reconhecimento e detecção facial, outro ponto levantado pela concessionária no sentido de defender que o tratamento dos dados obtidos pelo sistema das Portas Interativas não gerava a identificação das pessoas, e, portanto, não podem ser considerados pessoais, é de que os dados coletados eram anonimizados.

Como visto no segundo capítulo do presente trabalho, a Lei 13.709 não se aplica ao tratamento de dados anonimizados, assim definidos aqueles relativos à pessoa não identificada ou que não possa ser identificada considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, haja vista que não são considerados dados pessoais[47]. Sendo assim, a concessionária alega que não somente não realizava reconhecimento facial, como também que não havia de se falar em qualquer violação aos preceitos da LGPD, já que ela não se aplicaria ao caso.

Apesar disso, a lei será aplicável quando o processo de anonimização for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. A lei oferece um indício interpretativo para a expressão “esforços razoáveis” indicando que, para tanto, devem ser considerados fatores objetivos, como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. Mesmo assim, trata-se de expressão vaga e aberta, podendo ser compreendida de diversas maneiras a depender do caso. Outrossim, a lei também se aplica aos dados utilizados para formação do perfil comportamental de determinada pessoa natural identificada, ainda que submetidos ao processo de anonimização.

Quanto a formação de perfis comportamentais, embora a concessionária já tenha se pronunciado de modo a demonstrar interesses mercadológicos com o tratamento de dados e haja indícios que despertem a suspeita de que o conjunto

[47] Cf. Art. 5º, III c/c art. 12 ambos da Lei n° 13.709/2018

de dados coletados poderiam levar a elaboração desses perfis, não há como se afirmar com certeza que essa era a finalidade do projeto Portas Digitais. Não obstante, em uma economia cada vez mais orientada pelo fenômeno do *big data*, a possibilidade de que a anonimização desses dados possa ser revertida utilizando esforços razoáveis é altamente tangível.

Big data é o termo que designa uma quantidade volumosa de dados estruturados, semiestruturados ou não estruturados que têm o potencial de ser explorados para obter informações (MAGRANI, 2018). Trata-se de um conceito para definir o fenômeno provocado pela enorme quantidade de dados de variados formatos produzidos em curto espaço de tempo aliada à alta velocidade com que são analisados e visualizados. Embora organizada, o *big data* refere-se à informação bruta, isto é, sem passar por nenhum tipo de interpretação. Segundo Hannes Grassegger e Mikael Krogerus:

> "Big data significa, em essência, que tudo o que fazemos, tanto online como offline, deixa vestígios digitais. Cada compra que fazemos com nossos cartões, cada busca que digitamos no Google, cada movimento que fazemos quando nosso telefone celular está em nosso bolso, cada like é armazenado. Especialmente cada like. Durante muito tempo, não era inteiramente claro o uso que esses dados poderiam ter — exceto, talvez, que poderíamos encontrar anúncios de remédios para hipertensão logo após termos pesquisado no Google "reduzir a pressão arterial". (GRASSEGGER e KROGERUS apud MAGRANI, 2018)

Em relação aos riscos para a privacidade, Paul Ohm critica a crença na anonimização dos dados e argumenta que, por mais que um dado tenha sido suprimido para garantir a privacidade do usuário, é possível reidentificá-lo (ou desanonimizá-lo) por meio do cruzamento de outras informações disponíveis na rede (MAGRANI, 2018, p. 97). Scott R. Peppet argumenta ainda que, mesmo que o conjunto de dados coletados pelos sensores seja considerado esparso, a reidentificação ainda é possível. Isso porque os sensores utilizados no reconhecimento facial registram uma multiplicidade de dados e os correlacionam com diferentes tipos de dados, permitindo a identificação de traços capazes de destacar determinados usuários de outros (MAGRANI, 2018, p. 97). Portanto, ainda que os dados sejam anonimizados, isso não significa que os requisitos

estabelecidos na Lei 13.709 para o tratamento de dados não precisem ser observados.

3.2 Coleta ilegal de dados

O Idec sustenta ter ocorrido no caso verdadeiro tratamento ilegal de dados pessoais em virtude da captura de imagens nas câmeras que foram instaladas nas Portas Interativas pela Via Quatro. Nesse sentido, sustenta que essa coleta é ilegal baseando-se, principalmente, em dois aspectos centrais da Lei nº 13.709: a ausência de informação clara sobre o funcionamento e a finalidade do sistema de sensores instalados nas portas do metrô; e a ausência de consentimento prévio e informado por parte dos passageiros que tiveram seus dados coletados.

