DOI: https://doi.org/10.23925/ddem.i3.53875

TECNOLOGIAS DE RECONHECIMENTO FACIAL: UM ESTUDO A PARTIR DO CONTEXTO DE VIGILÂNCIA DIGITAL E SUTIL

FACIAL RECOGNITION TECHNOLOGIES: A STUDY FROM THE CONTEXT OF DIGITAL AND SOFT SURVEILLANCE

Elísio Augusto Velloso Bastos[1]
Vitória Barros Esteves[2]

RESUMO
O artigo avalia de que forma as tecnologias de reconhecimento facial se inserem no contexto de vigilância digital e sutil, e quais os riscos sociais ocasionados pelo uso destas ferramentas. Constatou-se que a tecnologia moderna transformou a estrutura da vigilância e possibilitou o aperfeiçoamento dos mecanismos de análise facial. Surgiram novas aplicações para as tecnologias de reconhecimento facial, possibilitando que sirvam "sutilmente" à propósitos vigilantes. Conclui-se pela necessidade de avaliação crítica dos seus usos, principalmente frente aos riscos sociais. Trata-se de uma pesquisa exploratória do fenômeno, com caráter teórico-descritivo e viés qualitativo, que é proposto dentro de uma perspectiva crítico e reflexiva sobre as tecnologias de reconhecimento facial, sendo tal compreensão crítica, alicerçada nos referenciais utilizados, pouco explorada pelas pesquisas que tratam sobre este fenômeno e, assim, possuindo originalidade neste campo de pesquisa. Utiliza-se o método dedutivo, o método de procedimento histórico-comparativo e a técnica de pesquisa da documentação indireta.

Palavras-Chave: Vigilância Digital. Reconhecimento Facial. Tecnologia.

ABSTRACT
The article assesses how facial recognition technologies are inserted in the context of subtle and digital surveillance, and what are the social risks caused by the use of these tools. It was found that modern technology transformed the structure of surveillance and made it possible to improve the mechanisms of facial analysis. New applications have emerged for facial recognition technologies, enabling them to serve "subtly" for vigilant purposes. It is concluded that there is a need for a critical assessment of its uses, especially in the face of social risks. It is exploratory research of the phenomenon, with theoretical and descriptive character and qualitative bias, which is proposed within a critical and reflective perspective on the

[1] Doutor em Direito do Estado pela faculdade de Direito da Universidade de São Paulo (USP). Professor em Direitos Humanos e em Teoria Geral da Constituição (Graduação) e em Teoria da Constituição no Centro Universitário do Estado do Pará- CESUPA. Coordenador do Grupo de Pesquisa Inteligência Artificial, Democracia e Direitos Fundamentais. Procurador do Estado do Pará. Advogado. elisio.bastos@uol.com.br. https://orcid.org/0000-0001-8183-5920.
[2] Mestranda em Ciência Política no Programa de Pós-Graduação em Ciência Política da UFPA. Pós-Graduanda em Direito Digital pelo Complexo de Ensino Renato Saraiva. Membro do Grupo de Pesquisa em Inteligência Artificial e Direitos Fundamentais da Liga Acadêmica Brasileira de Direito do Estado. Advogada. vik_esteves@hotmail.com. https://orcid.org/0000-0003-3914-6499.

technologies of facial recognition, such critical understanding, based on the references used, little explored for research dealing with this phenomenon and thus having originality in this field of research. The deductive method, the historical-comparative procedure method and the indirect documentation search technique are used.

Keywords: Digital Surveillance. Facial Recognition. Technology.

INTRODUÇÃO

A ideia de que a vigilância seria um dos pilares das sociedades modernas já está presente em diversas obras desde o século passado, tendo sido igualmente propalado o imaginário no qual a dominação e o controle de um Estado totalitário são executados por intermédio de instrumentos e ferramentas físicos de vigilância.

Portanto, o processo de vigilância não é um fenômeno novo.

