UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

RECONHECIMENTO FACIAL E *SURVEILLANCE*: DESAFIOS À PROTEÇÃO DE DIREITOS FUNDAMENTAIS ANTE À COLETA INDISCRIMINADA DE DADOS PESSOAIS BIOMÉTRICOS

AMANDA LUNA DE AZEVEDO TERRA

RIO DE JANEIRO
2021

AMANDA LUNA DE AZEVEDO TERRA

RECONHECIMENTO FACIAL E *SURVEILLANCE*: DESAFIOS À PROTEÇÃO DE DIREITOS FUNDAMENTAIS ANTE À COLETA INDISCRIMINADA DE DADOS PESSOAIS BIOMÉTRICOS

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 da **Professora Dra. Cintia Muniz de Souza Konder**.

Rio de Janeiro

2021

AMANDA LUNA DE AZEVEDO TERRA

RECONHECIMENTO FACIAL E *SURVEILLANCE*: DESAFIOS À PROTEÇÃO DE DIREITOS FUNDAMENTAIS ANTE À COLETA INDISCRIMINADA DE DADOS PESSOAIS BIOMÉTRICOS

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 da **Professora Dra. Cintia Muniz de Souza Konder**.

Data da aprovação: __/__/____.

Banca Examinadora:

_____
Orientadora

_____
Membro da Banca

_____
Membro da Banca

Rio de Janeiro

2021

RESUMO

A presente monografia analisa as implicações do desenvolvimento e da utilização de tecnologias de reconhecimento facial como ferramenta de *surveillance*, pelo Estado e por agentes privados do mercado, à proteção de direitos fundamentais – mais especificamente, aos direitos à privacidade e à proteção de dados pessoais. Metodologicamente, trata-se de pesquisa exploratória realizada por meio de levantamento bibliográfico e jornalístico, cujo escopo, de forma geral, propõe-se a compreender de que maneiras as novas tecnologias de vigilância afetam aquilo que se compreende por "vida privada". Buscar-se-á discutir a conceituação e evolução do direito à privacidade na chamada "sociedade da vigilância", analisar e entender o funcionamento dessas tecnologias e, por fim, debater a influência e as implicações que o advento das novas tecnologias, em especial, aquelas relacionadas a sistemas de reconhecimento facial, exerce sobre os direitos fundamentais à privacidade e à proteção de dados pessoais.

Palavras-chave: privacidade; proteção de dados pessoais; *surveillance*; tecnologia do reconhecimento facial; violação a direitos fundamentais.

SUMÁRIO

INTRODUÇÃO

A presente monografia tem como objetivo propor uma análise acerca da proteção dos direitos fundamentais – em especial, aqueles relacionados ao tema da privacidade – sob a perspectiva da utilização de equipamentos de alta tecnologia dotados do recurso do reconhecimento facial em políticas de vigilância, visando a demonstrar que esses meios tecnológicos de vigilância são permeados por vieses preconceituosos, já que manipulados por operadores humanos, suscetíveis a essas preconcepções, em paralelo à concepção generalizada de que é necessário aprofundar a vigilância sobre os indivíduos em nome do bem maior promovido pela sensação de segurança.

A popularização da internet e a consequente dinamização das relações interpessoais na sociedade trouxeram consigo algumas questões, principalmente no tocante à proteção dos dados pessoais. O desenvolvimento tecnológico, apesar do seu lado positivo, permite uma maior vulnerabilidade dos sujeitos na medida em que há, nas plataformas digitais, uma constante exposição pública – cenário este que evidencia a necessidade de um fortalecimento da tutela dos direitos à privacidade e à proteção dos dados pessoais.

Novas tecnologias de vigilância estão sendo rapidamente inseridas no cotidiano das pessoas sem a devida avaliação dos seus efeitos nas relações de poder na sociedade. Uma das tecnologias que vem sendo cada vez mais implementada como mecanismo para a realização desse monitoramento é o reconhecimento facial, que, no Brasil, começou a ser agregada aos sistemas de *surveillance* por gestores públicos por volta do ano de 2019.

Ocorre que a tecnologia pode ser implementada de modo a favorecer que determinados grupos de indivíduos estabeleçam certo controle sobre outros grupos. Nessa disputa, os direitos à privacidade e à proteção de dados pessoais acabam sendo atropelados, em vista à máxima de que conhecimento é poder e ao fato de que aqueles que têm acesso e podem armazenar dados alheios angariam considerável vantagem. Esse desnível de poder, conforme será demonstrado, aumenta o risco de persuasão, chantagem e outros usos danosos de informações pessoais sensíveis por terceiros, com o propósito de dominação, discriminação, violência e coerção.

Com efeito, os sistemas de vigilância baseados em reconhecimento facial têm seus algoritmos de funcionamento configurados por um programador humano, este que é suscetível a vieses e preconcepções. Ao serem transferidos esses vieses ao modo de funcionar dos sistemas de reconhecimento facial, dá-se ensejo aos efeitos nocivos da tecnologia aos direitos fundamentais, já que a automaticidade da operação eleva o potencial discriminatório a níveis estratosféricos.

Ainda que os algoritmos para busca e cruzamento de dados não sejam elaborados para reproduzir discriminação, os dados inseridos neles são enviesados, o que pode resultar, por exemplo, em uma tecnologia de reconhecimento facial racista e sexista. Exatamente nesse sentido, diversos estudos confiáveis vêm demonstrando as altas taxas de erro apresentadas pelos mais variados sistemas de reconhecimento facial existentes – taxas essas que são consideravelmente mais expressivas com relação, principalmente, a mulheres negras.

Dessa forma, a problemática a ser abordada neste trabalho de conclusão de curso consubstancia-se, exatamente, nos limites que devem pautar o uso da tecnologia do reconhecimento facial como ferramenta de *surveillance* de modo a serem resguardados os direitos e garantias fundamentais inerentes aos sujeitos – mais especificamente, os direitos à privacidade e à proteção dos dados pessoais.

Assim, a hipótese que se buscou defender vai no sentido da necessidade de alcançar um equilíbrio entre os direitos supramencionados e a coleta e tratamento de dados pessoais dos indivíduos pelo Estado e por agentes privados do mercado que, por vezes faz-se necessária para que sejam satisfeitas demandas sociais pelas mencionadas instituições. Para a escolha do recorte relacionado especificamente à implementação da tecnologia do reconhecimento facial, levou-se em consideração que a impressão facial é um tipo de dado biométrico, cuja natureza vulnerável ensejou, inclusive, a sua classificação pela Lei Geral de Proteção de Dados (LGPD) como “dado pessoal sensível.

Para esse fim, a presente monografia se divide em quatro capítulos. O primeiro deles tem como objetivo trazer a evolução do conceito de privacidade, demonstrando a sua íntima conexão

com a evolução tecnológica. Nessa esteira, apresenta-se a definição de *surveillance* que – considerada, de forma simplista, como o monitoramento rotineiro, sistemático e contínuo dos comportamentos dos indivíduos para fins de influência, administração ou proteção, que pode e tem sido realizado por meios tecnológicos – é responsável por moldar as alterações no conceito de privacidade ao longo do tempo.

Outrossim, no segundo capítulo, a presente monografia buscou elucidar o histórico da proteção legal ao direito à privacidade e à proteção dos dados pessoais no Brasil, culminando a análise na apresentação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD), um marco normativo indispensável à integração dos sujeitos de direito à economia digital, o qual, pela primeira vez, trouxe os dados biométricos, como a impressão facial capturada pelos sistemas de reconhecimento facial, como dados pessoais sensíveis, conferindo-lhes proteção diferenciada.

Nessa esteira, o terceiro capítulo falará especificamente sobre a tecnologia do reconhecimento facial, buscando trazer explicações acerca do seu mecanismo de funcionamento que são essenciais à compreensão de como sistemas de reconhecimento facial podem ser empregados, ainda que não intencionalmente, como ferramenta capaz de ensejar violações a direitos fundamentais.

Finalmente, o quarto capítulo tem como finalidade traçar um paralelo exatamente entre a proteção aos direitos à privacidade e à proteção de dados pessoais ante à disseminação do uso de sistemas de reconhecimento facial como ferramenta de *surveillance* pelo Estado e por instituições privadas, indicando seus potenciais lesivos a direitos fundamentais e externalidades negativas. Para isso, em subcapítulo, foi realizado levantamento jornalístico visando a enriquecer o presente trabalho com exemplos de casos concretos em que o uso da tecnologia do reconhecimento facial, seja como ferramenta de *surveillance* ou não, apresentou resultados problemáticos e preocupantes.

O recurso metodológico em que se pauta este trabalho, em vista à natureza do tema abordado, será, no que tange aos seus objetivos, a pesquisa exploratória com estudo bibliográfico e de casos específicos de natureza jornalística. A partir da escolha da metodologia descrita,

pretende-se ver demonstrado que o ordenamento jurídico deve se amoldar ao novo perfil de privacidade verificado em uma sociedade que muda com velocidade, em decorrência da evolução tecnológica, sendo imprescindível um aumento da participação e influência dos sujeitos de direito no manejo das informações que lhes dizem respeito – implemento do denominado "direito de acesso" –, para o que é extremamente necessário que se confira transparência à coleta e ao tratamento de dados pessoais obtidos como fruto de atividades de vigilância. Afinal, assim, será possível que os indivíduos possam reivindicar os seus direitos e sejam ouvidos pela administração pública, que, a seu turno, seguirá trabalhando e se amoldando ao progresso natural impulsionado pelo desenvolvimento de novas tecnologias.

1. ENTRE A PRIVACIDADE E A VIGILÂNCIA

Parte-se, para a compreensão da problemática a ser abordada neste trabalho, da ideia de privacidade, cuja origem, segundo Danilo Doneda[1], remete ao "o direito de estar só"[2]. De acordo com o conceito desenvolvido por Warren e Brandeis, cuja característica marcante é o individualismo exacerbado, quase egoístico, algumas atividades poderiam ser exercidas na esfera pública, enquanto outras deveriam se restringir à esfera individual dos sujeitos. Nas palavras de Doneda, "[e]sta concepção foi o marco inicial; a temperá-la, posteriormente, temos a crescente consciência de que a privacidade é um aspecto fundamental da realização da pessoa e do desenvolvimento da sua personalidade"[3].

A este período, remonta o paradigma da privacidade como uma *zero-relashionship*: a ausência de comunicação entre um sujeito e os demais[4]. O conceito vem, no entanto, sofrendo modificações ao longo do tempo, e a sua evolução, conforme será visto em maior nível de detalhe ao longo deste trabalho, está intrinsecamente conectada ao desenvolvimento das tecnologias da informação, cujos aprimoramento e expansão proporcionaram a criação de um ambiente propício aos debates sobre a proteção ao direito das pessoas a suas vidas privadas.

Nessa esteira, essa concepção essencialmente individualista do conceito de privacidade vem perdendo espaço para uma noção que transcende a ideia simplória do "ser deixado em paz" e compreende o efetivo controle dos indivíduos sobre suas informações pessoais. Essa nova compreensão ultrapassa a liberdade negativa do sujeito em decidir os aspectos de sua vida que estarão contidos em sua esfera privada[5], englobando o "direito do indivíduo de escolher aquilo que está disposto a revelar aos outros"[6]. Caminhou-se, portanto, da sequência "pessoa-informação-sigilo" para "pessoa-informação-circulação-controle"[7].

---

[1] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 6.
[2] WARREN, S. D.; BRANDEIS, L. D. The right to privacy. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890, p. 205.
[3] DONEDA, D. *Op. cit.*, p. 6.
[4] DONEDA D. *Op. cit.*, p. 6.
[5] RODOTÀ, S. Il diritto di avere diritti. Roma: Laterza, 2012, p. 320.
[6] RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 74.
[7] *Ibid*., p. 93.

Nesse sentido, ainda que o sujeito opte por compartilhar acontecimentos de sua vida íntima com terceiros, em maior ou menor número, estará, de todo modo, exercendo o seu direito fundamental à privacidade, na medida em que este se trata, sob essa perspectiva, da possibilidade de o indivíduo controlar o acesso às suas informações, restringindo-as do público em geral e disponibilizando-as para um grupo específico de pessoas, selecionadas ao seu critério. Trata-se da faculdade que se dispõe ao indivíduo em manejar o uso que aqueles que terão acesso à sua esfera privada farão das informações que lhe dizem respeito.

As modificações narradas surgem essencialmente como resultado das novas dinâmicas associadas à informação e ao expressivo crescimento do fluxo de dados possibilitado pelo desenvolvimento tecnológico – que proporcionou um aumento na capacidade técnica de coleta, tratamento e transmissão de dados. Esse cenário conferiu grande importância à informação, de modo a se poder considerá-la como elemento nuclear para o desenvolvimento humano, responsável pela configuração de uma nova forma de organização social escorada nesses mecanismos capazes de processar e compartilhar informações cada vez mais rapidamente, em função da evolução tecnológica[8].

Nesse cenário, protagonistas das sociedades modernas em que conhecimento é poder, a informação e, em específico, os dados pessoais passam a representar verdadeiros "vetores das vidas e das liberdades individuais, assim como da sociedade e da própria democracia"[9]. E a importância da informação vai aumentando exponencialmente na medida em que a evolução tecnológica possibilita sua transformação em uma utilidade, a um custo razoável[10]. Sobre o tópico, confira-se o que expõe a renomada jurista Ana Frazão:

> Vistos já como o novo petróleo, os dados são hoje insumos essenciais para praticamente todas as atividades econômicas e tornaram-se, eles próprios, objeto de crescente e pujante mercado. Não é sem razão que se cunhou a expressão *data-driven economy*, ou seja, economia movida a dados, para designar o fato de que, como aponta Nick Srnicek,

[8] BIONI, B. R. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 4.
[9] FRAZÃO, A. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1.ed. São Paulo: Thomson Reuters, 2019, p. 24.
[10] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 8.

> o capitalismo do século XXI passou a centrar-se na extração e no uso de dados pessoais.[11]

Nesse sentido, as novas tecnologias são as responsáveis por delinear o entrelace entre privacidade e informação pessoal. Sem perder de vista a ideia de que, desde que o mundo é mundo, conhecimento é poder, a evolução tecnológica, ao possibilitar a intensificação dos fluxos de informação, ensejou alterações na distribuição de poder na sociedade, "mudando os eixos de equilíbrio na equação entre poder – informação – pessoa – controle"[12]. Assim, ao contrário do "direito de estar só", o direito à proteção de dados pessoais é guiado pela liberdade positiva de se efetivamente controlar a informação de que lhe diz respeito, independentemente dessa informação ser pública ou privada – e, nessa medida, diferencia-se do direito à privacidade, já que este é direito essencialmente negativo vinculado ao binômio público-privado[13].