3.2.1 Ausência de informações

A divulgação da tecnologia implementada no transporte paulistano restringiu-se a uma nota[48] destinada à imprensa na página eletrônica da Via Quatro poucos dias antes do início da execução do projeto. Nesse comunicado, o presidente da concessionária, Harald Zwetkoff afirmou (grifos acrescidos):

> "As portas de plataforma interativas são uma tecnologia inovadora desenvolvida pela Via Quatro para aprimorar transmissão de informações

[48] "Conectada a inovações tecnológicas que resultam em prestação de serviço com qualidade aos usuários, a Via Quatro, concessionária que opera a Linha 4-Amarela de metrô, inaugura, dia 18 de abril, um novo recurso visual, que auxiliará a comunicação com passageiros. A novidade é a instalação de portas de plataforma interativas nas estações Luz, Paulista e Pinheiros, com funcionamento durante todo o horário de operação da linha. As portas interativas digitais serão estratégicas para a comunicação da Via Quatro e seus parceiros com os usuários. Cada estação receberá quatro portas interativas, na área central da plataforma, sendo a instalação em pares e de forma espelhada. Modelo inédito de interatividade com o público, as portas digitais interativas são um recurso visual tecnológico, que visa incrementar a comunicação com o passageiro, por meio de transmissão de campanhas de orientação, mensagens de prestação de serviço e anúncios publicitários. Sua tecnologia é formada por uma lente com sensor que reconhece a presença humana e identifica a quantidade de pessoas que passam e olham para tela. Basicamente os dados gerados são identificação de expressão de emoção (raiva, alegria, neutralidade) e características gerais que podem indicar se é um rosto feminino ou masculino. 'As portas de plataforma interativas são uma tecnologia inovadora desenvolvida pela Via Quatro para aprimorar transmissão de informações aos passageiros da Linha 4-Amarela. Essa nova ferramenta na área de comunicação e marketing, com recursos sofisticados, pode colaborar na criação de novas estratégias para públicos específicos, visando mais efetividade na troca de mensagens importantes ou mesmo o incremento em vendas', explica Harald Zwetkoff, presidente da Via Quatro." Cf. nota integral divulgada no *site* da Via Quatro.

> aos passageiros da Linha 4-Amarela. Essa nova ferramenta na área de comunicação e marketing, com recursos sofisticados, **pode colaborar na criação de novas estratégias para públicos específicos, visando mais efetividade na troca de mensagens importantes ou mesmo o incremento em vendas**"

Assim, o sistema começou a operar sem que houvesse qualquer anúncio prévio a respeito de sua implementação, seu funcionamento e suas finalidades aos passageiros, nem havia qualquer sinalização no metrô de que era realizada coleta de dados. Ao mesmo tempo, mídia, população e especialistas em direito digital levantaram críticas a respeito da tecnologia por trás das Portas Digitais, sobretudo acerca da sua finalidade, cogitando-se, inclusive, a possibilidade de eventual utilização dos dados captados por empresas anunciantes. Tais suspeitas foram reforçadas com a declaração do presidente da Via Quatro ao portal eletrônico CityLab, na matéria intitulada "The Metro Stations of São Paulo That Read Your Face"[49] , em que informou que o projeto tinha a multinacional LG e a empresa farmacêutica HyperaPharma, detentora das marcas Epocler e Apracur, como anunciantes.

Em razão da repercussão negativa, a Via Quatro emitiu nova nota[50] à imprensa, que, diferente da primeira, omitiu o caráter mercadológico da invenção, afirmando que a principal funcionalidade seria tão somente a veiculação de avisos ao público. Ainda, a segunda comunicação, informou que a tecnologia utilizada no projeto não era capaz de recolher ou cruzar dados dos passageiros, nem captava, gravava ou armazenava imagens deles. Por fim, em agosto, a empresa retirou da sua página virtual qualquer menção à nova tecnologia.

---

[49] Cf. AMIGO, Ignacio. As estações de metrô de São Paulo que lêem seu rosto. **City Lab**. São Paulo, 08 mai. 2018. Disponível em: https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/. Acesso em: 11 abr. 2019.

[50] "Conectada a inovações tecnológicas que resultam em prestação de serviço com qualidade aos passageiros, a Via Quatro, concessionária responsável pela operação e manutenção da Linha-4-Amarela do metrô, dispõe de um novo recurso visual. A novidade, em funcionamento há menos de um mês, está presente nas estações Luz, República, Paulista, Fradique Coutinho, Faria Lima, Pinheiros e Butantã. Localizada na área central das plataformas, as portas digitais são um recurso visual-tecnológico, que incrementa a comunicação com o passageiro, por meio de veiculação de campanhas de orientação, mensagens de prestação de serviço, além de anúncios publicitários." Cf. Nota integral divulgada no site da Via Quatro.