No século XVIII, por exemplo, idealizou-se a estrutura arquitetônica de um prédio, no qual uma única pessoa (chamado de inspetor) pudesse observar vários indivíduos, sem que estes soubessem que estavam sendo vigiados. Trata-se, como se verá adiante, de uma estrutura nomeada e conhecida, posteriormente, como Panóptico.

O poder, precisamente a partir do século XVIII, passa a assumir determinadas configurações, as quais fazem da vigilância hierárquica um dos seus principais instrumentos, passando a ser fundamental para o exercício do poder moderno, junto com a sanção normalizadora e o exame.

Ademais, será, precisamente, a vigilância que permitirá conhecer aqueles que são vigiados e, a partir desse conhecimento, exercer o domínio sobre a pessoa vigiada.

É claro que a sociedade atual difere da sociedade moderna que serviu de modelo para as proposições iniciais sobre a vigilância, mas, suas considerações têm sido ponto de partida importante para os estudos da vigilância.

Contudo, a estrutura clássica de vigilância da atividade policial ainda pressupõe a presença humana física em ambas as extremidades da relação de vigilância, ou seja, em alguém (humano), fisicamente presente, que vigiava e alguém que era vigiado (também humano). Com a expansão das novas tecnologias de informação e comunicação (NTIC), a partir da década de noventa do século XX, e o próprio aumento da capacidade computacional, a configuração dessa relação transforma-se, de modo contundente.

A partir de um caráter teórico-descritivo e viés qualitativo, o objetivo deste artigo será primeiramente entender como funciona esse novo cenário de vigilância sutil e quais os novos

mecanismos de análise da face humana. Por conseguinte, analisar em que medida as atuais tecnologias de reconhecimento facial se inserem nesse contexto. Argumenta-se, ao final, pela necessidade de observação crítica dos riscos gerados pelo uso dessas tecnologias, especialmente em razão dos limitados marcos regulatórios e a potencial violação a um direito de autodeterminação informativa.

1. TECNOLOGIAS DE RECONHECIMENTO INSERIDAS NO CONTEXTO DA VIGILÂNCIA SUTIL

A ideia de que a vigilância seria um dos pilares das sociedades modernas já estava presente em "1984" de George Orwell (ORWELL, 2009). Publicada originalmente em 1949, a distopia futurista tornou-se um clássico literário por ilustrar uma sociedade vigiada, completamente dominada pelo Estado. A frase "O grande irmão está de olho em você" (ORWELL, 2009, p. 12) representa simbolicamente o imaginário do livro, no qual a dominação e o controle de um Estado totalitário são executados por intermédio de instrumentos e ferramentas físicos de vigilância.

No séc. XVIII, por exemplo, Bentham idealizou a estrutura arquitetônica de um prédio, no qual uma única pessoa (chamado de inspetor) pudesse observar vários indivíduos, sem que estes soubessem que estavam sendo vigiados (BENTHAM, 2008 *apud* Fialho, 2017). Essa estrutura ficou conhecida como Panóptico e ganhou notoriedade após a análise de Michael Foucault na obra "Vigiar e Punir". Foucault (1987, p. 225) ao discorrer sobre o panóptico afirma:

> Por isso Bentham colocou o princípio de que o poder devia ser visível e inverificável. Visível: sem cessar o detento terá diante dos olhos a alta silhueta da torre central de onde é espionado. Inverificável: o detento nunca deve saber se está sendo observado; mas deve ter certeza de que sempre pode sê-lo.

Foucault (1996 *apud* BARRICHELLO; MOREIRA, 2015) tornou a vigilância um dos aspectos fundamentais de sua pesquisa. Para ele a vigilância sobre o comportamento dos indivíduos e das populações é uma questão que merece estudo a partir de suas manifestações na Idade Moderna, do final do séc. XVIII até meados do séc. XX. É nesse período que o poder assume determinadas configurações, as quais fazem da vigilância hierárquica um dos seus principais instrumentos.