Dessa vinculação do conceito de proteção de dados pessoais a uma lógica social surge o conceito de privacidade conforme concebido nos dias de hoje, na medida em que este se manifesta principal e justamente através do resguardo das informações particulares dos indivíduos. Nesse sentido, a privacidade

> deixa de dar vazão somente a um imperativo de ordem individualista, mas passa a ser a frente onde irão atuar vários interesses ligados à personalidade e às liberdades fundamentais da pessoa humana, fazendo com que na disciplina da privacidade passe a se definir todo um estatuto que perpassa as relações da própria personalidade com o mundo exterior.[14]

Tem-se, assim, que o resguardo da privacidade na sociedade da informação, concebida na forma da proteção aos dados pessoais, torna-se ferramenta para proporcionar aos indivíduos os meios necessários ao desenvolvimento de suas esferas privadas – mas dentro da lógica social, afastando-se das concepções de mero isolamento ou tranquilidade[15]. Até mesmo porque o

---

[11] FRAZÃO, A. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.).. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1.ed. São Paulo: Thomson Reuters, 2019, p. 24.
[12] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 10.
[13] BIONI, B. R. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 98 e 99.
[14] DONEDA, D. *Op. cit.*, p. 21.
[15] DONEDA, D. *Op. cit.*, p. 17.

advento das novas tecnologias relacionadas, por exemplo, à captura de imagens e áudio, juntamente à possibilidade de conexão interpessoal a nível global e a qualquer momento, tornaram tênues as divisórias entre o que se tem por esfera particular e, de outro lado, o que integra a vida pública.

Nesse fio, naturalmente, governos e instituições privadas no mundo todo começaram a se aparelhar com equipamentos de alta tecnologia para o monitoramento desse alto fluxo de informação, o que se justifica por dois fatores primordiais: o controle e a eficiência[16]. E exemplos do emprego dessas tecnologias são cada vez mais comuns, sendo possível indicar, inclusive, o surgimento de "uma tendência que já parece irresistível, comum aos mais diversos países"[17].

Concomitantemente ao desenvolvimento das novas tecnologias no campo das comunicações – e, muito provavelmente, em função delas – foram verificadas mudanças substanciais nas noções de democracia e da proteção aos direitos fundamentais. Em uma conjuntura de crescimento populacional em áreas urbanas, que inevitavelmente implica em uma maior demanda pela atuação do Estado, verificou-se uma modificação na própria estrutura da administração pública, que passou a assumir um maior número de funções e demandas de maior complexidade. Esse fato ensejou a implementação, não apenas no Brasil, mas no mundo, de sistemas automatizados para a realização de atividades e serviços públicos, inclusive aqueles relacionados à vigilância e ao controle social[18].

A essa vigilância, atribui-se a definição de *surveillance*, cujo conceito popularizou-se nos anos 1980 como "*the systematic investigation or monitoring of the actions or communications of one or more persons*"[19]. Esse conceito eventualmente se tornou obsoleto, na medida em que a *surveillance* passou a ser implementada, na sociedade moderna, para muito além do mero monitoramento de ações e comunicações, mas enquanto, verdadeiramente, a "*focused, systematic*

[16] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 9.
[17] RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 147.
[18] EGGERS, W.; SCHATSKY, D.; VIECHNICKI, P. AI-augmented government: Using cognitive technologies to redesign public sector work. [S.l], 2017. Disponível em <https://www2.deloitte.com/insights/us/en/focus/cognitive-technologies/artificial-intelligence-government.html>. Acesso em 9 de set. de 2021.
[19] "[A] investigação ou monitorização sistemática das ações ou comunicações de uma ou mais pessoas" (Tradução livre). (CLARKE, R. A.. Information Technology and Dataveillance. Communications of the ACM 31, 1988, p. 498. Disponível em <http://www.rogerclarke.com/DV/CACM88.html>. Acesso em 07 de maio de 2021).

and routine attention to personal details for purposes of influence, management, protection or direction"[20]. Em comentário a esta concepção, desenvolvida por David Lyon, disserta Neil Richards:

> *Four aspects of this definition are noteworthy, as they expand our understanding of what surveillance is and what its purposes are. First, it is focused on learning information about individuals. Second, surveillance is systematic; it is intentional rather than random or arbitrary. Third, surveillance is routine — a part of the ordinary administrative apparatus that characterizes modern societies. Fourth, surveillance can have a wide variety of purposes — rarely totalitarian domination, but more typically subtler forms of influence or control*.[21]

Trata-se do monitoramento dos indivíduos que, em função das novas infraestruturas e barateamento da tecnologia da informação, é realizado rotineiramente, estabelecendo-se não apenas como resultado de uma atividade estatal ou encabeçada por entidades privadas, mas como um fruto do comportamento das próprias pessoas, que participam do processo disponibilizando suas informações pessoais nas redes.

Nesse esteio, a *surveillance* possibilitada pelas novas tecnologias de vigilância afastou-se de suas origens geralmente relacionadas ao modelo arquitetônico carcerário do Panóptico, de Jeremy Bentham. Este modelo – consubstanciado numa construção em formato de círculo, na qual, ao centro, posicionava-se estrategicamente um observatório de onde se podia ver todas as celas ocupadas pelos prisioneiros, sem que estes pudessem saber, no entanto, se estavam ou não sendo, de fato, observados – fora projetado para coordenar uma observação presencial e direta com o objetivo de "induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder" que "[g]raças a seus mecanismos de observação,

[20] "[A] atenção focalizada, sistemática e rotineira a detalhes pessoais para efeitos de influência, gestão, proteção ou direcionamento" (Tradução livre). (LYON, D. Surveillance studies: an overwiew, Cambridge: Polity, 2007, p. 14).

[21] "Quatro aspectos desta definição são dignos de nota, pois expandem a nossa compreensão do que é a vigilância e quais são os seus objetivos. Primeiro, concentra-se na aprendizagem de informação sobre indivíduos. Em segundo lugar, a vigilância é sistemática; é intencional e não aleatória ou arbitrária. Terceiro, a vigilância é rotineira - uma parte do aparelho administrativo ordinário que caracteriza as sociedades modernas. Quarto, a vigilância pode ter uma grande variedade de propósitos - raramente dominação totalitária, mas mais tipicamente formas mais sutis de influência ou controle." (Tradução livre). (RICHARDS, N. M.. The dangers of surveillance. 126 HARV. L. REV. 1934, 1935, 2013, p. 1935. Disponível em: <https://harvardlawreview.org/wpcontent/uploads/pdfs/vol126_richards.pdf>. Acesso em: 07 de maio de 2021).

ganha em eficácia e em capacidade de penetração no comportamento dos homens"[22]. Nas palavras de Foucault:

> O Panóptico de Bentham é a figura arquitetural dessa composição. O princípio é conhecido: na periferia uma construção em anel; no centro, uma torre; esta é vazada de largas janelas que se abrem sobre a face interna do anel; a construção periférica é dividida em celas, cada uma atravessando toda a espessura da construção; elas têm duas janelas, uma para o interior, correspondendo às janelas da torre; outra, que dá para o exterior, permite que a luz atravesse a cela de lado a lado. Basta então colocar um vigia na torre central, e em cada cela trancar um louco, um doente, um condenado, um operário ou um escolar. Pelo efeito da contraluz, pode-se perceber da torre, recortando-se exatamente sobre a claridade, as pequenas silhuetas cativas nas celas da periferia. Tantas jaulas, tantos pequenos teatros, em que cada ator está sozinho, perfeitamente individualizado e constantemente visível. O dispositivo panóptico organiza unidades espaciais que permitem ver sem parar e reconhecer imediatamente. Em suma, o princípio da masmorra é invertido; ou antes, de suas três funções — trancar, privar de luz e esconder — só se conserva a primeira e suprimem-se as outras duas. A plena luz e o olhar de um vigia captam melhor que a sombra, que finalmente protegia. A visibilidade é uma armadilha. [...]
> Cada um, em seu lugar, está bem trancado em sua cela de onde é visto de frente pelo vigia; mas os muros laterais impedem que entre em contato com seus companheiros. É visto, mas não vê; objeto de uma informação, nunca sujeito numa comunicação. A disposição de seu quarto, em frente da torre central, lhe impõe uma visibilidade axial; mas as divisões do anel, essas celas bem separadas, implicam uma invisibilidade lateral. E esta é a garantia da ordem.[23]

Em tempos de evolução tecnológica, no entanto, a observação ostensiva realizada em estrutura física conforme prevê o modelo de Bentham é substituída pelo emprego de sistemas informatizados nas atividades de monitoramento. A vigilância passa a ser empreendida à distância e de modo velado, assentando-se sobre aparente ausência de controle. Rodotà, sobre o ponto, traça um paralelo com relação à mudança do paradigma tecnológico: "[a]s velhas tecnologias tinham esta vantagem. Eram visíveis, volumosas, rumorosas. Impunham-se com tal materialidade que todos eram constritos a sentir seu peso e, quando pareciam intoleráveis, bastava pedir a alguém para que as suprimisse"[24].

Notadamente, quanto mais visibilidade se dá aos mecanismos de observação, maior é a resistência por parte dos observados; ao passo que, quanto mais camuflado, maior a espontaneidade das ações dos indivíduos e maior, inclusive, a sua sensação de segurança no

[22] FOUCAULT, M. Vigiar e punir: nascimento da prisão. Petrópolis: Vozes, 27ª ed., 1987, p. 228.
[23] FOUCAULT, M. Vigiar e punir: nascimento da prisão. Petrópolis: Vozes, 27ª ed., 1987, p. 223/224..
[24] RODOTÀ, S. "Un Codice per l'Europa? Diritti nazionali, diritto europeo, diritto globale", in: Codici. 56 Una riflessioni di fine millennio. Paolo Cappellini. Bernardo Sordi (orgs.). Milano: Giuffrè, 2002, p. 564.

compartilhamento dos seus próprios dados – de modo a que contribuam com o maquinário da *surveillance*. Essa vigilância deixa, portanto, de ser um evento específico e direcionado para constituir-se enquanto característica das sociedades contemporâneas, um fenômeno cotidiano e onipresente que ultrapassa a esfera privada dos indivíduos, na medida em que é realizado, inclusive, em espaços públicos.

Nessa linha, com a convergência do desenvolvimento das tecnologias no campo das comunicações e o aumento do fluxo de informação tendo como denominador comum o meio digital, verifica-se um interessante fenômeno: "uma parte do que era antes considerado uma vigilância física, bem como psicológica, deverá passar a ser tratado como forma de vigilância sobre dados pessoais"[25]. Seguindo essa mesma lógica, Rodotà discorre sobre como a expansão da Internet, em paralelo à crescente e incisiva coleta de dados pessoais dos indivíduos, somada à fácil disponibilidade e interconexão entre diversos bancos de dados que possibilitam a agregação de informações, promovem uma sociedade da vigilância e classificação[26].

Dito isso, fato é que estamos a viver na era da vigilância. Conforme afirma Richards, as mesmas tecnologias inovadoras que nos trouxeram inúmeras facilidades e revolucionaram nossas vidas diárias são também responsáveis por criar registros cada vez mais detalhados sobre essas vidas[27]. Sobre o tópico, o estudioso aduz, ainda, que "[t]*he escope and variety of the types of surveillance that are possible today are unprecedent in human history. This fact alone should give us pause*."[28]. Nesse mesmo sentido, já no início da década de 1970, Westin apontou que existiriam três espécies de ameaças à privacidade de natureza tecnológica: a vigilância física (através de microfones, etc), a vigilância psicológica e a vigilância de dados pessoais[29].

[25] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 17.
[26] RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 146.
[27] RICHARDS, N. M. The dangers of surveillance. 126 HARV. L. REV. 1934, 1935, 2013, p. 1934. Disponível em: <https://harvardlawreview.org/wpcontent/uploads/pdfs/vol126_richards.pdf>. Acesso em: 07 de maio de 2021.
[28] [O] alcance e a variedade dos tipos de vigilância que são possíveis hoje em dia não têm precedentes na história da humanidade. Este fato, só por si, deveria nos provocar uma pausa." (Tradução livre). (RICHARDS, N. M. The dangers of surveillance. 126 HARV. L. REV. 1934, 1935, 2013, p. 1934. Disponível em: <https://harvardlawreview.org/wpcontent/uploads/pdfs/vol126_richards.pdf>. Acesso em: 07 de maio de 2021).
[29] WESTIN, Alan. Privacy and Freedom. Estados Unidos: Ig Publishing, 2015, p. 65-168.

A implementação ostensiva do *surveillance* na sociedade contemporânea é motivo de preocupação na medida em que "os riscos da sociedade de vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos"[30]. Nesse sentido, Doneda explica que essa coleta maciça de informação, além de ser de grande utilidade à administração pública, funciona como ferramenta ao controle social:

> 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 – não é por outro motivo que um forte controle da informação é característica comum aos regimes totalitários.[31]

Sobre o tópico, destaca Ana Frazão que "o ponto de partida de toda essa engrenagem é a coleta de dados, cada vez mais maciça e muitas vezes realizada sem o consentimento e até sem a ciência dos titulares desses dados", de modo que, "se os cidadãos não conseguem saber nem mesmo os dados que são coletados, têm dificuldades ainda maiores para compreender as inúmeras destinações que a eles pode ser dada e a extensão do impacto destas em suas vidas"[32].

Como resultado, o que se têm é uma profunda alteração nas dinâmicas de poder entre quem vigia e quem é vigiado, aumentando o risco de persuasão, chantagem e outros usos danosos de informações pessoais sensíveis por terceiros[33]. Isso porque governos e agentes econômicos privados têm se utilizado dos dados pessoais para a criação do que denominou "*one-way mirror*" (em português, um espelho unidirecional), por meio do qual acessam tudo que há para saber

[30] RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 113.
[31] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 9.
[32] FRAZÃO, A. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1.ed. São Paulo: Thomson Reuters, 2019, p. 23-52.
[33] RICHARDS, N. M. The dangers of surveillance. 126 HARV. L. REV. 1934, 1935, 2013, p. 1945. Disponível em: <https://harvardlawreview.org/wpcontent/uploads/pdfs/vol126_richards.pdf>. Acesso em: 07 de maio 2021.

acerca dos cidadãos, enquanto estes ficam no escuro[34] – dinâmica que confere ao observador enorme poder para direcionar o objeto da *surveillance*.

Destaque-se o que argumenta Schneier, para quem a *surveillance*, essa forma de vigilância pautada no desequilíbrio de poder em favor do governo e dos grandes *players* do mercado, espraia-se facilmente porque é feita – graças ao desenvolvimento tecnológico e barateamento dos equipamentos de monitoramento – em massa, de forma pouco custosa, escondida, automática e ubíqua[35]. É nesse contexto em que despontam preocupações no que se refere à proteção dos direitos à privacidade e à proteção dos dados dos indivíduos.

Inicialmente associados a construções como o "*Big Brother*" de Orwell, os perigos e horrores dessa nova modalidade de *surveillance* estatal, caracterizada pela substituição dos olhos de observadores humanos por lentes de câmeras e microfones – no caso da obra, as "teletelas" – vêm despertando atenção. Esse modelo incisivo de realização da *surveillance* é, razoavelmente, interpretado como uma ameaça a direitos fundamentais, incluindo os direitos à privacidade e à proteção dos dados pessoais. Como destaca Doneda,

> [n]otícias sobre 'o fim da privacidade' ou sobre a formação de uma 'sociedade de dossiers' chamaram atenção para novos problemas e situações, porém por vezes vêm acompanhadas de uma tendência para o fantástico, não raro chegando a sobrevalorizar o papel da tecnologia em um mundo no qual, felizmente, o arsenal de controles democráticos ainda não foi exaurido, e eventualmente dá sinais de renovar-se.[36]

Ocorre que essa superexposição da temática acaba sendo simplista, revelando sinais de incompreensão sobre o assunto. Isso porque não se sabe ao certo a real extensão e como efetivamente se dá o emprego das novas tecnologias em prol da *surveillance*, o que se justifica pelo seu caráter essencialmente velado e "por de baixo dos panos" – "sabê-lo pode não ser de grande ajuda, frente à escassez de meios para controlá-las"[37]. Nesse sentido, é possível afirmar que os sujeitos estejam partindo do pressuposto de que abrir mão de determinados níveis de sua

[34] PASQUALE, F. The black box society. The secret algorithms that control money and information. Cambridge: Harvard University Press, 2015, p. 9.
[35] SCHNEIER, B. Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Notton & Company, 2015, p. 57.
[36] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 12.

privacidade seria uma consequência natural da evolução social, ante ao advento das novas tecnologias no campo das comunicações[38].