Quanto a falta de informação a respeito do tratamento de dados, o Ministério Público, considerou que a conduta dispensada pela empresa constitui afronta direta ao art. 6º, III do CDC, o qual garante a informação adequada, clara e especificada sobre os diferentes produtos e serviços, e inclusive sobre os riscos que apresentem, e ao art. 7º, VIII do MCI, que impõe um dever de transparência por parte dos agentes de dados, sobretudo, quanto à delimitação da finalidade específica do tratamento.

Outrossim, o direito ao acesso a informações do titular de dados é resguardado pelo art. 43 do CDC, que institui para as empresas dever de comunicar, de maneira acessível, os consumidores sobre as informações registradas em cadastros sobre ele, e suas respectivas fontes. Na mesma linha, o art. 31 da Lei de Acesso à Informação, assegura que o tratamento de informações pessoais deve ser feito de forma transparente.

Também a Lei do Cadastro Positivo com as alterações introduzidas pela LC 166/19, assegura que os consumidores devem ser informados a respeito da abertura de cadastros em seu nome no prazo de até trinta dias, bem como têm direito de receber informações claras e objetivas sobre os canais disponíveis para cancelamento de seu cadastro[51]. Além disso, ela garante algumas prerrogativas ao consumidor como o acesso gratuito às informações sobre ele existentes; conhecimento dos principais elementos e critérios considerados para a análise de risco; ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais; e a revisão de decisões automatizadas[52].

Já a Lei Geral de Proteção de Dados determina que o tratamento de dados se orienta pelo princípio da finalidade, adequação, necessidade, livre acesso, transparência, responsabilização e prestação de contas. Do princípio da finalidade, decorre que o encarregado pelos dados tem o dever de se manifestar de forma clara acerca da finalidade do tratamento, pois o consentimento[53] ficará vinculado

---

[51] Cf. art. 4º, §4º da Lei nº 14.414/2011 com a redação dada pela Lei Complementar nº 166/2019
[52] Cf. art. 5° da Lei nº 14.414/2011com a redação dada pela Lei Complementar nº 166/2019
[53] Ver item 3.2.2

àquele fim específico. Ainda, ter a finalidade delimitada para que seja possível verificar a adequação e a necessidade dos dados coletados. Apesar disso, não somente a finalidade do tratamento de dados necessita ser anunciada, mas também todas as demais informações sobre o tratamento de dados devem ser prestadas ao titular, com exceção do que pode ser considerado segredo comercial e industrial, sem o que não restará observado o requisito do consentimento informado[54]. Sendo assim, a comunicação das informações a respeito das operações realizadas com os dados pessoais é pré-requisito para que as demais imposições estabelecidas pela lei sejam observadas, como a necessidade de obter o consentimento do titular que se analisará a seguir.

Desse modo, considerando a postura adotada pela Via Quatro, verifica-se a ausência de transparência e a oscilação de posicionamentos em relação ao às Portas Digitais, violando todo esse sistema normativo que assegura o acesso às informações sobre o tratamento de dados. Conforme aponta o Idec, a concessionária não se portou como uma fonte confiável de informações sobre o funcionamento e as finalidades da tecnologia implementada. Assim, ao agir dessa forma, a empresa afastou a possibilidade de que os passageiros formassem uma opinião informada sobre permitir, negar ou revogar a cessão de dados, bem como de buscarem formas de reivindicar seus direitos ou ainda alguma fiscalização sobre o exercício do sistema de sensores.

3.2.2 Ausência de consentimento

Além da falta de transparência da concessionária frente aos usuários do metrô, verifica-se que em nenhum momento ela procurou obter a autorização dos passageiros para proceder a coleta dos dados. Assim, ainda que a empresa tivesse divulgado amplamente as informações necessárias para que os passageiros formassem uma opinião sobre autorizar ou não a coleta de dados, fato é que não havia a possibilidade de escolha, os dados eram captados pelos sensores, independentemente de consentimento pelo titular. Na verdade, da maneira como o

[54] Ver item 3.2.2

sistema foi concebido, os passageiros nem tinham como saber que os dados eram coletados, já que ao olhar para as telas, não era visível a presença de câmeras.