Para ele, a vigilância passa a ser fundamental para o exercício do poder moderno, junto com a sanção normalizadora e o exame. É a vigilância que permite a produção do conhecimento sobre aqueles que são vigiados. Em outras palavras, vigiar viabiliza a produção do saber, e o saber produzido sobre determinado objeto reforça as possibilidades de exercer poder sobre ele (1996 *apud* BARRICHELLO; MOREIRA, 2015). É claro que a sociedade atual difere da sociedade moderna que serviu de modelo para as proposições de Foucault, mas, suas considerações têm sido ponto de partida importante para os estudos da vigilância.

Os processos de vigilância também sempre estiveram presentes no cenário da atividade policial, especialmente em regimes autoritários, onde os atos cotidianos dos cidadãos eram/são constantemente vigiados por agentes policiais. Contudo, as análises de Bentham e Foucault pressupõem, como dito, a presença humana física em ambas as extremidades da relação de vigilância. Isso muda com a expansão das novas tecnologias de informação e comunicação (NTIC).

Sim, porque, atualmente, os "inspetores" são cada vez menos humanos e a tecnologia assume em grande parte essa função de vigiar, seja por intermédio de tecnologias expressamente anunciadas para este fim, ou de forma mais sutil por meio de monitoradores algorítmicos. No primeiro caso estão inseridas, por exemplo, as câmeras de monitoramento eletrônico (circuito fechado ou circuito interno de televisão) usadas amplamente tanto pelo setor público quanto pelo setor privado, assim como *drones* e dispositivos de segurança. No segundo, temos algoritmos e softwares trabalhando para monitorar, coletar e rastrear dados e informações do ambiente online e das atividades realizadas nele.

Logo, os processos de vigilância tornam-se digitais, onde a posição de "vigilante" é assumida por um objeto tecnológico, frequentemente equipado com um software avançado de coleta e análise de dados. As empresas de tecnologias disputam uma corrida tecnológica para colocarem no mercado objetos cada vez mais "inteligentes".

De celulares que se transformaram em *smarthphones*, das câmeras conectadas à internet, dos objetos de casas inteligentes como a *Alexa* da Amazon, entre outros. E não apenas objetos, mas também plataformas, sites e aplicativos inteligentes que, por meio da coleta de dados, conseguem adaptar-se, melhorar, personalizar. O objetivo anunciado é sempre oferecer a melhor experiência para o usuário. No entanto, não é difícil perceber que essa rede difusa e complexa de aparelhos tecnológicos colabora para que os dados se tornem o insumo primário da vigilância.

Essa conexão com a rede, junto com o aumento da capacidade computacional, transformou as formas tradicionais de se realizar a vigilância, conforme será visto a seguir.

1.1 Vigilância Sutil, *Big Data*, IOT e Hiperconectividade

O termo em inglês *Surveillance* foi criado pelo sociólogo Gary T. Marx em 1984, e desde então se tornou um tema recorrente (LYON, 1995 *apud* FIALHO, 2017). Na concepção tradicional de Marx, a vigilância podia ser definida como observação próxima, particular, de uma pessoa suspeita. Tal conceito recorda as formas de vigilância clássicas exercidas pela atividade policial e espionagem. No entanto, a vigilância moderna, como já dito, abrange cada vez mais tecnologias sofisticadas, capazes de coletar informações pessoais que transcendem barreiras físicas e naturais (distância, luminosidade etc.). Trata-se de uma rede de vigilância generalizada, que não se aplica particularmente a uma pessoa suspeita, mas a contextos, lugares, períodos de tempo, redes, sistemas e categorias de pessoas (NORRIS; ARMSTRONG, 1999 *apud* PEDRO, SZAPIRO, RHEINGATZ, 2015). Além de difusa é também mais sutil e oculta, não necessitando de proximidade física podendo agir inclusive mediante monitoramento remoto (MARX, 2002 *apud* PEDRO, SZAPIRO, RHEINGATZ, 2015).