Parece-se ter alcançado um ponto chave à delimitação dos limites do alcance e abrangência do uso dessas ferramentas dotadas de tecnologia de ponta como forma de realização da *surveillance*, de modo a que coexistam com o respeito e a proteção aos direitos fundamentais dos sujeitos, para o que "tanto o sustento quanto a recusa incondicionados das novas tecnologias deixaram de ser proponíveis"[39]. Nesse sentido, Danilo Doneda sustenta que o "centro de gravidade da privacidade tem se reposicionado decisivamente em função da multiplicidade de interesses envolvidos e da sua importância na tutela da pessoa humana"[40].

Com efeito, é possível a realização da *surveillance* de forma neutra, consubstanciada no simples acúmulo de dados sobre os cidadãos. Um exemplo disso é a mencionada realização periódica de censos, visando a possibilitar a regulação do funcionamento dos serviços públicos oferecidos pelos entes estatais. O modelo neutro diferencia-se do modelo de *surveillance* prejudicial aos sujeitos, este que desloca desproporcionalmente as dinâmicas de poder na sociedade na medida em que é pautado no acúmulo indiscriminado, velado e desregulado de informações sobre os indivíduos com o propósito de dominação, discriminação, violência e coerção do dominador – podendo este ser o próprio Estado ou agentes privados do mercado – sobre a sociedade, refém. Destaque-se, nesse ponto, a noção foucaultiana de vigilância, segundo a qual esta seria inerentemente coercitiva e dominadora[41].

Assim, tratar-se-ia a vigilância negativa do acúmulo e processamento de dados de indivíduos para que aquele que detenha a posse dessas informações encontre-se em posição de ameaçar comportamentos indesejados visando a moldá-los ao seu bel prazer. Nesse sentido, destaca Christian Fuchs a necessidade de que se diferencie qualquer recuperação de informações, o que seria natural à sociedade da informação, dos padrões desiguais de poder provocados por uma prática negativa da *surveillance*, o que, a seu turno, configuraria a sociedade da vigilância. O

[38] *Ibid.*, p. 14.
[39] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 15.
[40] *Ibid.*, p. 16.
[41] FUCHS, Christian. Como podemos definir vigilância?. MATRIZES, v. 5, n. 1, 2011, p. 117.

resultado é o fomento de uma economia de vigilância fundamentada em verdadeiro varejo de dados pessoais[42] – situação que abre precedente para a ocorrência de uma série de violações a direitos fundamentais.

[42] BIONI, B. R.. Proteção de dados pessoais: a função e os limites do consentimento**.** Rio de Janeiro: Forense, 2019, p. 42.

2. HISTÓRICO DA PROTEÇÃO LEGAL AO DIREITO À PRIVACIDADE E À PROTEÇÃO AOS DADOS PESSOAIS

Sabe-se que a privacidade começou a se fazer notar pelo ordenamento jurídico somente no final do século XIX, tendo assumido suas feições atuais nas últimas décadas – trata-se de um debate recente. As atenções voltaram-se à proteção direito à privacidade e à proteção de dados pessoais no momento em que se tomou consciência a respeito do papel da tecnologia e a forma como a sua utilização em larga escala influenciam diretamente no exercício das liberdades fundamentais dos indivíduos e no gozo dos seus direitos fundamentais.

Sendo assim, importa verificar como o desenvolvimento tecnológico age sobre a sociedade e os efeitos que produz sobre o ordenamento jurídico, devendo-se considerar, para isso, o potencial das novas tecnologias, principalmente relacionadas ao campo das comunicações, para imprimir suas próprias características no meio sobre o qual se projetam[43]. Isso porque, em uma sociedade digital, o tratamento dos dados pessoais é cada vez mais expansivo, alcançando um número relevante de pessoas e diferentes realidades sociais.

Todo esse contexto fez emergir a necessidade de desenvolvimento de um sistema de proteção legal de dados que realmente colocasse o titular do direito a essa proteção como participante no processo do tratamento dos seus próprios dados, em vista à sua (hiper)vulnerabilidade, consentindo ou não com os procedimentos aos quais sua informação é submetida.

Nesse contexto, a proteção de dados pessoais consubstancia-se enquanto a tutela da "própria dimensão relacional da pessoa humana"[44], na medida em que resguarda uma série de liberdades individuais que se relacionam à proteção de dados pessoais e são exercidas em sociedade. Rememore-se que a resguarda dos dados pessoais dos indivíduos extrapola os limites de tutela do direito à privacidade, já que, conforme anteriormente exposto neste trabalho, não é atrelada a uma divisão entre as esferas pública e privada de seus titulares.

[43] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 11.
[44] BIONI, B. R.. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 99.

Assim, tem-se que a expansão da compreensão daquilo que se deve buscar tutelar com o objetivo de resguardar as vidas privadas dos sujeitos foi e é acompanhada da evolução do tratamento da privacidade pelo ordenamento jurídico, podendo-se indicar como ponto de partida a sua caracterização como direito fundamental. Este desdobramento decorreu, sobretudo, da forma com que o tema foi abordado na Carta dos Direitos Fundamentais da União Europeia, cujos artigos 7º e 8º trazem, respectivamente, o direito ao "respeito pela vida familiar e privada" e o direito à "proteção dos dados pessoais".

Nota-se que a carta bem traduz a complexidade dos interesses ligados à proteção da esfera privada dos indivíduos, seja esta considerada enquanto uma concepção individualista, sendo resguardada de intromissões exteriores (art. 7º), ou mesmo concebida dentro de uma dinâmica social, por meio da qual tutela-se os dados pessoais em suas diversas modalidades (art. 8º), sem perder de vista, no entanto, o foco da proteção: a dignidade do ser humano.

Seguindo esse fio, de acordo com a visão de Mayer-Scönberger, a regulamentação da proteção de dados pessoais percorreu quatro gerações distintas, que, de acordo com Danilo Doneda, são "leis que partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais"[45].

A primeira das gerações de leis surgiu a partir da década de 70 como reação imediata ao acúmulo, união, processamento e manutenção de dados pessoais dos indivíduos, pelo Estado e por empresas privadas, em grandes bancos centralizados. Segundo Doneda,

> [o] núcleo dessas leis girava em torno da concessão de autorizações para a criação desses bancos de dados e do seu controle a posteriori por órgãos públicos. Essas leis também enfatizavam o controle do uso de informações pessoais pelo Estado e pelas suas

[45] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. Espaço Jurídico. Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 96. Disponível em <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em 9 de setembro de 2021.

> estruturas administrativas, que eram o destinatário principal (quando não o único) dessas normas.[46]

Assim, pode-se indicar como característica marcante dessa primeira geração de leis, que não previa mecanismos de proteção à dignidade individual e privada, a descrição dos procedimentos a serem adotados pelos bancos de dados em prol da proteção dos dados pessoais, tendo o Estado como destinatário dos regulamentos direcionados à tecnologia. Alguns exemplos são as Leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973) e o *Privacy Act* dos Estados Unidos da América (1974).

A rápida multiplicação e descentralização dos bancos de dados acessados pelo Estado e pelos agentes privados do mercado, além de ter escancarado a deficiência das normas da primeira geração em não provisionarem formas de proteção à dignidade individual e privada dos sujeitos, tornou obsoletas as normas procedimentais que se prestavam a regular o funcionamento dos bancos de dados centrais, fato que ensejou o surgimento da segunda geração de normas.

Esta surgiu com o objetivo de garantir aos indivíduos, mediante a figura do consentimento, um maior controle sobre seus próprios dados, garantindo-se uma maior participação no processo do tratamento desses dados nas fases da sua coleta, uso e compartilhamento[47]. Entretanto, a exigência do consentimento dos titulares dos dados, por vezes, não surtia, na prática, os efeitos esperados, a depender da forma como era obtida, o que acabou por criar situações em que posta em xeque a possibilidade de reparação por eventual violação ao direito à privacidade.

A terceira geração de leis surgiu, assim, preocupada com a tutela do direito à privacidade, indo além de conferir aos sujeitos a liberdade de optar por ceder ou não seus dados, focando em garantir a efetividade desse direito – ou seja, foram endereçados alguns dos pontos fracos das leis da segunda geração. Há, aqui, a introdução do conceito da autodeterminação informativa, que busca aproximar o titular dos dados do controle da sua proteção a partir do requerimento do seu consentimento e da garantia da sua participação no processamento, desde a fase da coleta dos dados, até o seu armazenamento. Nas palavras de Doneda:

---

[46] *Ibid.*, p. 96.
[47] BIONI, B. (org.). Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021, p. 66.

> A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes proporcionando o efetivo exercício da autodeterminação informativa.[48]

A ampliação da participação dos titulares dos dados no seu processamento exigia deles, no entanto, uma árdua dedicação no sentido de acompanhar e controlar o fluxo e o uso das suas informações, principalmente levando-se em conta a descentralização dos bancos de dados e servidores, que atrapalha a identificação do local de armazenamento dos dados.

Tendo isso em vista, deu-se início à quarta e atual geração de leis, com o objetivo de superar as desvantagens do enfoque individual conferido pelas gerações anteriores e de fortalecer a política de compensação de danos causados por eventuais violações. Notadamente, as normas da quarta geração priorizam os titulares dos dados em relação a terceiros que realizem a manipulação das suas informações pessoais. O consentimento continua sendo o traço mais marcante dos regulamentos, mas passam a ser delineados limites e condições de forma de adequação à autonomia informativa dos titulares dos dados. Tem-se, portanto, uma transformação na concepção do consentimento, cuja manifestação passa a precisar ser "livre, informada e inequívoca", nos atuais termos do art. 5º, XII, da Lei Geral de Proteção de Dados, cujo conteúdo será analisado mais a fundo no próximo tópico deste trabalho.

No Brasil, o atual arcabouço legal para proteção da privacidade e de dados pessoais provém de uma combinação entre fundamentos constitucionais e normas ordinárias, que regulam relações especiais. Ainda que tacitamente, a proteção de dados começa a ser tratada como direito à personalidade, à liberdade de expressão e direito à informação a partir da Constituição Federal de 1988 (CF/88) (art. 5º, incisos IX e XIV). A Carta Magna garante, ainda, a inviolabilidade da vida privada e intimidade (art. 5º, X), o *habeas data* (art. 5º, LXXII) e a inviolabilidade do sigilo de dados e das comunicações telefônicas (Art. 5º, XII). A partir da definição desses princípios pela norma geral, o panorama das normas de proteção de dados pessoais passa a ser complementado por normas específicas setoriais.

[48] DONEDA, Danilo. op. cit., p. 97.

A partir da promulgação da CF/88, outras normas passaram a dispor sobre a proteção de dados, como o Código de Defesa do Consumidor (CDC), em 1990. Este, em seu art. 43, prevê que "[o] consumidor 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", garantindo-se a proteção do titular dos dados frente a bancos de dados. O código exige transparência, objetividade e verossimilitude ao cadastro desses dados, que deverão, ainda, ser dispostos em linguagem de fácil compreensão, devendo o consumidor ser informado sempre que um novo cadastro, ficha ou registro de seus dados pessoais forem realizados. Sobre o tópico, aduz Doneda que parte da doutrina elege o CDC como um "marco normativo dos princípios de proteção de dados pessoais" no Brasil[49].

A legislação consumerista, no entanto, preocupava-se essencialmente em regular os bancos de dados, visando a alcançar todo e qualquer acervo capaz de atingir o livre desenvolvimento da personalidade do consumidor[50], colocando para escanteio a questão da necessidade do consentimento. Nesse ponto, conforme argumentam Andrade e Moura, pode-se afirmar que a referida lei se aproxima mais da primeira geração das normas sobre dados pessoais:

> O presente artigo, entretanto, analisa a regra do CDC de forma mais crítica, pois se preocupa mais com a regulamentação dos Bancos de Dados do que com o consentimento prévio ao registro ou arquivamento dos mesmos (sic), estando mais próxima das normas de primeira geração do que as de terceira. Ademais, a suposta autodeterminação informacional do consumidor resta ainda mais fragilizada a partir da Súmula no 404, do STJ, que adverte: "É dispensável o aviso de recebimento (AR) na carta de comunicação ao consumidor sobre a negativação de seu nome em bancos de dados e cadastros.[51]

Seguindo a cronologia, houve, em 2011, a promulgação da Lei do Cadastro Positivo (Lei nº 12.414/11), que se propunha a regulamentar as bases de dados com informações e histórico de

[49] DONEDA, Danilo. A Proteção dos Dados Pessoais como um Direito Fundamental. Espaço Jurídico. Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 103. Disponível em <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em 9 de setembro de 2021.

[50] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019.

[51] ANDRADE, Diego de Calasans Melo; MOURA, Plínio Rebouças de. O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço. Revista de Direito, Governança e Novas Tecnologias, Goiânia, v. 5, n. 1, 2019, p. 110-133.

crédito dos consumidores, com o objetivo de facilitar a concessão de crédito por instituições financeiras[52]. A lei em referência foi responsável por introduzir ao ordenamento jurídico brasileiro o conceito da autodeterminação informativa, já que – ao contrário do CDC, que previa a obrigatoriedade da mera notificação do consumidor – trouxe o consentimento como elemento necessário à licitude do tratamento e compartilhamento de dados pessoais. Ademais, estabeleceu responsabilidades em caso de danos decorrentes do manuseio dos dados pessoais, trouxe previsão expressa do direito ao pedido de revisão, pelo consumidor, de qualquer decisão tomada por meio automatizado[53], além da proibição de armazenamento de dados pessoais sensíveis, referentes a etnia, informações genéticas, orientação sexual, política etc.

Naquele mesmo ano, surgiu a Lei de Acesso à Informação (Lei nº 12.527/11), que inovou ao trazer um arcabouço legal à proteção de dados pessoais manuseados por entes públicos. A norma limitou o acesso de terceiros aos dados de particulares, elencando expressamente as exceções possíveis. De acordo com o art. 31 do referido diploma legal, o tratamento de informações pessoais "deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais", associando, pois, a proteção dos dados pessoais à proteção do direito à privacidade e ao exercício das liberdades individuais.

Na sequência, deve-se mencionar o Marco Civil da Internet (Lei nº 12.965/14), que estabelece um conjunto de princípios, garantias, direitos e deveres dos usuários da Internet no Brasil. A regulamentação teve o seu trâmite legislativo acelerado, curiosamente, em razão do grande escândalo de espionagem denunciado por Edward Snowden, ex-analista da Agência Nacional de Segurança dos Estados Unidos, que demonstrou repercussões dessa espionagem, inclusive, para o Brasil.