De acordo com o parecer do Ministério Público, a conduta da Via Quatro viola diversas normas do ordenamento brasileiro, como o art. 6º, II do CDC que assegura a liberdade de escolha como direito básico do consumidor, e o art. 7º, VII e IX do MCI, que asseguram ao usuário da internet, respectivamente (i) o não fornecimento a terceiros de seus dados pessoais, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; e (ii) o direito ao consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais. Ainda, o art. 31 da Lei de Acesso à Informação dispõe que qualquer transferência de dados a terceiros apenas poderá ser realizada caso estipulada por previsão legal ou com o consentimento expresso do titular. Além disso, o Ministério Público sustenta que:

> "A captação de dados sem o consentimento do titular, aliás, coaduna-se com a forma pela qual o sistema 'Porta Digitais' foi concebido para coletar imagens de modo dissimulado. Assim se conclui pela camuflagem da câmera no painel eletrônico publicitário em posição tal que passa despercebido ao usuário, atraído para olhar as mensagens publicitárias, ser ele próprio objeto de filmagem não autorizada".

Ademais, considerando a LGPD, a Via Quatro estaria violando o art. 7º, I, que condiciona o tratamento de dados pessoais ao consentimento livre, inequívoco e informado do titular deles. Consentimento esse, ainda, que, nos termos do art. 8º, caput e §§ 2º e 3º, precisa ser realizado de modo manifesto e cuja demonstração é ônus do agente de tratamento de dados.

Outrossim, o Idec compara as Portas Interativas com um caso semelhante ocorrido na Holanda em junho de 2018, no qual uma empresa holandesa que havia instalado um sistema de "outdoors digitais", denominado *Normenkader Digitale Billboards*, ao quais eram acopladas câmeras que identificavam as reações dos transeuntes. Após denúncias de cidadãos incomodados com a violação à proteção de seus dados pessoais, a Autoridade de Proteção de Dados Pessoais da Holanda notificou a empresa para que ela interrompesse os processos de coletas de dados

pessoais sem consentimento dos titulares. Segundo a nota oficial[55] sobre a advertência da autoridade holandesa, obtida em seu sítio eletrônico (grifos acrescidos):

> "As pessoas só podem ser observadas através de câmeras em outdoors sob determinadas condições. Após denúncias de transeuntes preocupados, a Autoridade da Holanda para a Proteção de Dados Pessoais (AP) deu mais explicações para a indústria sobre as regras de proteção de dados pessoais neste ponto. Observar pessoas através de uma câmera em outdoors geralmente é um processamento de dados pessoais. Quase sempre a permissão dos transeuntes é necessária para cumprir a legislação de privacidade. A Autoridade de Dados Pessoais apela à indústria para tomar medidas para cumprir a lei de proteção de dados pessoais. (...) Se as pessoas parecem reconhecíveis, existe um processamento de dados pessoais. Isso significa que a legislação europeia de proteção de dados pessoais (GDPR) se aplica. Um operador deve ter uma base legal para processar esses dados. (...) Na prática, isso significa que um operador do sistema de outdoors digitais deve ter o consentimento do transeunte para poder processar seus dados. De acordo com a Lei Geral de Proteção de Dados Pessoais, esse consentimento deve atender a várias condições. Por exemplo, o consentimento deve ser informado e específico. **Deve ficar claro quais dados alguém dá permissão e para qual propósito específico os dados são usados pelo anunciante. Um operador de exibição pode, por exemplo, fazer isso solicitando uma autorização específica através de uma etapa intermediária com um código QR ou um aplicativo.**"

Dessa forma, considerando a inspiração da Lei nº 13.709/18 no *General Data Protection Regulation* da União Europeia, a interpretação da autoridade holandesa oferece um importante precedente para interpretação do arcabouço normativo brasileiro acerca da proteção de dados pessoais, inclusive do consumidor.

Outro importante precedente para a discussão sobre consentimento e coleta de dados pessoais é o caso "União versus Microsoft"[56], proposta em razão de coleta de dados pessoais sem consentimento do titular pelo Windows 10. No feito, a União alegou que qualquer coleta de dado pessoal dos usuários somente poderia ocorrer com expressa e prévia autorização deles, nos termos do art. 6º do Código de Defesa do Consumidor. Ainda, de acordo com o pleito da União, o

---

[55] AUTORITEIT PERSOONSGEGEVENS. **AP informeert branche over norm camera's in reclamezuilen. Nieuwsbericht**, 26 jun. 2018. Disponível em: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera%E2%80%99s-reclamezuilen. Acesso em: 20 maio 2019.