A vigilância moderna estrutura-se, dessa forma, principalmente em razão da conexão com a internet. Por meio da conexão com a rede tornou-se mais fácil coletar, combinar, armazenar e analisar dados. De certa forma, também vigiar. A sutileza da vigilância moderna está justamente na sua capacidade de ser manter oculta. As pessoas raramente têm conhecimento de que estão sendo vigiadas, quais dados estão sendo registrados e para quais fins. Quando se entra em certo estabelecimento comercial se pode até ver a placa "você está sendo filmado". Já imaginar uma placa ou aviso desse jeito em nossos *smartphones* seria catastrófico. É por isso que Marx (2005, p. 36) denominou essa nova forma de vigilância de "*Soft Surveillance*" ou vigilância sutil. Em suas palavras:

> Yet the culture of social control is changing. Hard forms of control are not receding, but soft forms are expanding. I note several forms of this, from requesting volunteers based on appeals to good citizenship or patriotism to using disingenuous communication to profiling based on lifestyle and consumption to utilizing hidden or low-visibility, information collection techniques.[3]

[3] Tradução livre: No entanto, a cultura do controle social está mudando. As formas rígidas de controle não estão diminuindo, mas as formas flexíveis estão se expandindo. Observo várias formas disso, desde a solicitação de voluntários com base em apelos à boa cidadania ou patriotismo, ao uso de comunicação fraudulenta, a criação de

Sobre a nomenclatura, discorre também Fialho (MARX, 2005 *apud* 2017, p. 07):

> Para Gary, por haver uma forma de exercer controle e vigilância que não seja necessariamente invasiva ao corpo humano (com coleta de DNA ou revistas corporais, por exemplo), a nova vigilância acaba se tornando mais aceitável pela população. Ao haver uma intervenção física no corpo do indivíduo, este ao menos pode perceber e ter noção de que algo está acontecendo com ele, o que não ocorre quando falamos de formas sutis de vigilância, pois conforme Gary "o que não sabemos também pode nos prejudicar". Do mesmo modo as câmeras de vigilância. Por não serem uma forma agressiva de ultrapassar a esfera íntima do indivíduo, este não se "incomoda" com a sua presença (...).

Magrani (2018, p. 96) cita exemplo de como essa sutileza pode ser perigosa. O site *www.insecam.org* disponibiliza filmagens ao vivo de milhares de câmeras de segurança ao redor do mundo, invadidas apenas por ainda possuírem senhas-padrão. Há filmagens de garagens, rodovias, escritórios de empresas, salas de aulas. Segundo o site, o objetivo da exposição não autorizada das imagens é criar um alerta para a privacidade online.

No contexto de vigilância sutil, a perda da privacidade também pode ser feita de maneira voluntária. Atualmente, tende-se a encarar com normalidade a entrega de dados e informações para ambientes difusos de vigilância. Seja essa entrega para acessar plataformas ou serviços, seja para adequar-se às expectativas sociais de participação na vida online. Pariser (2012) comenta que isso pode gerar, inclusive, um fenômeno de aprisionamento dos usuários, os quais já forneceram tantos dados para determinada plataforma que mesmo que um concorrente apresente um serviço melhor não valeria a pena mudar. Por exemplo, se determinado usuário é membro do Facebook, imagine o que representaria para ele mudar para outro site de relacionamento social. Provavelmente demandaria um trabalho enorme de recriar todo o perfil.

Marx (2005) entende que essa voluntariedade no fornecimento de dados é, de certa forma, obrigatória. Pois, como acessar o conhecimento disponível na internet sem estar sujeito ao rastreamento e a coleta? Como transitar por um aeroporto onde funcionam câmeras de vigilância com reconhecimento facial sem estar sujeito aos seus mecanismos de identificação? São poucas as opções de não estar sujeito à um mecanismo de vigilância. Logo, a privacidade deixa de ser a regra para ser exceção. E não raro, ela passa a ser vista também como uma *commodity*, para a qual os dados parecem ser a principal moeda de troca. Cada atividade *online*, e até mesmo as *offline*, deixa "rastros de dados", os quais são armazenados em enormes bancos

perfis com base no estilo de vida e consumo e à utilização de técnicas de coleta de informações ocultas ou de baixa visibilidade (T. MARX, 2005).

de dados. À essa nova realidade, de produção e armazenamento de uma quantidade massiva de dados (estruturados ou não) denomina-se de *big data*. Constantiou e Kallinikos (2015, *apud* ZUBOFF, 2019, p. 19) afirmam que:

> O *big data* anuncia a transformação da sociedade e da economia contemporânea [...] uma mudança muito mais abrangente que faz dos dados que são produzidos na cotidianidade um componente intrínseco à vida institucional e organizacional [...] e um alvo prioritário para estratégias de comercialização [...].