---

[52] KRIEGER, Maria Victoria Antunes. A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18). Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, 2019. Data da publicação: 05 dez. 2019. Disponível em <https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y>. Acesso em 12 de set. de 2021.

[53] DONEDA, Danilo; MENDES, Laura Schertel. Data Protection in Brazil: New Developments and Current Challenges. *In*: Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Springer Netherlands, 2014, p. 8-9

Para Bioni, o Marco Civil da Internet constitui-se enquanto uma reação à tentativa de regular o uso da Internet pela via das leis penais, na medida em que pautar-se em técnicas prescritivas e restritivas para regular o uso das redes digitais poderia resultar em uma desaceleração da inovação tecnológica no país[54]. Por esse motivo, o Marco Civil propõe uma regulação principiológica do uso da Internet no país, conferindo aos cidadãos direitos e garantias nas quais passam a se respaldar as relações travadas no meio virtual.

Nos termos dos artigos 2º e 3º da Lei nº Lei nº 12.965/14, o uso da Internet era regulado com fundamento no respeito pela liberdade de expressão e garantindo aos indivíduos a proteção aos direitos à privacidade e à proteção dos dados pessoais. Nesse sentido, o art. 7º previa que o acesso à Internet é essencial ao exercício da cidadania, assegurando aos usuários das redes os direitos à "inviolabilidade da intimidade e da vida privada", a "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 em termos de uso de aplicações de internet", bem como ao "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais". A garantia ao direito à privacidade era reforçada no art. 8º enquanto condição para o pleno acesso à Internet.

Dessa forma, o Marco Civil da Internet consagrava um regime jurídico de proteção de dados pessoais e garantia do direito à privacidade prevendo o consentimento como pressuposto de licitude do tratamento. Principalmente após o escândalo exposto por Snowden, buscou-se atribuir proteção especial aos titulares dos dados, conferindo-lhes o direito de participarem do processamento de suas informações. Ocorre que o regulamento em referência ainda não era direcionado, especificamente, à proteção dos dados pessoais, além do que não era aplicável às tecnologias implementadas com recurso à biometria. Nesse contexto é que se deu início à elaboração da Lei Geral de Proteção de Dados, conforme será exposto a seguir.

[54] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2019.

2.1 A Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD) assurge em um contexto de um massivo fluxo de dados na Internet. Trata-se da primeira lei que, no Brasil, propôs-se a tratar de modo sistemático e coerente a proteção de dados pessoais, dispondo de regras e procedimentos basais a essa área do direito capazes de impactar significativamente a vida dos indivíduos e dos entes públicos e privados, conforme destaca Ricardo Villas Bôas Cueva:

> Com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 ou LGPD), passamos a contar com um marco normativo indispensável à nossa integração à economia digital. Já contávamos, por certo, com normas protetivas de grande alcance. Na Constituição Federal já se asseguravam os direitos à intimidade, à vida privada e ao sigilo de dados e prevê o habeas data. No Código de Defesa do Consumidor (Lei nº 8.078/1990) foram enunciados importantes direitos relativos a cadastros de consumidores, como os de acesso, comunicação, correção e limitação temporal, que prefiguraram alguns dos princípios caros às legislações de proteção de dados pessoais. Na Lei do Cadastro Positivo (Lei nº 12.414/2011), na Lei de Acesso à Informação (Lei nº 12.527/2011) e no Marco Civil da Internet (Lei nº 12.965/2014), já se identificavam importantes contribuições à proteção de dados pessoais. Mas a LGPD é a primeira lei no Brasil a tratar de modo sistemático e coerente a proteção de dados pessoais, definindo regras e procedimentos estruturantes dessa nascente área do direito, o que terá grande impacto na vida das pessoas, das empresas e dos entes dos setores público e privado, de modo geral.[55]

Nessa esteira, a LGPD dispõe sobre o tratamento de dados pessoais, sendo este considerado como "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", nos termos do que dispõe o art. 5º, X, da lei.

Em um contexto de vigilância incisiva, o titular de dados corre o risco de ter diversos de seus direitos fundamentais violados – eis a evidente importância de que participe do processo de tratamento de suas informações. Partindo desse pressuposto, a LGPD objetiva ajudar na organização da informação[56]. O art. 6º da lei em referência elenca, para que essa organização possa ser alcançada, os princípios da finalidade, adequação, necessidade, livre acesso, qualidade

[55] Prefácio por CUEVA, Ricardo Villas Boas *in* BIONI, B. (org.). Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.
[56] BIONI, B. (org.). Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021, p. 70.

dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas. Veja-se, sobre o tópico, o que dispõe Bioni:

> A LGPD parte da premissa de que toda a organização deve não só conhecer os dados que possui, mas, sobretudo, convertê-los em uma informação útil. Todo o sistema gira em torno da lógica em se criar uma trilha auditável do dado, pela qual o cidadão e os demais agentes econômicos enxerguem todo o seu ciclo de vida e principalmente a sua repercussão nas atividades econômicas e relações sociais que fazem parte. A nova lei não veio para travar o fluxo informacional, mas, muito pelo contrário, estimulá-lo dentro de uma lógica de sustentabilidade entre quem produz essa matéria prima e quem a explora.[57]

Esse equilíbrio ao qual se refere Bioni é facilmente vislumbrado quando analisado o requisito do consentimento do titular, trazido pela lei no seu art. 2º como um passo rumo à concretização do princípio da autodeterminação informativa. Na medida em que dispensa a necessidade do consentimento para o cumprimento de leis e políticas públicas, assim como para órgãos de pesquisa, a LGPD revela o seu claro objetivo de conciliar as vontades do titular e as necessidades dos controladores de dados ao exercerem suas atividades, já que o tratamento de determinados dados é imprescindível ao cumprimento das obrigações de alguns setores específicos.

Não obstante, é fundamental observar que a LGPD destaca o princípio da autodeterminação informativa, que, conforme anteriormente explicado, busca colocar o titular dos dados no controle da sua administração e proteção. Com a necessidade do consentimento do usuário e a consequente expansão da sua participação no tratamento das suas informações privadas, é correto afirmar que a LGPD efetivamente se preocupa com a garantia desse princípio, em especial, mas também de todos os outros elencados no seu art. 2º.

A título de registro, destaque-se que, para além do consentimento e da autodeterminação informativa, são os outros fundamentos da disciplina da proteção de dados pessoais o respeito à privacidade; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os

[57] BIONI, B. (org.). Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021, p. 70.

direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

No que se refere aos dados pessoais, especificamente, a lei os divide em dois grupos distintos, conferindo-lhes tipos de proteção diversos. São eles os dados pessoais e os dados pessoais sensíveis. Quanto à primeira categoria, trata-se, de acordo com o art. 5º, I, da LGPD, dos dados das pessoas naturais que permitem que sejam identificadas ou que sejam capazes de torná-las identificáveis. Conforme explica Bioni, a Lei Geral adota o conceito expansionista de dados pessoais na medida em que os relaciona a sua capacidade de interferência no desenvolvimento da personalidade de seus titulares (Art. 2º, VII)[58].

De outro lado, os dados pessoais sensíveis relacionam-se a elementos mais profundos da personalidade de seus titulares, reconhecendo aspectos da subjetividade que não são disponíveis aos indivíduos e devem, portanto, gozar de uma proteção mais incisiva. O inciso II do art. 5º os define como aqueles dados dos sujeitos que digam respeito à sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, opinião política, dado referente à saúde ou à vida sexual e dado genético ou biométrico, quando vinculado a uma pessoa natural. Esses dados recebem tratamento diferenciado pela lei, na medida em que o seu tratamento informatizado, se realizado da mesma forma por meio da qual se dá o tratamento dos demais dados pessoais, poderia dar ensejo a situações discriminatórias. Sobre o ponto, explica Bioni que

> a proteção dos dados pessoais perpassa a própria tutela do princípio da isonomia, na medida em que é um instrumento de contenção às práticas discriminatórias. (...) Tal tutela jurídica procura assegurar que o titular dos dados pessoais possa se relacionar e se realizar perante a sociedade, sem que eventuais práticas frustrem tal projeto.[59]

Aos dados biométricos, em específico, deve-se destinar especial atenção, já que são mais vulneráveis. O Art. 2º, II, do Decreto 10.046/2019 define os dados biométricos como "características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a

[58] BIONI, B. R.. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 66 a 81.
[59] *Ibid*., p. 84

retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar". Assim, ressalta Wright que "[u]*nlike financial information, biometric data is 'more vulnerable as a data set,' because you can't 'replace* [it] *like you can a credit card*"[60]. Não à toa, a LGPD incluiu os dados biométricos no rol dados pessoais sensíveis.

Para os fins deste trabalho, importa analisar as aplicações dos princípios da finalidade e da não discriminação, já que a inobservância dessas diretrizes no tratamento dos dados pessoais pode, fatalmente, acarretar a violação a direitos fundamentais. Isso porque o maior risco para o cidadão é a comunicação dos dados – é dizer, a leitura conjunta dos mais diversos dados agregados –, e não o seu mero armazenamento, de modo que a forma e o porquê do tratamento desses dados influenciam diretamente nos efeitos gerados por essa comunicação entre eles.

Os mencionados princípios e fundamentos trazidos pela LGPD atendem, assim, à máxima de que se deve "visar a um tratamento limitado desses dados, para evitar o seu eventual uso para propósitos que não atendam aos fundamentos republicanos do Estado Democrático de Direito"[61]. Prestam-se justamente, pois, a proporcionar uma estrutura legal que proteja garantias fundamentais em qualquer ambiente de fluxo de dados que os avanços tecnológicos da sociedade da informação venham nos apresentar – os quais são numerosos e diversos.

Nesse sentido, destaque-se que o mero "fato de participarmos desta época é suficiente para que soframos constante vigilância, através de câmeras, sensores e o monitoramento dos dados que produzimos diariamente"[62], do que se extrai que, voluntária ou involuntariamente, vive-se sob o constante monitoramento possibilitado pelo avanço tecnológico, principalmente considerando a implementação da tecnologia de reconhecimento facial, em específico, como ferramenta à vigilância desenvolvida.

---

[60] "[A]o contrário da informação financeira, os dados biométricos são 'mais vulneráveis como um conjunto de dados', porque não se pode 'substituí-los como se fosse um cartão de crédito'." (Tradução livre). (WRIGHT, E. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 2019, p. 163).

[61] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, 2018, 19.3: 159-180. p. 163

[62] SOUZA, Thiago Pinheiro Vieira de. A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal de Uberlândia, Minas Gerais, 2018, p. 577.

3. A TECNOLOGIA DO RECONHECIMENTO FACIAL

O desenvolvimento tecnológico avança em ritmo acelerado no mundo globalizado. Uma das tecnologias que acompanham essa evolução é a do reconhecimento facial, que permite a identificação de pessoas em meio à multidão, sendo aplicada para os mais diversos fins, inclusive para a realização de vigilância em prol da segurança pública e privada. Esse uso voltado à *surveillance* foi bastante estimulado pelo barateamento das ferramentas tecnológicas de monitoramento, fato que traçou a tendência da sua realização de forma rotineira[63].

Isso porque as facilidades de importação e o aumento de sua produção no país a partir dos anos 1990 permitiram essa redução dos preços dessas tecnologias de vigilância e impulsionaram o setor da segurança. Tão logo, juntamente ao surgimento de inúmeros desafios à administração pública relacionados à segurança e ao controle social, foi possível observar a adesão dos Estados ao uso das novas tecnologias de vigilância alimentadas pelo *Big Data*, capazes de processar enormes volumes de dados, justamente em razão do seu potencial de auxiliar no manejo social.

Essa "popularização" do uso da tecnologia do reconhecimento facial no mundo ensejou o seu desenvolvimento de forma ainda mais acelerada. Em especial, com o aumento do número de pessoas realizando viagens internacionais, após os eventos do 11 de setembro nos Estados Unidos da América, passaram os Estados a adotar todos os meios possíveis para, de forma eficiente e pretensamente precisa, regular as idas e vindas de pessoas pelo mundo por vias da identificação dos seus rostos[64].

A introdução de sistemas de vigilância baseados em circuitos fechados de televisão (CFTV/CCTV) foi responsável por modificar a natureza da *surveillance*, tanto quantitativa quanto qualitativamente. Para o Norris, com o uso da tecnologia de circuitos fechados de televisão,

---

[63] CLARKE, R. A. Information Technology and Dataveillance. Communications of the ACM 31, 1988. Disponível em: <http://www. rogerclarke. com/DV/CACM88.html> Acesso em: 07 de maio de 2021.

[64] VU, Brandon. ―A Technological and Ethical Analysis of Facial Recognition in the Modern Era. *In*: A Technological and Ethical Analysis of Facial Recognition in the Modern Era, 2018, p. 11-12. Disponível em: <https://www.academia.edu/38066258/A_Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era>. Acesso em 11 set. de 2020.

> o escopo da vigilância foi expandido para um nível inimaginável com base na co-presença; o escopo da vigilância não mais se restringe às limitações espaciais inerentes à vigilância presencial; o escopo da vigilância fica livre das restrições temporais da interação face-a-face e da presença humana; a vigilância e a intervenção autoritária tornam-se funcionalmente separadas; o ato de vigilância se torna mais democrático: todos ficam igualmente sujeitos ao olhar de vigilância; o projeto disciplinar do *panopitcon* é expandido à medida que o controle social inclusivo é promovido sobre a exclusão.[65]

Sendo assim, correto afirmar que a transição de uma sociedade analógica para uma sociedade digital, principalmente com a evolução das tecnologias de reconhecimento facial, resultou na intensificação da *surveillance*, seja ela realizada por entes públicos ou por agentes privados do mercado.

Com efeito, o reconhecimento facial diz respeito à habilidade que *softwares* de computador possuem de reconhecer e identificar rostos de pessoas a partir de fotos ou vídeos constantes das bases de dados utilizadas como referência. Trata-se de uma forma de biometria, que é a ligação entre um elemento do corpo humano de um indivíduo com uma unidade de registro. A partir da identificação, os detalhes dos rostos são catalogados, por biometria, para que imagens obtidas a partir de um computador, *smartphone* ou câmera de vigilância possam ser processadas de tal modo a que se encontre uma correspondência e, posteriormente, utilizadas para uma gama de propósitos[66].

A biometria, a seu turno, é uma tecnologia que permite o reconhecimento automático dos indivíduos com base em suas características comportamentais e biológicas. Dados biométricos podem ser adquiridos de qualquer fonte que documente visualmente um indivíduo ou que observe características identificáveis como frequência cardíaca ou odor. Podem derivar, pois, da marcação automatizada de fotos em sites como o Facebook, da atividade e o monitoramento da

[65] NORRIS, C. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge: New York, 2003. p. 253.