[56] Ação civil pública nº 5009507-78.2018.4.03.6100 da 9ª Vara Cível Federal de São Paulo. Decisão disponível no sítio do Observatório do Marco Civil da Internet: http://www.omci.org.br/m/jurisprudencias/arquivos/2018/jfsp_50095077820184036100_27042018.pdf.

consentimento deveria se dado com alertas específicos sobre suas consequências para a privacidade para cada tipo de dado ou informação pessoal a ser coletado. Em decisão de antecipação de tutela, a juíza julgou que:

> "vislumbra-se em parte, todavia, a plausibilidade parcial do direito invocado, no tocante a determinar-se que a Microsoft adote procedimentos específicos, no prazo de 30 (trinta) dias, de modo a permitir que o usuário do sistema operacional Windows 10, em caso de não autorizar o uso de seus dados, tenha ferramenta operacional que permita o exercício de tal opção de forma tão simples e fácil quanto a que permite a atualização com a autorização dos dados".

À luz dos casos que também envolvem coleta de dados pessoais sem a autorização expressa do titular, depreende-se que estaria também embasado o pedido de cessação de violação de direito e obrigação de fazer específica para que os usuários da Linha Amarela do metrô de São Paulo possam dar consentimento informado e em destaque na coleta de seus dados pessoais por meio das câmeras instaladas na portas interativas.

Assim, nos termos em que os fatos ocorreram, o usuário não tinha a opção de recusar a coleta de dados. De acordo com o Idec a prática seria uma espécie de pesquisa de opinião compulsória, o que viola a Constituição Federal e diversas leis infraconstitucionais que compõem o arcabouço da proteção de dados pessoais brasileiro, além de configurar uma prática que vai na contramão da LGPD, à quem as empresas já devem começar a se adaptar tendo em vista que será a principal regulação sobre o tema em vigor a partir de agosto de 2020. Tendo isso em vista, de acordo com o parecer da Promotoria de Justiça do Consumidor:

> "Trata-se de prática comercial abusiva, dentre aquelas vedadas pelo rol exemplificativo do artigo 39 do C.D.C., por se valer a Via Quatro, em sua atividade, de método comercial desleal (art. 6º, IV) para enganar o consumidor, faltando com o dever de transparência (art. 4º, caput) e com cláusula geral de boa-fé objetiva (art. 4º,III), que devem pautar suas relações com os usuários de seus serviços, que devem ser, sobretudo, adequados (art. 6º, VIII)".

Desse modo, a decisão foi imposta pela Via Quatro aos passageiros, que se viam obrigados a aceitá-la caso quisessem utilizar o transporte público já que a instalação ficava bem na porta dos vagões, por onde, necessariamente, passariam as pessoas que fossem embarcar ou desembarcar. Portanto, a única

alternativa ao passageiro que não quisesse se submeter a tal sistema era simplesmente usar outro meio de locomoção pela cidade. Além de tudo, os passageiros não ganhavam nada com isso, ao contrário, ainda pagavam as passagens do metrô.

CONCLUSÃO

Da análise do caso das Portas Interativas Digitais é possível extrair importantes observações acerca da proteção de dados pessoais no Brasil, especialmente quanto às características próprias das tecnologias que realizam reconhecimento facial. Primeiramente, verificou-se a necessidade de se ter um direito à proteção de dados pessoais como mecanismo de garantia da privacidade, e quais as necessidades para sua tutela. Depois, se analisou como esse direito é garantido pelo ordenamento jurídico brasileiro e em que medida ele atende às demandas que a proteção de dados pessoais exigem. E, por fim, na análise do caso das portas digitais do metrô de São Paulo, se discorreu acerca dos desafios à proteção de dados trazidos pelo reconhecimento facial, como representante da utilização integrada do *big data* e de dispositivos inteligentes.

Verificou-se que a privacidade hoje não se limita a um direito subjetivo como em seus primórdios. Ao contrário, ela teve que se adaptar à dinamicidade e à pluralidade que o desenvolvimento da Sociedade de Informação exigia. Da evolução da privacidade como liberdade positiva chegou-se à acepção do direito à proteção de dados pessoais atual, de caráter coletivo e corolário da autodeterminação informativa, e que vem descobrindo seu modo de se expressar diante das constantes alterações promovidas pela inovação tecnológica.