Para que esses dados sejam coletados é necessário criar uma rede de sensores inteligentes, inclusive com aparelhos conectados à internet. Computadores, celulares, televisões, geladeiras são alguns dos dispositivos que já possuem essa capacidade. Dessa forma, há um estado contínuo de hiperconectividade. Esse termo foi cunhado inicialmente para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento (QUAN-HAASE, WELLMAN, 2006 *apud* MAGRANI, 2018), mas hoje descreve também o estado em que as pessoas estão conectadas a todo o momento (*always-on*), a possibilidade de estarem prontamente acessíveis (*readibly acessible*), a interatividade e o armazenamento ininterrupto dos dados (*always recording*) (FREDETTE, 2012 *apud* MAGRANI, 2018). Assim como, as comunicações entre indivíduos (*person-to-person*), indivíduos e máquinas (*human-to-machine*, H2M) e entre máquinas (*machine-to-machine*) (BREWSTER, 2014 *apud* MAGRANI, 2018).

No contexto da hiperconectividade, a coleta de dados não ocorre apenas de objetos, mas também de corpos. São os chamados dados biométricos, biológicos ou genéticos. Empresas de tecnologia procuram investir cada vez mais em *dispositivos e tecnologias* que patrulham o corpo humano procurando por sinais de doença e dispositivos inteligentes para o monitoramento do lar. É um investimento na chamada "internet das coisas" (sigla IOT, derivada do inglês "*Internet of Things*"). A expressão é utilizada para designar a conectividade e interação entre vários tipos de objetos do dia a dia, sensíveis à internet (SANTOS, 2016 *apud* MAGRANI, 2018). IOT, refere-se tanto a objetos quanto a pessoas, assim como aos próprios dados e suas interações no ambiente virtual.

Essa nova arquitetura combinada de hiperconectividade com IOT configura um ubíquo e novo regime que registra, modifica e mercantiliza a experiência cotidiana, desde o uso de um eletrodoméstico até os corpos, tudo com vista a estabelecer novos caminhos para a monetização e o lucro (ZUBOFF, 2019). Toda essa coleta de dados tem um propósito específico: conhecer. Como diz a frase motriz da empresa de tecnologia mais poderosa do mundo no romance

futurista *"O Círculo"* de Dave Eggers (2013, p. 77): "Tudo o que acontece deve ser conhecido". Seja conhecer um usuário, grupo de usuários, ou certos padrões de comportamentos e atividades, o conhecimento servirá como base das estratégias de controle e previsão, para alimentar mercados ou governos. Assim, quanto mais dados os algoritmos tiverem acesso mais eles conseguem se aprimorar, prever e, por que não, controlar. Segundo Hannes Grassegger e Mikael Krogerus (2017, *apud* Magrani, 2018, p. 101):

> Anyone who has not spent the last five years living on another planet will be familiar with the term Big Data. Big Data means, in essence, that everything we do, both on and offline, leaves digital traces. Every purchase we make with our cards, every search we type into Google, every movement we make when our mobile phone is in our pocket, every "like" is stored. (…) "For a long time, it was not entirely clear what use this data could have—except, perhaps, that we might find ads for high blood pressure remedies just after we've Googled "reduce blood pressure.[4]

Outrossim, Harari (2016, p. 342) prossegue e fornece-nos um exemplo da capacidade de aprimoramento e previsão que os algoritmos podem atingir a partir dos dados:

> Um estudo recente encomendado (pelo) (...) Facebook apontou que já em nossos dias o algoritmo do Facebook é melhor do que amigos, pais e cônjuges como juiz de personalidade e disposições humanas. O Estudo foi conduzido com 86 220 voluntários que têm conta no Facebook e que preencheram um questionário com cem itens sobre sua personalidade. Esse algoritmo previu as respostas dos voluntários com base no monitoramento dos likes do Facebook – quais páginas da web, imagens e clipes eles tinham marcado com esse botão. Quanto mais "likes", mais precisas as predições. (...). Incrivelmente, os algoritmos só precisavam de um conjunto de 10 "likes" para superar as predições dos colegas de trabalho, 70 para as dos amigos, 150 para a dos familiares e 300 para se sair melhor do que cônjuges.

Se o curso do desenvolvimento tecnológico mantiver-se minimamente regular, nos próximos anos, o fluxo de informações e dados tornar-se-á ainda mais rápido e a capacidade de processamento será ainda maior. E por necessidade, vontade ou obrigatoriedade, as pessoas irão fazer parte desse fluxo, mesmo que isto signifique perda da privacidade, da autonomia e da individualidade. Diante disso, o processo de vigilância digital acaba por superar a estrutura do

[4] Tradução livre: "Qualquer pessoa que não tenha passado os últimos cinco anos vivendo em outro planeta estará familiarizada com o termo *big data*. Big Data significa, em essência, que tudo o que fazemos, tanto online com offline, deixa vestígios digitais. Cada compra que fazemos com nossos cartões, cada busca que digitamos no Google, cada movimento que fazemos quando nosso telefone celular estará em nossos bolso, cada *like* é armazenado. Especialmente cada *like*. Durante muito tempo, não era inteiramente claro o uso que esses dados poderiam ter – exceto, talvez, que poderíamos encontrar anúncios de remédios para hipertensão logo após termos pesquisado no Google "reduzir a pressão arterial."

panóptico de Bentham. O panóptico constituía-se como uma metáfora adequada para os espaços hierárquicos do local de trabalho (ZUBOFF, 2019).

Mas ao contrário de imaginar uma estrutura panóptica centralizada e física, a estrutura de vigilância contemporânea mostra-se mais virtual, sutil e difusa, principalmente em razão contexto do *Big Data* e do estado de hiperconectividade. O poder vigilante já não pode ser mais resumido por esse símbolo totalitário de comando e controle centralizado. É a partir dessa conjectura de vigilância sutil, hiperconectividade, *Big Data*, objetos inteligentes (sensores) e inteligência computacional, que analisaremos, agora, especificamente, as tecnologias de reconhecimento facial.

2. TECNOLOGIAS DE RECONHECIMENTO FACIAL

Uma das imagens mais recorrentes nos dias subsequentes ao atentado do 11 de setembro, foi a captura de tela de uma câmera de vigilância do Aeroporto de Portland, que mostrava Mohamed Atta, suspeito de ter sequestrado um dos aviões, passando pelo detector de metal do aeroporto. Na época afirmou-se que a utilização da tecnologia certa de reconhecimento facial poderia ter ajudado a evitar os ataques. Segundo essa tese, já existiam sistemas disponíveis comercialmente que poderiam ter checado a imagem do suspeito na lista de terroristas e alertado a segurança do aeroporto (GATES, 2011).

A ideia de que os eventos do 11/09 poderiam ter sido evitados com o uso do reconhecimento facial mostra o potencial desse tipo de tecnologia, mas também já anuncia suas controvérsias mais sensíveis, especialmente para a área da segurança. De setembro de 2001 até hoje o número de sistemas de reconhecimento facial disponíveis no mercado aumentou, assim como, suas diversas aplicações. Temos softwares de reconhecimento oferecidos por grandes marketplaces, como o Rekognition da Amazon. Agências de segurança utilizando reconhecimento facial para identificar criminosos ou procurados. Organizações estatais e não estatais manuseando softwares para identificar vítimas de sequestro e tráfico internacional. Empresas de transporte urbano utilizando biometria facial para autenticar passageiros. Lojas identificando e analisando seus clientes. As aplicações são muitas.