[66] NABEEL, F. Regulating Facial Recognition Technology in Public Places. Centre for Strategic and Contemporary Research, 2019, p. 1. Disponível em: <https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public _Places.> Acesso em: 07 de maio de 2021.

saúde através de equipamentos vestíveis com o Fitbit e até mesmo dos gestos usados quando os indivíduos interagem com seus telefones e computadores. Nas palavras de Wright:

> *The faceprint measurements and other collected information are "biometric data," which are compiled into a database.49 Using the biometric database, faceprints may then allow for: (1) facial classification, by classifying the face into categories such as an estimation of gender, age or race; (2) verification, by comparing the similarity of previously stored faceprint of any particular individual to a new faceprint and establishing a confidence score that the two individuals are the same; and (3) identification, by comparing a person's facial image to a database of stored faceprints*.[67]

Nos últimos anos, as tecnologias biométricas melhoraram de forma consciente após o aumento dos investimentos e pesquisas em sistemas de reconhecimento facial. Embora as técnicas empregadas variem, os sistemas de reconhecimento facial geralmente operam de uma forma padrão. Isso porque, apesar de o rosto humano apresentar características variáveis de pessoa para pessoa, existem combinações básicas que se verificam como regra, notadamente, os dois olhos e a distância entre eles, o nariz e o seu comprimento, as bochechas, a boca e o queixo, atributos que podem ser lidos por *softwares* regidos por algoritmos gravados e armazenados em bancos de dados – estes que operam a detecção das formas geométricas da face, montagem do quebra-cabeça e, posteriormente, a realização comparações com as fotos existentes em bancos de dados[68].

Assim, a face não é analisada por completo: são escolhidos alguns pontos do rosto e, com base nas distâncias entre esses pontos, é calculada a probabilidade de aquele rosto pertencer à pessoa cadastrada no banco de dados selecionado para a análise. No caso do rosto humano, as possibilidades de haver diferenças ou modificações nessas distâncias são grandes, já que as pessoas envelhecem e perdem colágeno, podem estar bocejando, piscando, sorrindo etc.

Nessa esteira, pode-se afirmar que os sistemas de vigilância baseados em reconhecimento facial, inclusive os mais modernos, são bastante simplistas: além de operarem conforme um

[67] WRIGHT, E. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 2019.
[68] KOCH, MÁRCIO. Visão computacional para reconhecimento de faces aplicado na identificação e autenticação de usuários na web, 2012. BATISTA, Gabriel Almeida et al. Sistema de identificação e autenticação biométrica. 2017. 121f. Atividade supervisionada (Curso de Ciências da Computação) – Universidade Paulista, São Paulo, 2017.

protocolo padrão, não utilizam outra lógica senão aquela que houver sido inserida no seu *software* por um programador humano, sendo o ponto final desse processamento a criação de um sistema binário determinístico de classificação: o acesso é aceito ou negado; a identidade é confirmada ou rejeitada; o comportamento é legítimo ou ilegítimo[69].

Além disso, o uso das tecnologias de reconhecimento facial requer acesso a um material de referência através de um banco de dados, tratando-se este de um acervo contendo um ou mais tipos de informações como textos, imagens, clipe de vídeo, som, diagramas e animações gráficas[70]. O material em banco de dados multimídia pode ser gerado pelo sistema e povoado a partir de uma variedade de fontes, e a crescente disponibilidade pública de imagens de rostos, especialmente considerando que companhias como o Facebook fomentam políticas de identidade real, pode resultar em um imenso banco de dados pesquisáveis para indivíduos previamente não identificados.

Em todo caso, existentes os sistemas digitais que possibilitam o reconhecimento de pessoas a partir de cruzamento de informações com enormes bases de dados, a própria imagem de vídeo se torna fonte de informação. Assim, em que pese *softwares* de reconhecimento facial representem um avanço em relação às informações geradas em um circuito fechado de televisão, em termos técnicos, uma vez que as imagens sejam dispostas em um banco de dados digital, sendo o seu processamento realizado por meio de algoritmos, amplia-se, no entanto, o potencial de conexão com bancos de dados existentes, de modo que "a ligação de informações extraídas de imagens de CFTV a informações relacionadas a identidade em bases de dados exponencialmente aumenta o seu 'efeito pan-óptico'"[71].

A tecnologia, no sentido mais abrangente da palavra, tem como característica intrínseca a imprevisibilidade; as possibilidades que oferece, a seu turno, vão além daquilo que o homem

[69] NORRIS, C. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge: New York, 2003. p. 276.
[70] WRIGHT, E. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 2019.
[71] NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge: New York, 2003. p. 269-270.

jamais teve a oportunidade de administrar. Tal imprevisibilidade, assim, não é de todo positiva, tal qual pode ser observado da metáfora apresentada por Doneda em sua obra:

> O Golem, criatura da mitologia hebraica, é um humanóide de argila, feito pelo homem; ele é poderoso e sua força cresce a cada dia. Ele segue as ordens do seu criador, auxilia-o, mas é um pouco tolo e inconsciente de sua força: é capaz, se não for bem comandado, de destruir seu próprio senhor. A ideia de um "Golem tecnológico", aqui utilizada para nos aproximar um pouco do problema, pode induzir à constatação de que se ele não é, em última análise, responsável pelos seus atos, é, porém, uma criação do gênio humano, por cujos defeitos somos responsáveis – do que surge nossa obrigação de conhecê-lo a fundo.[72]

Nessa esteira, a ideia de "conhecer a fundo o Golem" pode ser traduzida na necessidade de explorar as origens da tecnologia do reconhecimento facial, que são problemáticas. Isso porque remontam às teorias eugenistas de Francis Galton, que sobrepôs imagens de homens condenados por crimes na tentativa de encontra a essência do rosto de uma pessoa naturalmente inclinada ao cometimento de crimes. Ele também tentou usar retratos sobrepostos para determinar um "tipo" ideal para cada raça, e sua pesquisa foi citada por Hans F.K. Gunther, um eugenista nazista que escreveu um livro cuja leitura era obrigatória nas escolas alemãs durante o Terceiro Reich.

Ainda que desnecessário o emprego de maiores esforços para explicar o óbvio, importa mencionar que a teoria de Galton padece de inúmeros vícios, já que pautada em premissas fundamentalmente equivocadas, quais sejam: (i) de que as pessoas condenadas por crimes são representativas daqueles que os cometem, esquecendo-se de que a justiça é lamentavelmente permeada por vieses; (ii) de que o conceito de criminalidade inata seria sólido, este que, na verdade, não se sustenta, já que as circunstâncias da vida acabam por moldar a inclinação de um sujeito ao cometimento de um crime; e (iii) que a aparência facial traduziria o caráter e as emoções reais dos indivíduos, ao passo que as emoções não podem ser reduzidas a categorias tão facilmente interpretáveis – e computacionalmente convenientes.

As semelhanças entre a análise facial moderna e sua versão analógica anterior causam espanto. Ambas, por exemplo, originaram-se de tentativas de rastrear criminosos e potenciais ameaças à segurança dos indivíduos de uma sociedade. Alphonse Bertillon, um policial francês e

[72] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 91.

pioneiro nos estudos acerca da análise das feições do rosto, na intenção de identificar criminosos reincidentes, inventou a *mugshot* e nela passou a incluir medidas específicas do corpo do sujeito, como o comprimento da cabeça. Com registros de mais de 100.000 prisioneiros, coletados entre 1883 e 1893, ele identificou 4.564 reincidentes.

O esquema de classificação de Bertillon foi, posteriormente, substituído por um sistema mais eficiente pautado no uso de impressões digitais, mas a ideia básica de usar medidas corporais para identificar pessoas a serviço de um aparelho de inteligência renasceu com o desenvolvimento da moderna tecnologia do reconhecimento facial, cujo progresso foi estimulado, inclusive, por investimentos militares e competições entre governos do mundo.

A evolução permitiu, ao final dos anos 90, que os algoritmos mapeassem automaticamente as feições dos rostos, sendo capazes de escanear vídeos em tempo real. Atualmente, os serviços de análise facial são disponibilizados no mercado por *players* como a Amazon e a Microsoft a preços acessíveis, podendo ser usados por qualquer um que deseje adivinhar a identidade, sexo, idade e, em tese, o estado emocional de uma pessoa. Há, ainda, plataformas como Face++ que também se propõem a adivinhar a raça da pessoa cujo rosto se propõe a analisar.

Ocorre que nenhum sistema de análise facial é perfeitamente preciso. E, embora isso não represente um problema grave quando se trata de do desbloqueio de um telefone celular, torna-se um grande obstáculo quando usado para identificar indivíduos suspeitos de crimes. A título de exemplo, o Rekognition (sistema de identificação facial da Amazon), ao analisar o rosto da Oprah Winfrey, concluiu de que se trataria de um homem. Ele também encontrou correspondências, erroneamente, de 28 membros do Congresso Americano, com relação a um banco de dados de *mugshots*.

Diversas pesquisas mostram que estes erros não são incomuns. Um estudo do MIT[73] sobre três sistemas comerciais de reconhecimento de gênero revelou que eles tinham taxas de erros de

[73] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. Face recognition vendor test (FRVT) Part 3: Demographic Effects. Estados Unidos: National Institute of Standards and Technology, U.S. Department of Commerce, 2019. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 11 de set. de 2021.

até 34% para mulheres de pele escura – uma taxa quase 49 vezes maior do que para homens brancos. Esse mesmo estudo indicou que, quando analisado o recorte dos casos em que o algoritmo reconhecia duas pessoas como a mesma, as taxas de erro foram duas vezes maiores com relação a homens e mulheres africanos, em comparação a europeus.

O enviesamento e a imprecisão que tais pesquisas revelam são resultado da forma como essas ferramentas são desenvolvidas. Algoritmos são ensinados a identificar uma face quando a ele expostos milhões de imagens de rostos humanos, assim, se os rostos usados para treinar o algoritmo forem predominantemente pertencentes a homens brancos, o sistema terá mais dificuldade para reconhecer qualquer um que não se encaixe nesse padrão.

Há quem diga que, com ensinamento suficiente e exposição a um banco de dados amplo, composto dos mais variados perfis de pessoas, a questão do enviesamento dos algoritmos poderia ser eliminada. No entanto, mesmo se o sistema funcionasse perfeitamente, ainda seria motivo de preocupação, na medida em que estaria sendo treinado por seres humanos, suscetíveis a preconcepções originalmente enviesadas.

Ao fim e ao cabo, a reprodução perfeita de um padrão tendencioso não contribuiria para a aceitação do uso da ferramenta do reconhecimento facial como ferramenta de *surveillance* sem que fossem geradas preocupações, de qualquer forma. Nas palavras de Aguera y Arcas, "*using scientific language and measurement doesn't prevent a researcher from conducting flawed experiments and drawing wrong conclusions – especially when they confirm preconceptions*"[74].

Em que pese o uso da tecnologia apresente pontos positivos, como, por exemplo, o aumento da segurança pública, possibilitando que as autoridades competentes encontrem pessoas desaparecidas, criminosas ou em situações suspeitas, retirando das ruas as que possuem pendências judiciais, os pontos negativos são tão graves que não podem ser ignorados. Tratar-se-

[74] "utilizar linguagem e medição científicas não impedem um pesquisador de conduzir experimentos com falhas e tirar conclusões erradas – especialmente quando essas confirmam preconceitos." (Tradução Livre) (ARCAS, Blaise Agüera y; MITCHELL, Margaret; TODOROV, Alexander. Physiognomy's new clothes. Blaise Agüera y Arcas, 2017. Disponível em <https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a>. Acesso em 10 de set. de 2021).

ia de um falso *trade off*. Não por acaso, verifica-se, em vários lugares do mundo, movimentos em busca do banimento dessa tecnologia[75].

Cabe ao direito nesse cenário, pois, mostrar-se apto a responder à novidade proposta pela tecnologia com a reafirmação e defesa de seus valores e, ao mesmo tempo, deve fornecer a segurança necessária para que haja a previsibilidade e segurança devidas para se resguarde o efeito prático das garantias constitucionais aos indivíduos. O verdadeiro problema não é saber sobre o que o direito deve atuar, mas, sim, como se deve interpretar a tecnologia e suas possibilidades de aplicação e uso para que sejam reguladas de modo a que seja preservado o indivíduo e os direitos que lhe são atribuídos.

[75] Disponível em <https://www.banfacialrecognition.com/>. Acesso em 11 de set. de 2021.

4. O POTENCIAL LESIVO DO USO DA TECNOLOGIA DO RECONHECIMENTO COMO FERRAMENTA DE SURVEILLANCE

Conforme amplamente explorado neste trabalho, o grande avanço das tecnologias de processamento de dados em larga escala, seja por organismos públicos ou privados, colocou o indivíduo em posição de vulnerabilidade quanto ao tratamento e uso de seus dados pessoais. A denominada sociedade da vigilância tem o potencial de discriminar e classificar seus indivíduos, e essa vigilância é caracterizada pelo modo rotineiro em que ocorrem a coleta e manuseio de dados pessoais, encabeçada pelo uso de tecnologias extremamente modernas capazes de perfilar o indivíduo com pretensa precisão. Daí que, a partir desse ponto,

> nota-se a necessidade de que a tutela jurídica dos dados pessoais abranja também a proteção da igualdade dos cidadãos e não apenas a sua liberdade, como ocorreu majoritariamente nas primeiras normas de proteção de dados. Para tanto, a proteção de dados pessoais deve ser apta a combater a discriminação passível de ocorrer em razão das informações extraídas dos bancos de dados, buscando fornecer uma tutela mais rígida em caso de tratamento de dados sensíveis e de situações potencialmente discriminatórias.[76]

A utilização de sistemas de reconhecimento facial como ferramenta de *surveillance* indica que o simples fato de vivermos nesses tempos é suficiente para que incida sobre nós uma vigilância constante, esta que é dotada de considerável potencial lesivo aos direitos fundamentais. Nesse sentido, podem ser elencados alguns dos potenciais lesivos do uso da tecnologia do reconhecimento facial como ferramenta de *surveillance*: (i) a agregação das impressões faciais capturadas com a tecnologia do reconhecimento facial a enormes bancos de dados compostos de informações das mais variadas naturezas ("*Big Data*"); (ii) uso secundário desses dados, é dizer, a sua aplicação a fins distintos daqueles revelados a princípio; (iii) discriminação e exclusão de determinados grupos sociais a partir da categorização dos indivíduos que se dá na fase do tratamento dos dados coletados e agregados; e (iv) criação de um desnível nas relações de poder entre quem vigia e quem é vigiado[77].

[76] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 59.

[77] RICHARDS, N. M. The dangers of surveillance. 126 HARV. L. REV. 1934, 1935, 2013. Disponível em: <https://harvardlawreview.org/wpcontent/uploads/pdfs/vol126_richards.pdf>. Acesso em: 07 de maio de 2021.

Nota-se que o acúmulo indiscriminado de dados permite que eles se comuniquem entre si, fato preocupante se levado em conta que se está vivendo em tempos de *Big Data* e *data aggregation*, de modo que possível, por meio do tratamento de toda essa informação, a criação e inserção de sujeitos em categorias arbitrárias. Tais compilados de informação estariam fora do escopo de controle dos cidadãos, abrindo uma deixa preocupante à proteção dos dados pessoais, já que, no fim das contas, estar-se-ia afastando o indivíduo do processo de tratamento e leitura dos seus dados, ao passo que um volume de informações detalhado sobre uma pessoa permite a composição de um perfil muito preciso sobre a sua personalidade, nesse caso, sem o seu eficaz consentimento. Esses fatos, por si só, revelam a possibilidade de enquadramento da *surveillance* como uma ferramenta reprodutora de discriminação e amplificadora de desigualdades sociais

Com efeito, o processamento de dados em tempos de *Big Data* ocorre em volume, velocidade e variedade maiores. Permite-se, assim, uma agregação maciça de dados, do que é possível inferir padrões de comportamento e preferências dos titulares ao final do tratamento. É dizer, outras informações pessoais podem ser extraídas de uma massa de dados, quando combinados.