Ao longo do estudo, ainda, foram mencionados diversos casos de utilização de reconhecimento facial, que demonstram o crescente uso dessa tecnologia para variadas finalidades. De fato, como já intuído antes da pesquisa, o reconhecimento facial é uma tecnologia que afeta ainda mais a privacidade do indivíduo comparada a outras. Isso porque, primeiro ele permite identificar individualmente a pessoa; depois, ele coleta dados biométricos, isto é, dados que permitem revelar não apenas a identidade, mas também informações que podem ser utilizadas contra o sujeito de forma discriminatória ou impedindo, até mesmo, o gozo de direitos fundamentais; e, ainda, ele permite revelar a localização da pessoa. Além, os dispositivos que o realizam podem estar instalados em qualquer lugar, às vezes,

inclusive, podem estar escondidos, possibilitando que a pessoa tenha sua imagem captada sem, ao menos, saber.

Por tudo isso, é preciso tomar muito cuidado com a banalização do reconhecimento facial. É inegável que ele tem sua utilidade dentro da sociedade, mas considerando que ele permite tamanha violação da privacidade, é preciso usá-lo somente quando extremamente necessário, e não, por exemplo, para realização de pesquisas de opinião - como ocorreu aparentemente no caso das portas interativas - que poderiam ser facilmente realizada, por meio de questionários, por exemplo.

Da análise do caso envolvendo as Portas Interativas Digitais, verifica-se que a alegação da Via Quatro de que os dados coletados eram impessoais, não se coaduna com a coleta de dados biométricos pelo sistema de sensores instalados nas portas do metrô. Considerando, portanto, que havia verdadeiro tratamento de dados pessoais, a conduta da concessionária esbarra em diversas violações à regulamentação brasileira a respeito da temática, sobretudo, no que tange às relações de consumo. Diante disso, a análise da coleta ilegal de dados, centrou-se em dois aspectos fundamentais: a ausência de informações a respeito da finalidade e do funcionamento do tratamento de dados e de consentimento dos titulares para a prática.

Verificando o ordenamento jurídico brasileiro, constata-se que há um arcabouço de proteção de dados pessoais que necessita ser interpretado sistematicamente para garantir proteção ao titular de dados. Quanto a Lei nº 13.709/18 que regula especificamente a proteção de dados pessoais, verifica-se que ela comtempla uma sólida regulamentação quanto às especificidades da questão, promovendo a autodeterminação informativa. Contudo, a análise do caso revela alguns aspectos em que a lei abre brecha para que as empresas, na prática, usufruam delas para afastar a aplicação da lei, e não tenham que adotar as exigências por ela estipuladas.

No caso, em razão da LGPD ainda não estar em vigor, a interpretação sistemática das legislações esparsas que compõem o arcabouço jurídico que tutela a proteção de dados brasileira é fundamental para efetiva garantia desse direito. Não obstante, parece que a resolução do caso dependerá fortemente da normativa consumerista. Mais que tudo, considerando a compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, as portas interativas concretizam eminente prática abusiva no fornecimento do serviço de transporte público, caracterizando verdadeira afronta ao princípio da boa-fé das relações jurídicas.

Ao mesmo tempo, o caso paulista antecipa alguns argumentos que muitas empresas poderão se valer quando da vigência da lei de dados. Nesse sentido, percebe-se que o ponto nerval da questão é o afastamento da pessoalidade dos dados sob o fundamento da anonimização. Essa argumentação não se aplica ao caso das portas digitais, como visto, por envolver dados sensíveis e se fundar em bases consumerista, porém, muitas situações poderão ficar de fora do âmbito de aplicação da Lei nº 13.709 em virtude da anonimização.

O fenômeno do *big data* aliado ao desenvolvimento de dispositivos inteligentes revolucionou as operações de tratamentos de dados, tornando a linha divisória entre dados pessoais e dados anonimizados bastante tênue. Com a enorme diversidade e quantidade de dados existentes, cada indivíduo deixa seu rastro digital, assim, mesmo que um dado seja suprimido para garantir a privacidade do usuário, é possível reidentificá-lo por meio do cruzamento de outras informações disponíveis na rede.

A LGPD, embora preveja a possibilidade de anonimização ser revertida, não delimita os contornos da anonimização, ao passo que atrela a possibilidade de reversão à condição de que seja feita por esforços razoáveis *e* por meios próprios, conceitos esses que não são esclarecidos pela lei. Portanto, ficará a cargo da Autoridade Nacional de Proteção de Dados, delimitar o processo de anonimização considerando a sensibilidade da questão. Enquanto tal esclarecimento não vier, os agentes de tratamento de dados deverão desenvolver políticas robustas de

controle de anonimização para mitigar os riscos de eventual descumprimento da lei, e de prejuízos aos cidadãos. Todavia, tendo em vista como foi formulada a Autoridade pela MP n° 869/18, há contundente preocupação a respeito de sua autonomia para orientar a aplicação da lei com efetiva segurança jurídica.