Conforme aduz Bioni, "[o] conjunto agregado dessas informações pode estruturar um perfil bem detalhado a orientar decisões, sejam elas automatizadas ou não, sobre a pessoa de carne e osso, ora intermediado por seus dados pessoais"[78]. Essa falta de transparência permite que muitos cidadãos sejam perfilizados e categorizados à sua revelia, sujeitando-se a um processo de tomada de decisões do qual sequer têm conhecimento.

Verifica-se que a questão trata de mecanismo que, em última análise, promove a classificação de pessoas segundo critérios predeterminados e, com base nisso, tentar prever seus próximos passos a partir de estimativas de padrões comportamentais – o que é possível a partir da comunicação dos dados pessoais agregados. Como resultado, modificam-se as relações de visibilidade/opacidade, inclusão/exclusão de determinadas categorias sociais, com base na ampla disponibilidade de informações personalizadas e compiláveis sobre elas.

[78] BIONI, B. R. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019, p. 35.

Destaque-se que, em termos gerais, essa categorização ocorre automaticamente por algoritmos de tratamento de dados cuja função é classificar, a partir de critérios pré-estabelecidos pelos seus programadores, todas as informações coletadas. Sendo assim, todos os sistemas de vigilância baseados em reconhecimento facial utilizarão a sistemática que houver sido inserida em seu *software* por um programador humano. Sobre o tópico, a jurista Ana Frazão argumenta que, "[a]final, algoritmos são criados por seres humanos, com todos os seus vieses e falibilidades, bem como com todas as possibilidades de desvirtuamento, a fim de privilegiar os interesses daqueles para quem foram programados"[79]. Ironicamente, no entanto, o processo de classificação binária de dados é realizado por decisões algorítmicas totalmente automatizadas.

Assim, a utilização dos algoritmos como ferramenta à criação e inserção dos indivíduos em categorias arbitrárias possibilita que a *surveillance* funcione como um meio de reprodução de discriminação e amplificação de desigualdades sociais. Frazão complementa aduzindo que "[a]final, são as categorias para as quais nossas vidas datificadas serão convertidas que passarão a definir não apenas quem somos, mas também quem seremos, na medida em que os dados nos representam ao mesmo tempo que nos regulam."[80].

Na realidade, vê-se que a utilização dessa tecnologia possibilita que a comunidades específicas seja imposto um monitoramento incisivo, centrado na proibição, na rejeição e na ilegitimidade, enquanto outras recebem um tratamento no sentido oposto, facilitado pela configuração do algoritmo. Assim, "*the fact that the way in which our lives are shaped* (…) *depends heavily on the kinds of data available about us means that politics of information is an*

[79] FRAZÃO, A. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1.ed. São Paulo: Thomson Reuters, 2019, p. 33.

[80] FRAZÃO, A. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1.ed. São Paulo: Thomson Reuters, 2019, p. 35.

increasingly important arena for debate. (...) [S]ocial categorization affects ordinary people's choices and chances"[81].

Por esse ângulo, Wright traz que o uso do reconhecimento facial como ferramenta de *surveillance* efetivamente degrada uma divisão já instável entre o espaço corpóreo e o cyber-espaço, na medida que a leitura resultante da transformação das expressões faciais a um formato legível por máquina acaba por reduzir a singularidade humana a um sistema binário determinístico[82]. Verificam-se, assim, alguns dos riscos do uso do reconhecimento facial como ferramenta de *surveillance*, tal qual enumerado por Wright: (i) as preocupações de privacidade biométrica envolvendo dados de localização e vigilância; (ii) os riscos de violação da privacidade de dados; (iii) como a agregação pelos corretores de dados pode agravar os riscos de privacidade[83].

A gravidade da situação resta evidenciada quando constatada a opacidade e a falta de transparência que a gerem. Conforme destaca Solove, os governos têm coletado e feito uso dos dados pessoais dos nossos dados pessoais sem conferir-nos o direito de saber quais dados estão sendo coletados, com qual finalidade e se isso está sendo feito de forma apropriada e legítima[84]. O cenário remete ao mundo kafkiano de Josef K. (protagonista de "O Processo"), em que decisões estão sendo feitas sobre a vida dos indivíduos com base em suas informações pessoais sem que, no entanto, tenham participação nesse processo ou sequer conhecimento sobre o contexto em que se encontram inseridos.

---

[81] "[O] fato de que a forma como as nossas vidas são moldadas (...) depende muito dos tipos de dados disponíveis sobre nós significa que a política de informação é uma arena cada vez mais importante para o debate. (....) A categorização social afeta as escolhas e oportunidades das pessoas comuns." (Tradução livre) (LYON, D. Surveillance studies: an overwiew, Cambridge: Polity, 2007, p. 8).

[82] WRIGHT, E. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 2019, p. 610-611)

[83] WRIGHT, E. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 2019, p. 611)

[84] SOLOVE, D. Daniel Solove: Nothing to Hide, Nothing to Fear? Entrevista concedida a Steve Paikin. Canal The Agenda with Steve Paikin. Disponível em <https://www.youtube.com/watch?v=FqJ8EMwj7zY&ab_channel=TheAgendawithStevePaikin>. Acesso em 26 de maio de 2021.

Diante dessa conjuntura, pretende-se, aqui, questionar em que medida o desenvolvimento e a utilização de sistemas de vigilância por reconhecimento facial são compatíveis com a proteção dos direitos fundamentais. Várias são as amostras estatísticas e jornalísticas indicando as expressivas taxas de erro apresentadas pelos *softwares* de reconhecimento facial, as quais são maiores ou menores a depender do grupo social no qual está inserto o indivíduo[85], conforme será demonstrado, com a apresentação de casos concretos, no ponto 3.1. deste trabalho.

Garfinkel, na linha do que se vem sustentando, procura mostrar que, por detrás da tecnologia, estão seres humanos que a criam e a projetam com o intuito de desnivelar as relações de poder na sociedade, fomentando o seu controle sobre algumas de suas parcelas, justamente, por meio da violação de sua privacidade[86]. Segue argumentando, nesse sentido, que "a tecnologia não existe no vácuo"[87] na medida em que, em verdade, são ou deixam de ser regulamentadas a depender das prioridades da sociedade sobre a ciência, o mercado, a política etc.

Há muitas referências na história que mostram o uso negativo da tecnologia, a qual tende sempre a violar a privacidade. Até mesmo porque é sabido ser mais complexo e mais caro produzir tecnologia que proteja a privacidade dos indivíduos. Assim, não faz sentido acreditar em uma neutralidade inerente à tecnologia, a qual é dotada, em realidade, da capacidade de ser cada vez mais intrusiva, na medida em que se encontra em constantemente aprimoramento das suas funções de classificação e busca das informações.

Ao fim e ao cabo, a verdade é que, em uma democracia, os cidadãos são os donos do poder, e para que o exerçam, é necessária transparência para que entendam as ações de seus líderes e, assim, as possam avaliar. Sobre o tópico, registra Ana Frazão:

---

[85] A título de exemplo, mencione-se o estudo "*Face Recognition Vendor Test*", realizado pelo MIT (disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.), que analisou três sistemas comerciais de reconhecimento facial voltado à identificação de gênero e constatou que as taxas de erro na identificação de mulheres negras foram superiores a 34%, enquanto que a porcentagem de acerto para homens brancos foi 49% maior. Além disso, quando analisado o recorte dos casos em que o algoritmo reconhecia duas pessoas como a mesma, as taxas de erro foram duas vezes maiores com relação a homens e mulheres de origem africana, em comparação a homens e mulheres de origem europeia.

[86] GARFINKEL, Simson. The Death of Privacy in the 21st Century. Cambridge: O"Riely, 2000. p. 15-16.

[87] GARFINKEL, Simson. The Death of Privacy in the 21st Century. Cambridge: O"Riely, 2000. p. 15-16.

> [...] seria necessário haver algum tipo de controle tanto sobre (i) a qualidade dos dados, a fim de saber se atendem aos requisitos da veracidade, exatidão, precisão, acurácia e sobretudo adequação e pertinência diante dos fins que justificam a sua utilização, quanto sobre (ii) a qualidade do processamento de dados, a fim de saber se, mesmo a partir de dados de qualidade, a programação utilizada para o seu tratamento é idônea para assegurar resultados confiáveis.[88]

Ora, se não são esclarecidas questões como quem terá acesso a esses registros biométricos, por quanto tempo ficarão armazenados ou se os dados podem ser transferidos para outros sistemas, em se tratando de dados sensíveis, está-se ignorando por completo os fundamentos da proteção de dados dispostos no art. 2º da LGPD. Assim, conclui Rodotà que "existem evidentemente muitas boas razões que sustentam a necessidade de usar todas as oportunidades oferecidas pelas novas tecnologias para proteger a sociedade dos crimes", sendo imperioso, assim, "buscar o equilíbrio entre a visão individualista da privacidade e a satisfação das demandas da sociedade"[89].

4.1 Análise dos casos em que a tecnologia do reconhecimento facial foi utilizada como ferramenta de **surveillance**

De fato, um dos efeitos mais intrusivos possibilitados pela tecnologia do reconhecimento facial está na vigilância. A sensação de se estar em meio ao constante aprimoramento tecnológico nos faz acreditar, quase sempre, que ele tende a servir ao bem da sociedade. O que se vê, em realidade, é o contrário. Por vezes a tecnologia é aplicada de modo a privilegiar determinado grupo de indivíduos, entidades, governos, para estabelecer certo controle sobre outros. E, na disputa pelo controle, a privacidade é alvo crucial de investidas tecnológicas[90].

Nesse sentido e conforme arguido anteriormente neste trabalho, a invasão da privacidade é uma escolha consciente dos operadores e desenvolvedores de tecnologias que agregam dados. Há muitas referências na história que mostram que o mal uso da tecnologia poderá ensejar violação a direitos fundamentais, tais como os direitos à privacidade e à proteção dos dados pessoais, o que

[88] FRAZÃO, A. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 1.ed. São Paulo: Thomson Reuters, 2019, p. 38.
[89] RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 148.
[90] DONEDA, D. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, p. 31 a 62.

se assevera se considerado que movas tecnologias de vigilância estão sendo rapidamente inseridas no cotidiano das pessoas sem a devida avaliação dos seus efeitos em toda a complexidade das relações de poder que permeiam o tecido social. Uma dessas novas técnicas é o reconhecimento facial, que vem ganhando popularidade.

No Brasil, tal tecnologia tem sido agregada a sistemas de vigilância com grande interesse por gestores públicos, testados principalmente em grandes eventos públicos. Os resultados dos projetos de monitoramento, por enquanto, podem ser resumidos a prisões de indivíduos reconhecidos pelo sistema das denominadas câmeras inteligentes.

A título de exemplo, cite-se o sistema de videomonitoramento inteligente implementado para auxiliar o trabalho da polícia militar na festa de ano novo de Salvador, na passagem de ano de 2018 para 2019, com um "recém-lançado software de reconhecimento facial", que indica a presença de pessoas cadastradas no banco de dados da Secretaria da Segurança Pública (SSP) como procuradas pela polícia baiana. Aproximadamente cinquenta câmeras foram instaladas na cidade para o evento, dentre elas as da Plataforma de Observação Elevada, que transmite imagens para o Centro de Comando e Controle (CICC), instalado no Centro de Operações e Inteligência, em tempo real[91].

Em salvador, naquele mesmo ano de 2019, houve registro da prisão de suspeito de homicídio, cujo rosto fora identificado por câmera de reconhecimento facial instalada em circuito do carnaval na cidade[92]. O rapaz foi o primeiro a ser preso com o auxílio da tecnologia do reconhecimento facial implementada pela Secretaria de Segurança Pública da Bahia no carnaval de Salvador, cujo objetivo era justamente identificar criminosos com mandados de prisão em aberto e impedir a entrada de armas de fogo e outros objetos que pudessem expor os foliões a risco na comemoração. Tal qual o sistema instalado na cidade para a virada do ano, os rostos

[91] HOSANA, Kelly. Videomonitoramento Inteligente estreia no Réveillon de Salvador. Secretaria de Segurança Pública da Bahia, 2018. Disponível em <http://www.ssp.ba.gov.br/2018/12/4933/Videomonitoramento-Inteligente-estreia-no-Reveillon-de-Salvador.html>. Acesso em 10 de set. de 2021.

[92] ALVES, Alan Tiago. Flagrado por câmera vestido de mulher no carnaval na BA matou homem após vítima passar perto dele de moto em alta velocidade. G1, 2019. Disponível em <https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml>. Acesso em 10 de set. de 2021.

identificados eram cruzados com a base de dados da SSP. Ao todo, foram capturados mais de 1,3 milhão de rostos no evento, o que resultou no cumprimento de 18 mandados e na prisão de 15 pessoas[93].

Um outro exemplo do uso da tecnologia do reconhecimento facial em grandes eventos foi o carnaval da cidade do Rio de Janeiro do ano de 2019[94]. O sistema implementado para a ocasião, que contou com um aparato de cerca de 30 câmeras em funcionamento, identificou 8 mil pessoas foragidas, suspeitas ou desaparecidas, tendo sido realizadas 10 prisões. As imagens capturadas eram transmitidas em tempo real para o Centro Integrado de Comando e Controle (CICC) e, posteriormente, cruzadas com as bases de dados da Polícia Civil e do Detran. Quando o sistema automatizado encontra uma correspondência, a imagem é congelada, apontando a identificação do indivíduo, e é acionada a unidade mais próxima para realizar a abordagem e identificação. Em vista ao "sucesso" do piloto, o governador do estado do Rio de Janeiro à época anunciou que o número seria aumentado de 34 para 140 câmeras até o mês de julho daquele ano.

O projeto de construção de uma "Muralha Digital" na cidade de Curitiba, em 2019, também deve ser citado como exemplo[95]. O projeto trata da instalação de câmeras dotadas da tecnologia do reconhecimento facial e de placas de carros em pontos-chave da cidade, visando à realização de um monitoramento público e privado. Segundo o projeto, a gestão das imagens será de responsabilidade de um comitê formado por integrantes de secretarias municipais e da Urbs, observando sempre o "respeito à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas".

A partir do exposto, pode-se afirmar que o uso das tecnologias de reconhecimento facial como ferramenta de *surveillance* no Brasil tomou popularidade no ano de 2019. Ocorre que,

[93] G1 BA. Feira de Santana registra 33 prisões por reconhecimento facial durante micareta. G1, 2019. Disponível em <https://g1.globo.com/ba/bahia/noticia/2019/04/29/feira-de-santana-registra-33-prisoes-por-reconhecimento-facial-durante-micareta.ghtml>. Acesso em 10 de set. de 2021.
[94] SILVA, Victor Hugo. Rio de Janeiro identificou 8 mil pessoas com reconhecimento fácil no Carnaval. Tecnoblog, 2019. Disponível em <https://tecnoblog.net/289696/rio-de-janeiro-identificou-8-mil-reconhecimento-facial/>. Acesso em 10 de set. de 2021.
[95] FONTES, Giulia. De olho no monitoramento, Curitiba muda regras para a instalação de câmeras. Gazeta do Povo, 2019. Disponível em <https://www.gazetadopovo.com.br/politica/parana/de-olho-no-monitoramento-curitiba-muda-regras-para-a-instalacao-de-cameras-dqpfkx5asc5ugd2m49ysd8jni/>. Acesso em 10 de set. de 2021.

desde logo, observou-se efeitos bastante negativos decorrentes desse uso. Em julho daquele ano, por exemplo, o sistema utilizado pela polícia do Rio de Janeiro identificou erroneamente, no seu segundo dia de atividade, uma mulher que estaria sendo procurada pela justiça. Além da moça cujo rosto fora identificado pelo reconhecimento facial não ser a pessoa que constava na base de dados como procurada pelo crime de homicídio, descobriu-se logo após que a criminosa procurada já estava presa há quatro anos – o que evidencia a desatualização das bases de dados usadas como referência à identificação dos rostos capturados com as câmeras dotadas da tecnologia do reconhecimento facial. Alguns dias depois, houve mais uma prisão por engano no Rio de Janeiro[96].

Apesar do caráter experimental da implementação da tecnologia, que já apresenta resultados no mínimo preocupantes, o governo federal tem dado sua contribuição para a expansão da tecnologia com a portaria n° 793, de outubro de 2019, que regulamenta o uso de dinheiro do Fundo Nacional de Segurança Pública para o "fomento à implantação de sistemas de videomonitoramento com soluções de reconhecimento facial, por *Optical Character Recognition* – OCR, uso de inteligência artificial ou outros"[97].

Não fossem bastantes as prisões levadas a cabo por falhas da tecnologia do reconhecimento facial, um estudo realizado pela Rede de Observatórios da Segurança, que monitorou casos de prisões e abordagens com o uso do reconhecimento facial desde a sua implementação, verificou que 90,5% das prisões decorrentes do uso da tecnologia foram de pessoas negras[98]. O levantamento realizado pela Rede de Observatórios da Segurança englobou as prisões ocorridas entre os meses de março a outubro em 5 estados – Bahia, Rio de Janeiro, Santa Catarina, Paraíba e Ceará – e verificou um número equivalente a 151 prisões, ao todo. Desses 151 casos, foi possível verificar informações acerca do sexo dos indivíduos presos em 66 deles, sendo 87,9% homens e 12,1% mulheres, com idade média de 35 anos.

[96] ALMEIDA, Emily. Homem é preso por engano em Copacabana. Band News, 2019. Disponível em <https://bandnewsfmrio.com.br/editorias-detalhes/homem-e-preso-por-engano-em-copacabana>. Acesso em 10 de set. de 2021.
[97] Consoante o disposto na Portaria n° 793, de 24 de outubro de 2019, do Ministério de Justiça e Segurança Pública.
[98] NUNES, Pablo. Exclusivo: Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. The Intercept Brasil, 2019. Disponível em <https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/>. Acesso em 10 de set. de 2021.

Percebe-se, pois, que o reconhecimento facial tem se mostrado uma forma de perpetuação de preconceitos, na medida em que apresenta deficiências marcantes no reconhecimento de diversidade fenotípica e de gênero. Com efeito, os estudiosos Joy Buolamwini e Timnit Gebru desenvolveram um projeto denominado "*Gender Shades*"[99] com o propósito de demonstrar essas taxas de erro, testando a precisão de três dos mais relevantes sistemas de reconhecimento facial do mercado: Microssoft, IBM e Face++. Demonstrou-se, por meio do estudo, que homens e mulheres de pele escura estão sujeitos a maiores taxas de erros nos algoritmos de reconhecimento facial em todos os três sistemas, em maior ou menor medida, do que homens e mulheres de pele clara.

As estatísticas são gritantes: a diferença entre as taxas de erro dos dois grupos – pele escura e pele clara – chega a 19,2%. Mulheres de pele escura estão sujeitas a taxas de erro que giram em torno de 20,8% a 34,7%, enquanto homens de pele clara quase não chegam a 0,3% de erro na identificação. Em paralelo, são encontradas falsas correspondências para pessoas de pele escura em 20% dos casos analisados, enquanto isso não ocorre com relação a pessoas de pele clara, que, de acordo com o estudo, não foram identificadas erroneamente nenhuma vez.

Um outro exemplo a ser citado nesse sentido trata da tecnologia de reconhecimento facial implementada no Reino Unido, testada inicialmente na final da *Champions League* de 2018. A polícia forneceu um relatório apresentando os resultados dos testes realizados na ocasião do evento de futebol, tendo sido acionados 2.470 alertas de possíveis suspeitos em tese identificados com o uso das câmeras inteligentes, dos quais apenas 173 foram corretamente reconhecidos. A impressionante taxa de erro foi de 92%[100].

Alguns outros casos emblemáticos não podem passar desapercebidos. Um deles é o Sistema de Crédito Social chinês. Trata-se de uma parceria público-privada baseada no compartilhamento de imagens públicas obtidas em algumas cidades por meio de câmeras dotadas da tecnologia do

[99] Disponível em <http://gendershades.org/overview.html>. Acesso em 10 de set. de 2021.
[100] Relatório "Freedom of Information Request 163/18" fornecido pela política do País de Gales. Disponível em <https://pt.scribd.com/document/377980664/South-Wales-Police?campaign=SkimbitLtd&ad_group=100796X1589915Xb4ad6971b6d92f7c0fdd0439e61e3a08&keyword=660149026&source=hp_affiliate&medium=affiliate>. Acesso em 10 de set. de 2021.

reconhecimento facial com empresas privadas que tenham o Sistema de Crédito Social[101]. As empresas têm acesso ao banco de dados relacionados a infrações e penalizações que o governo da cidade que cedeu as imagens tem e acoplam essas informações como um elemento da base de cálculo para a concessão de crédito ao indivíduo.

Os chineses são avaliados tanto por sua atuação na sociedade quanto pelo comportamento de consumo. Essa avaliação gera a atribuição de uma pontuação aos sujeitos, o que possibilita o seu ranqueamento e lhes confere direito ou não a crédito de compra a depender de suas posições no ranking. Mas, mais do que benefícios de crédito, assustam as restrições impostas a quem tem uma nota baixa: caso o cidadão não se classifique dentro de uma posição limite, é inserido em uma espécie de lista negativa capaz de impedi-lo, por exemplo, de comprar passagens de avião, trem-bala, alugar um apartamento ou conseguir um financiamento para uma casa. Os créditos dos sujeitos são armazenados e, a partir disso, determina-se em que atividades da vida social comunitária essas pessoas poderão participar.

Outro caso a ser destacado é o caso de uma estudante da Universidade Brown erroneamente identificada, via reconhecimento facial, como suspeita procurada em ataque terrorista pela polícia do Sri Lanka[102]. A organização policial divulgou os nomes e fotos de seis suspeitos procurados em conexão com ataques terroristas que mataram centenas de pessoas, solicitando ajuda do público para localizá-los. De alguma forma, uma foto antiga da estudante Amara Majeed chegou aos noticiários ao lado do nome Abdul Cader Fathima Qadiya, uma das suspeitas e, em função da veiculação de sua imagem no noticiário, Amara passou a receber todo tipo de acusação e ameaça em seu perfil no Facebook.

Um exemplo mais próximo se deu no metrô da cidade de São Paulo foi a recente condenação da ViaQuatro, empresa que tem a concessão da linha 4-amarela do metrô de São Paulo, pela captação de imagens por câmeras de reconhecimento facial sem o consentimento dos

[101] SILVEIRA, Janaína Camara da. Você está sendo filmado. Sorria?. Revista Trip, Uol, 2019. Disponível em <https://revistatrip.uol.com.br/trip/os-sistemas-de-reconhecimento-facial-e-monitoramento-na-china>. Acesso em 11 de set. de 2021.

[102] FARZAN, Antonia Noori. Sri Lankan police wrongly identify Brown University student as wanted suspect in terror attack. The Washington Post, 2019. Disponível em <washingtonpost.com/nation/2019/04/26/sri-lankan-police-wrongly-identify-brown-university-student-wanted-suspect-terror-attack/>. Acesso em 11 de set. de 2021.

passageiros. A condenação imposta à empresa pelo Tribunal de Justiça de São Paulo, no valor de R$ 100.000,00 (cem mil reais), responde a uma ação civil pública ajuizada pelo Instituto de Defesa do Consumidor (IDEC) em 2018.

Isso porque a ViaQuatro anunciou a instalação de portas de plataforma interativas em algumas das estações, as quais teriam lentes com um sensor que "reconhece[ria] a presença humana e identifica[ria] a quantidade de pessoas que passam e olham para a tela", com o objetivo de saber a reação dos usuários do metrô às publicidades e informações dispostas na via. Os dados gerados consubstanciar-se-iam na identificação de expressões de emoção, como alegria, raiva, neutralidade, e características gerais a indicar se seria um rosto feminino ou masculino. A empresa não guardava ou armazenava os dados coletados.

A IDEC argumentou que tratar-se-ia de ação ilegal, já que não submetida ao consentimento dos passageiros, sendo que p direito à imagem é garantido pela CF/88 como fundamental. Os usuários não foram advertidos ou comunicados prévia ou posteriormente acerca da utilização ou captação de sua imagem pelos totens instalados nas plataformas, ou seja, os usuários sequer sabiam que estavam sendo monitorados dessa forma.

Por fim, cite-se exemplo que assumiu papel de maior relevância considerando o cenário de pandemia global e migração do ambiente de trabalho para as plataformas virtuais. Juntamente ao do Twitter, o algoritmo de reconhecimento facial do aplicativo Zoom, amplamente utilizado para a realização de videoconferências em tempos de isolamento social, foi duramente criticado por apresentar notáveis falhas ao reconhecer os rostos de pessoas negras[103], o que dá ensejo ao debate acerca da discriminação racial por sistemas de inteligência artificial.

Ao notar a falha apresentada pela plataforma Zoom, que se manifestou com um de seus professores, um homem negro, que estava a usar um pano de fundo virtual, o acadêmico Colin Madland publicou um *tweet* reportando o ocorrido. Em resposta, um porta-voz do Zoom indicou

[103] ANDRADE, Francisca. Onda de contestação cresce por críticas de racismo nos algoritmos de reconhecimento fácil no Twitter e Zoom. SapoTek, 2020. Disponível em <https://tek.sapo.pt/noticias/internet/artigos/onda-de-contestacao-cresce-por-criticas-de-racismo-nos-algoritmos-de-reconhecimento-facial-do-twitter-e-zoom>. Acesso em 11 de set. de 2021.

à imprensa internacional que a companhia estava a investigar o problema, de modo a disponibilizar uma plataforma que fosse inclusiva aos usuários. No entanto, ao revisitar o seu tweet, Colin notou que o algoritmo do Twitter também era tendencioso e dava preferência a rostos brancos a serem destacados na imagem minimizada da *timeline*.

Anteriormente, o Twitter aduzia que o tamanho do conteúdo era propositalmente diminuído para evitar que as imagens tomassem um espaço demasiado na *timeline* dos utilizadores, recorrendo a algoritmos para centrar a atenção nas partes mais importantes da imagem, como rostos ou texto. Uma vez iniciado o debate por Colin Madland, não foram poucas as pessoas colocando a rede social à prova. Nesse contexto é que o engenheiro de infraestruturas e criptografia Tony Arcieri publicou uma série de tweets com os rostos de Mitch McConnell, senador republicano do estado do Kentuky/EUA, e Barack Obama, o ex-presidente norte americano, a cada vez, em posições diferentes.

O resultado foi que o algoritmo escolheu, em todas as vezes, por privilegiar o rosto de McConnell nas miniaturas das fotos. O único caso em que fora privilegiada a foto de Obama se deu em imagem cujas cores encontravam-se invertidas. Vários outros utilizadores das redes sociais, intrigados com o experimento, decidiram por repetir o teste com pessoas e fotos diferentes e acabaram por obter os mesmíssimos resultados.

Executivos do Twitter afirmaram que a plataforma reanalisaria os algoritmos que fazem recortes automáticos em fotos, em que pese testes tenham sido realizados anteriormente apontando a ausência de evidências que indicassem preconceito racial ou de gênero[104]. Os experimentos não científicos consubstanciados na publicação de fotos de pessoas de diferentes tons de pele, ao fim e ao cabo, lançaram luz sobre a necessidade da realização de maiores estudos e análises sobre o algoritmo de reconhecimento facial da rede social em questão.

Ante à grande amostra de casos em que o uso da tecnologia do reconhecimento facial, ainda que não como ferramenta de *surveillance*, é permeada por vieses claramente injustos e

[104] G1. Twitter diz que irá analisar algoritmo de prévia de imagens após queixas de racismo por usuários. G1, 2020. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/2020/09/21/executivos-do-twitter-dizem-que-irao-analisar-possivel-vies-discriminatorio-em-algoritmo-de-previa-de-imagens.ghtml>. Acesso em 11 de set. de 2021.

discriminatórios, verifica-se a necessidade da preocupação com o assunto, que deve ser tratado de forma atenta e delicada, com vistas a resguardar a efetividade dos direitos fundamentais atribuídos aos sujeitos pelo Estado democrático de direito.

CONCLUSÃO

O uso de reconhecimento facial como ferramenta de *surveillance* é, de acordo com o exposto neste trabalho, tecnologia que coloca em risco princípios fundamentais da proteção de dados pessoais, além de infirmar um dos pilares que compõem o entendimento contemporâneo sobre privacidade: a autodeterminação informativa, intrinsecamente atrelada à noção de consentimento dos titulares acerca dos procedimentos aos quais seus dados pessoais são submetidos. É de se dizer que esse cenário de ameaça a direitos fundamentais evidencia, por si só, o atropelo de princípios relacionados ao livre desenvolvimento da personalidade e da dignidade da pessoa humana, garantidos constitucionalmente.

Na verdade, a *surveillance* desenvolvida por vias de câmeras dotadas da tecnologia do reconhecimento facial coloca em xeque qualquer entendimento que se tenha sobre os limites da privacidade, já que desconstituí as divisórias entre as concepções de âmbito público e âmbito privado. Assim, o mero fato de vivermos em sociedade é suficiente para que sejamos objeto de constante vigilância, o que, não raro, é realizado sem que nos seja dada a oportunidade de manifestar consentimento ou mesmo de saber que esse monitoramento está sendo realizado.

Dessa forma, é imprescindível que nos debrucemos sobre os problemas originados da consolidação dessa sociedade de vigilância. E o potencial lesivo da implementação ostensiva dessa tecnologia, cujas origens remontam a teses eugenistas e deterministas e cuja calibração depende de critérios nela inseridos por operadores humanos permeados por vieses potencialmente preconceituosos, reside, principalmente, na utilização das informações pessoais coletadas e agregadas para a construção de perfis individuais ou de grupo.