REFERÊNCIAS BIBLIOGRÁFICAS

ADUANA. Sistema de reconhecimento facial da Receita Federal é destaque em revista internacional. **Revista da Organização da Aviação Civil Internacional**. [*s. l.*], 1 nov. 2017. Disponível em: http://receita.economia.gov.br/noticias/ascom/2017/novembro/sistema-de-reconhecimento-facial-da-receita-federal-e-destaque-em-revista-internacional . Acesso em: 9 jun. 2019.

AMIGO, Ignacio. As estações de metrô de São Paulo que lêem seu rosto. **City Lab.** São Paulo, 08 mai. 2018. Disponível em: https://www.citylab.com/design/2018/05/the-metro-stations-of-sao-paulo-that-read-your-face/559811/. Acesso em: 11 abr. 2019.

APPLE INC. **Sobre a tecnologia avançada do Face ID**: saiba como o Face ID ajuda a proteger as informações no iPhone e no iPad Pro. [*s. l.*]. 14 nov. 2018. Disponível em: https://support.apple.com/pt-br/HT208108. Acesso em: 11 jun. 2019.

AUTORITEIT PERSOONSGEGEVENS. **AP informeert branche over norm camera's in reclamezuilen**. Nieuwsbericht, 26 jun. 2018. Disponível em: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-informeert-branche-over-norm-camera%E2%80%99s-reclamezuilen. Acesso em: 20 maio 2019.

BARROSO, Luís Roberto. A viagem redonda: habeas data, direitos constitucionais e provas ilícitas. In: WAMBIER (coord.). Habeas data. São Paulo: **Revista dos tribunais**, 1998.

BIONI, Bruno. A produção normativa no cenário transfronteiriço. In: CONPENDI/UFSC (org.). **Direito e novas tecnologias**: XXIII Encontro Nacional do CONPEDI. Florianópolis: CONPENDI, 2014. Disponível em: http://www.publicadireito.com.br/artigos/?cod=575dc1140c7f1254. Acesso em: 17 ago. 2018.

BRANCO, Sérgio; TEFFÉ, Chiara de (Org.). **Privacidade em perspectivas**. Rio de Janeiro: Lumen Juris, 2018.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Diário Oficial da União: Seção 1, Brasília, DF, ano 126, n. 191-A, p. 1-32, 05 out. 1988.

_____ . Lei nº 10.406 de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**: Seção 1, Brasília, DF, ano 139, n. 8, p. 1-74, 11 jan. 2002.

_____ . Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**: Seção 1, Brasília, DF, p. 1-4, 18 nov. 2011.

_____ . Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Diário Oficial da União: Seção 1, Brasília, DF, p. 2, 10 jun. 2011, alterada pela Lei Complementar n° 166, de 8 de abril de 2019. Altera a Lei Complementar nº 105, de 10 de janeiro de 2001, e a Lei nº 12.414, de 9 de junho de 2011, para dispor sobre os cadastros positivos de crédito e regular a responsabilidade civil dos operadores. **Diário Oficial da União**: Seção 1, Brasília, DF, ano 157, n. 68, p. 1, 9 abr. 2019.

_____ . Lei n° 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil. **Diário Oficial da União**: Seção 1, Brasília, DF, ano 151, n. 77, p. 1, 24 abr. 2014.

_____ . Lei n° 13.709 de 14 de agosto 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**: Seção 1, Brasília, DF, n. 157, p. 59, 15 ago. 2018, alterada pela Medida Provisória n° 689 de 2018.

BUZANOVSKY, Flavio; LEITE, Douglas. Brasil aprova nova lei do Cadastro Positivo: Novas regras entram em vigor no dia 9 de julho de 2019. Veja o que muda. **Jota**. [*s. l.*], 10 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/brasil-aprova-nova-lei-do-cadastro-positivo-10042019. Acesso em: 30 maio 2019.

CEROY, Frederico Meinberg. Dados pessoais sensíveis: Três projetos de lei que tramitam no Congresso Nacional abordam o tema. **Jota**. [*s. l.*], 29 nov. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/dados-pessoais-sensiveis-29112017. Acesso em: 30 maio 2019.

DADOS de 87 milhões foram usados pela Cambridge Analytica diz Facebook: antes, informação era de que 50 milhões de usuários tinham sido afetados. **O Globo**. Rio de Janeiro, 4 abr. 2018. Disponível em: https://oglobo.globo.com/economia/dados-de-87-milhoes-foram-usados-pela-cambridge-analytica-diz-facebook-22556605. Acesso em: 10 jun. 2019.