Frise-se o fato de que diversos estudos têm apontado altas taxas de erro em sistemas de reconhecimento facial, que são mais ou menos gravosos a depender do grupo social ao qual pertence o indivíduo, sendo o mais afetado aquele composto por mulheres de pele negra. A perfilização e a categorização que resultam desse processo iniciado pela identificação dos rostos pela tecnologia do reconhecimento facial são deveras perigosas, visto que, como visto ao longo deste trabalho, jovens, homens e pessoas negras são alvo de maneira sistemática e

desproporcional de sistemas de vigilância sem embasamento em critérios objetivos comportamentais e individualizados e por nenhum motivo especial que não simples suspeitas categóricas que decorrem do fato desses sujeitos pertencerem a grupos sociais específicos. Trata-se de discriminação em sua forma mais crua.

Como largamente exemplificado no ponto 3.1, os sistemas de vigilância – no geral, mas, especificamente, aqueles baseados em tecnologia de reconhecimento facial – não são universais em sua aplicação; são, de outro modo, profundamente permeados por enviesamentos que, a nível algorítmico, são reproduzidos irracionalmente à exaustão, em detrimento de determinados grupos sociais. A esses, é conferido um tipo de tratamento voltado à repressão, à exclusão e à punição. A outros, confere-se um tratamento de privilégio, uma forma de vigilância mais "favorável". De acordo com essa lógica, não há indivíduos bons ou ruins, honestos ou desonestos, pobres ou ricos, mas, simplesmente, indivíduos detentores ou não da possibilidade de acesso e ingresso a determinados lugares, bens e serviços[105], a depender do grupo social ao qual pertencem.

Em vista ao exposto, deve-se refletir sobre o papel do ordenamento jurídico na promoção e defesa de seus valores fundamentais em um cenário em grande parte determinado pela tecnologia – o que pode implicar em reconhecer a insuficiência da dogmática tradicional. Essa dificuldade, traduzida em desafio, pode funcionar como força motriz para o objetivo de aproximar o ordenamento jurídico de um novo perfil da personalidade em uma sociedade que muda com velocidade, e da extensão da participação e influência dos sujeitos no manejo de informações que lhes dizem respeito.

É imprescindível, assim, que seja conferida transparência à coleta e ao tratamento de dados pessoais obtidos como fruto de atividades de vigilância – *in casu*, aquelas permitidas pelo reconhecimento facial. Insta que sejam postas em operação estratégias integradas, capazes de regular a circulação de informações em seu conjunto[106], destacando-se o "direito de acesso", que é, "antes de tudo, um instrumento diretamente acionável pelos interessados, que podem utilizá-lo

[105] NORRIS, C. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge: New York, 2003. p. 247-281.
[106] RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 60.

não somente com a finalidade de simples conhecimento, mas também para promover propriamente a efetividade" da proteção aos dados pessoais dos sujeitos[107].

Enquanto cresce a preocupação político-institucional no tocante à privacidade e à proteção das informações pessoais, verifica-se, em contraponto, uma preocupação com tópicos como a segurança pública e interesses de mercado. Nesse contexto, deve-se repensar a privacidade e a proteção dados como bens sociais para além da dimensão individual, concebendo-as numa perspectiva mais ampla, relacionada aos indivíduos enquanto sujeitos sociais. Surge a concepção dos conceitos de privacidade e proteção de dados como, ao fim e ao cabo, direito de acesso. Rodotà defende, sobre o ponto, que deve ser concedido à pessoa o poder de controle direto e contínuo sobre os coletores de informações, independentemente da existência de uma violação a seus direitos, alterando-se assim a técnica de proteção à privacidade e transformando o cerne da questão no bom funcionamento das regras sobre a circulação de informações *a priori*[108].

O direito de acesso, sob essa perspectiva, configura-se, portanto, como "um instrumento capaz de determinar formas de redistribuição de poder"[109], promovendo o reestabelecimento do equilíbrio entre quem vigia e quem é vigiado. Permitir que o cidadão tenha conhecimento sobre quais tecnologias de informação são empregadas pelo Estado, quais são as práticas de vigilância e como se dá o recolhimento, uso, tratamento e distribuição de seus dados significa, pois, "dar ao cidadão a garantia do exercício do controle social sobre a administração pública"[110], permitindo-lhe condições de reivindicar seus direitos e cobrar do Estado a sua efetividade – exatamente como deve ocorrer em uma sociedade democrática.

É evidente que há muito a se questionar sobre o uso dessas novas tecnologias, que lidam com dados sensíveis, por agentes de segurança do Estado. De outro lado, não se pode negar que o progresso tecnológico, irrefreável, é capaz proporcionar benefícios sociais inimagináveis. Conclui-se, assim, ser crucial ponderar os interesses em jogo, de modo a que sejam assegurados

[107] RODOTÀ, S. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 60.
[108] *Ibid*., p. 60.
[109] *Ibid*., p. 73.
[110] BARROS, Marina; VENTURINI, Jamila. Os desafios do avanço das iniciativas de cidades inteligentes nos municípios brasileiros. *In*: MAGRANI, Eduardo (org.). Horizonte presente: Debates de tecnologia e sociedade. 1ª ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 43.

tanto a garantia aos direitos fundamentais quanto o progresso da sociedade impulsionado pelo desenvolvimento de tecnologias inovadoras, sempre em consonância com a participação pública e com debates abertos sobre as limitações que se mostrarão necessárias para que a implementação das novas tecnologias observe os direitos e garantias conferidos aos sujeitos – até mesmo porque a proteção da pessoa deve ser tida como o valor máximo e alicerce do ordenamento jurídico.

REFERÊNCIAS

ALMEIDA, Emily. **Homem é preso por engano em Copacabana**. Band News, 2019. Disponível em <https://bandnewsfmrio.com.br/editorias-detalhes/homem-e-preso-por-engano-em-copacabana>. Acesso em 10 de set. de 2021.

ALVES, Alan Tiago. **Flagrado por câmera vestido de mulher no carnaval na BA matou homem após vítima passar perto dele de moto em alta velocidade**. G1, 2019. Disponível em <https://g1.globo.com/ba/bahia/carnaval/2019/noticia/2019/03/07/flagrado-por-camera-vestido-de-mulher-no-carnaval-na-ba-matou-homem-apos-vitima-passar-perto-dele-de-moto-em-alta-velocidade.ghtml>. Acesso em 10 de set. de 2021.

ANDRADE, Diego de Calasans Melo; MOURA, Plínio Rebouças de. **O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço**. Revista de Direito, Governança e Novas Tecnologias, Goiânia, v. 5, n. 1, 2019, p. 110-133.

ANDRADE, Francisca. **Onda de contestação cresce por críticas de racismo nos algoritmos de reconhecimento fácil no Twitter e Zoom**. SapoTek, 2020. Disponível em <https://tek.sapo.pt/noticias/internet/artigos/onda-de-contestacao-cresce-por-criticas-de-racismo-nos-algoritmos-de-reconhecimento-facial-do-twitter-e-zoom>. Acesso em 11 de set. de 2021.

ARCAS, Blaise Agüera y; MITCHELL, Margaret; TODOROV, Alexander. **Physiognomy's new clothes**. Blaise Agüera y Arcas, 2017. Disponível em <https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a>. Acesso em 10 de set. de 2021.

BARROS, Marina; VENTURINI, Jamila. **Os desafios do avanço das iniciativas de cidades inteligentes nos municípios brasileiros**. *In*: MAGRANI, Eduardo (org.). Horizonte presente: Debates de tecnologia e sociedade. 1ª ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 31-45.

BATISTA, Gabriel Almeida *et al*. **Sistema de identificação e autenticação biométrica**. 2017. 121f. Atividade supervisionada (Curso de Ciências da Computação) – Universidade Paulista, São Paulo, 2017.

BIONI, B. R. **Proteção de dados pessoais: a função e os limites do consentimento.** Rio de Janeiro: Forense, 2019.

_____ (org.). **Proteção de dados [livro eletrônico]: contexto, narrativas e elementos fundantes**. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado Federal, 1988.

BRASIL. **Decreto n. 10.046**, 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília: Diário Oficial da União, 2019.

BRASIL. **Lei n. 10.406**, 10 de janeiro de 2002. Institui o Código Civil., Brasília: Diário Oficial da União, 2002.

BRASIL**. Lei n. 13.709**, 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Diário Oficial da União, 2019.

CHINOY, Sahil. The racist history behind facial recognition. The New York Times, 2019. Disponível em < https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html>. Acesso em 12 de set. de 2021.

CLARKE, R. A. **Information Technology and Dataveillance**. Communications of the ACM 31, 1988. Disponível em: <http://www. rogerclarke. com/DV/CACM88.html> Acesso em: 07 de maio de 2021.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **A Proteção dos Dados Pessoais como um Direito Fundamental**. Espaço Jurídico. Joaçaba, v. 12, n. 2, jul./dez. 2011, p. 91-108. Disponível em <https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em 9 de set. de 2021.

DONEDA, Danilo; MENDES, Laura Schertel. **Data Protection in Brazil: New Developments and Current Challenges.** *In*: Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges. Springer Netherlands, 2014.

EGGERS, W.; SCHATSKY, D.; VIECHNICKI, P. **AI-augmented government: Using cognitive technologies to redesign public sector work.** [S.l], 2017. Disponível em <https://www2.deloitte.com/insights/us/en/focus/cognitive-technologies/artificial-intelligence-government.html>. Acesso em 9 de set. de 2021.

FARZAN, Antonia Noori. **Sri Lankan police wrongly identify Brown University student as wanted suspect in terror attack**. The Washington Post, 2019. Disponível em <washingtonpost.com/nation/2019/04/26/sri-lankan-police-wrongly-identify-brown-university-student-wanted-suspect-terror-attack/>. Acesso em 11 de set. de 2021.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

FONTES, Giulia. **De olho no monitoramento, Curitiba muda regras para a instalação de câmeras**. Gazeta do Povo, 2019. Disponível em <https://www.gazetadopovo.com.br/politica/parana/de-olho-no-monitoramento-curitiba-muda-regras-para-a-instalacao-de-cameras-dqpfkx5asc5ugd2m49ysd8jni/>. Acesso em 10 de set. de 2021.

FRAZÃO, A. **Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados**. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). Lei Geral de Proteção de Dados Pessoais e suas

repercussões no Direito Brasileiro. 1.ed. São Paulo: Thomson Reuters, 2019, p. 23-52.

FUCHS, Christian. **Como podemos definir vigilância?.** MATRIZES, v. 5, n. 1, 2011.

G1. **Twitter diz que irá analisar algoritmo de prévia de imagens após queixas de racismo por usuários**. G1, 2020. Disponível em <https://g1.globo.com/economia/tecnologia/noticia/2020/09/21/executivos-do-twitter-dizem-que-irao-analisar-possivel-vies-discriminatorio-em-algoritmo-de-previa-de-imagens.ghtml>. Acesso em 11 de set. de 2021.

G1 BA. **Feira de Santana registra 33 prisões por reconhecimento facial durante micareta**. G1, 2019. Disponível em <https://g1.globo.com/ba/bahia/noticia/2019/04/29/feira-de-santana-registra-33-prisoes-por-reconhecimento-facial-durante-micareta.ghtml>. Acesso em 10 de set. de 2021.

GARFINKEL, Simson. **The Death of Privacy in the 21st Century**. Cambridge: O‟Riely, 2000.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face recognition vendor test (FRVT) Part 3: Demographic Effects**. Estados Unidos: National Institute of Standards and Technology, U.S. Department of Commerce, 2019. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Acesso em: 11 de set. de 2021.

HOSANA, Kelly. **Videomonitoramento Inteligente estreia no Réveillon de Salvador**. Secretaria de Segurança Pública da Bahia, 2018. Disponível em <http://www.ssp.ba.gov.br/2018/12/4933/Videomonitoramento-Inteligente-estreia-no-Reveillon-de-Salvador.html>. Acesso em 10 de set. de 2021.

KOCH, MÁRCIO. **Visão computacional para reconhecimento de faces aplicado na identificação e autenticação de usuários na web**, 2012.

KRIEGER, Maria Victoria Antunes. **A análise do instituto do consentimento frente à lei geral de proteção de dados do brasil (lei nº 13.709/18)**. Trabalho de Conclusão de Curso (graduação) – Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, 2019. Data da publicação: 05 dez. 2019. Disponível em <https://repositorio.ufsc.br/bitstream/handle/123456789/203290/TCC.pdf?sequence=1&isAllowed=y>. Acesso em 12 de set. de 2021.

LYON, D. **Surveillance studies: an overwiew**, Cambridge: Polity, 2007.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

NABEEL, F. **Regulating Facial Recognition Technology in Public Places.** Centre for Strategic and Contemporary Research, 2019. Disponível em: <https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places.> Acesso em: 07 de maio de 2021.

NORRIS, C. **From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control**. *In*: LYON, David. Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge: New York, 2003. p. 247-281.

NUNES, P. **Exclusivo: Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros**, The Intercept, 2019. Disponível em: <https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/>. Acesso em: 10 de set. 2021.

PASQUALE, F. **The black box society. The secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015.

RICHARDS, N. M. **The dangers of surveillance**. 126 HARV. L. REV. 1934, 1935, 2013. Disponível em: <https://harvardlawreview.org/wpcontent/uploads/pdfs/vol126_richards.pdf>. Acesso em: 07 de maio de 2021.

RODOTÀ, S. **"Un Codice per l'Europa? Diritti nazionali, diritto europeo, diritto globale"**, in: Codici. 56 Una riflessioni di fine millennio. Paolo Cappellini. Bernardo Sordi (orgs.). Milano: Giuffrè, 2002.

RODOTÀ, S. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

_____ . **Il diritto di avere diritti**. Roma: Laterza, 2012.

SCHNEIER, B. **Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World**. New York: W. W. Notton & Company, 2015.

SILVA, Victor Hugo. **Rio de Janeiro identificou 8 mil pessoas com reconhecimento fácil no Carnaval**. Tecnoblog, 2019. Disponível em <https://tecnoblog.net/289696/rio-de-janeiro-identificou-8-mil-reconhecimento-facial/>. Acesso em 10 de set. de 2021.

SILVEIRA, Janaína Camara da. **Você está sendo filmado. Sorria?**. Revista Trip, Uol, 2019. Disponível em <https://revistatrip.uol.com.br/trip/os-sistemas-de-reconhecimento-facial-e-monitoramento-na-china>. Acesso em 11 de set. de 2021.

SOLOVE, D. **Daniel Solove: Nothing to Hide, Nothing to Fear? Entrevista concedida a Steve Paikin.** Canal The Agenda with Steve Paikin. Disponível em < https://www.youtube.com/watch?v=FqJ8EMwj7zY&ab_channel=TheAgendawithStevePaikin>. Acesso em 26 de maio de 2021.

SOUZA, Thiago Pinheiro Vieira de. **A proteção de dados pessoais como direito fundamental e a [in]civilidade do uso de cookies**. Trabalho de Conclusão de Curso (Bacharelado em Direito) - Universidade Federal de Uberlândia, Minas Gerais, 2018, p. 577.

VU, Brandon. **A Technological and Ethical Analysis of Facial Recognition in the Modern Era**. *In*: A Technological and Ethical Analysis of Facial Recognition in the Modern Era, 2018. Disponível em <https://www.academia.edu/38066258/A_Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era>. Acesso em 11 de set. de 2021.

WARREN, S. D.; BRANDEIS, L. D. **The right to privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, 1890.

WESTIN, Alan. **Privacy and Freedom**. Estados Unidos: Ig Publishing, 2015, p. 65-168.

WRIGHT, E. **The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector**, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 2019.