DIANIN, Antonio Henrique. As diferenças entre detecção de rosto e reconhecimento de rosto. **Portal Educação**. [*s. l.*], [20--]. Disponível em: https://www.portaleducacao.com.br/conteudo/artigos/informatica/as-diferencas-entre-deteccao-de-rosto-e-reconhecimento-de-rosto/67656. Acesso em: 18 maio 2019.

DONEDA, Danilo. A tutela da privacidade no Código Civil de 2002. **Anima: Revista Eletrônica do Curso de Direito da Opet**, v. 1, p. 89-100, Curitiba, 2009. Disponível em: http://www.anima-opet.com.br/pdf/anima1/artigo_Danilo_Doneda_a_tutela.pdf. Acesso em: 10 fev. 2019.

_____ . **Da Privacidade à Proteção de Dados Pessoais**. Rio de Janeiro: Saraiva, 2006.

FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis: A quinta parte de uma série sobre as repercussões para a atividade empresarial. **Jota**. [s. l.], 26 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 30 maio 2019.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. EUA espionaram milhões de e-mails e ligações de brasileiros: país aparece como alvo na vigilância de dados e é o mais monitorado na América Latina: País aparece como alvo na vigilância de dados e é o mais monitorado na América Latina. **O Globo**. Rio de Janeiro, 6 jul. 2013. Disponível em: https://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934. Acesso em: 10 jun. 2019.

MAGRANI, Eduardo. **Internet das Coisas**. Rio de Janeiro: FGV Editora, 2018.

MARTINS, Guilherme Magalhães (coord.); LONGHI, João Victor Rozatti (coord.). **Direito digital:** direito privado e internet. 2 ed. Indaiatuba, SP: Editora Foco, 2019.

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Philip; ROTENBERG, Marc (org.). **Technology and privacy: the new landscape**. Cambridge: MIT Press, 1997, p. 219-242.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. **Revista de Direito do Consumidor**, n. 106, jul./ago., [s. l.], 2016.

RINALDI, Camila. Entidades combatem câmeras do metrô de SP que leem emoções de passageiros para vender publicidade. **The Intercept Brasil**. 31 ago. 2018. Disponível em: https://theintercept.com/2018/08/31/metro-cameras-acao-civil/. Acesso em 11 abr. 2019.

RODOTÁ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Organização, seleção e apresentação de: Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

REIA, Jhessica *et al*. (org.). **Horizonte presente**: tecnologia e sociedade em debate. Belo Horizonte: Casa do Direito; FGV – Fundação Getúlio Vargas, 2019.

SANTOS, Maike Wile dos. O big data somos nós: a humanidade de nossos dados. **Jota**, [s. l.],16 mar. 2017. Disponível em: https://jota.info/ colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-big-data-somos-nos-a-humanidade-de-nossos-dados-16032017. Acesso em: 27 mar. 2019.

SÃO PAULO. Tribunal de Justiça do Estado de São Paul. 9ª Vara Cível. Decisão de antecipação de tutela. **Ação civil pública nº 5009507-78.2018.4.03.6100**. São Paulo, 27 abr. 2018. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2018/jfsp_500950778201840361 00_27042018.pdf. Acesso em: 20 maio 2019.

_____ . Tribunal de Justiça do Estado de São Paulo. 37ª Vara Cível. Decisão de antecipação de tutela. **Ação civil pública nº 1090663-42.2018.8.26.0100**. São Paulo, 14 set. 2018.

SINGER, Natasha. Esforços de reconhecimento facial do Facebook geram preocupação sobre privacidade. Traduzido por Paulo Migliacci. **Folha de São Paulo**. São Paulo, 11 jun. 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/07/esforcos-de-reconhecimento-facial-do-facebook-geram-preocupacao-sobre-privacidade.shtml. Acesso em: 9 jun. 2019.

SCHEREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2014.

VETTORAZZO, Lucas; PITOMBO, João Pedro. Rio e Salvador terão sistema de reconhecimento facial no carnaval: capital baiana utilizará o mesmo sistema vigente na China, em que as próprias câmeras detectam rostos. **Folha de São Paulo**. Rio de Janeiro e Salvador, 27 fev. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/02/rio-e-salvador-terao-sistema-de-reconhecimento-facial-no-carnaval.shtml. Acesso em: 9 jun. 2019.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, v. 4, n. 5, p. 193-220, Cambridge,15 dez.1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em 20 maio 2019.