Desde 1960 os softwares já evoluíram e conseguem operar hoje com um volume e complexidade maior de dados. Um dos fatores que possibilitou essa evolução foi a introdução da capacidade de aprender. Aprendizado de Máquina ou *Machine Learning* é uma técnica que orienta o programa a identificar padrões, e a partir daí encontrar respostas para as perguntas que

o orientam. Existem sistemas que já utilizam até algoritmos evolutivos, nos quais o programa busca uma solução otimizada para determinado problema por intermédio da evolução de seu código. Tais algoritmos inspiram-se em mecanismos biológicos como reprodução, mutação e seleção. A incorporação de *Machine Learning* possibilitou que as IA's fracas[5] pudessem aperfeiçoar suas técnicas de reconhecimento facial. Dessa forma, a possibilidade de reconhecimento facial automatizado deixa de ser um ideal tecnocrata, e torna-se uma tecnologia avançada aplicada ao cotidiano.

2.1 Classificação e Funcionamento

Pugliese (2010) insere as tecnologias de reconhecimento facial dentro dos chamados "sistemas biométricos", que possuem como principal funcionalidade escanear as características fisiológicas, químicas ou comportamentais de um indivíduo, com o objetivo de verificar ou autenticar sua identidade. Por sua vez, Wayman (2007) reporta que o termo "biométricos" só começa a ser utilizado na literatura inglesa a partir de 1980, visto que até a década anterior o campo ainda era conhecido como "identificação autônoma de pessoas".

Wayman define biométricos como "o reconhecimento autônomo de indivíduos vivos com base em suas características biológicas e comportamentais, excluindo especificamente os métodos forenses de reconhecimento e os não autônomos" (2007, p. 263). Lee-Morrison (2019) aduz que os sistemas biométricos utilizam tecnologias visuais avançadas, como sensores digitais, para escanear, medir ou capturar partes do corpo, formas e padrões de superfície. O que permite que as tecnologias biométricas determinem a identidade de uma pessoa é o fato do corpo humano possuir partes externas dotadas de singularidade como a impressão digital, a íris e o rosto. O processo de identificação torna-se cada vez mais digital, uma vez que incluiu o uso de algoritmos para ler dados corporais. Essa nova forma digital de identificar pessoas possibilitou a automatizações de certas funções no mercado de trabalho. Hoje, é possível imaginar uma câmera integrada com um computador identificando pessoas em vez de um funcionário parando e exigindo a documentação pessoal de cada indivíduo. Na verdade, esse exemplo nos leva a essencial pergunta de "por que o rosto?"

[5] *Artificial Narrow Intelligence*, IA Restrita, ou IA's fracas, são tecnologias especializadas em apenas uma área específica, com performances que podem facilmente ultrapassar a capacidade humana (MOREIRA, 2017). A terminologia "fraca" não significa diminuição da capacidade, e sim a especialidade em uma área.

Mister considerarmos que o rosto é uma parte do corpo humano fácil e secretamente acessível. Além disso, o reconhecimento a partir do rosto é menos invasivo, demanda uma menor atividade, ou nenhuma, do alvo da identificação, podendo ser feita a distância. Ao contrário de uma coleta de íris ou impressão digital, que exigem não só a aproximação física, mas podem gerar certo incômodo aos indivíduos. Fialho alerta (2017, p. 07) que "por não serem uma forma agressiva de ultrapassar a esfera íntima do indivíduo, este não se "incomoda" com sua presença – quando tem conhecimento de estar sendo vigiado".

Ademais, tais tecnologias também podem ser caracterizadas como tecnologias de captura, eis que frequentemente capturam imagens dos sujeitos. O processo de captura visual permite a criação de um modelo que será confrontado com o banco de dados do software, para verificar ou autenticar a identidade do sujeito em análise (PUGLIESE, 2010). Em sentido estrito, as tecnologias de reconhecimento facial tratam o rosto apenas como um index de identidade, desconsiderando sua expressiva capacidade de comunicação e interação social. Estabelecem seu marco de identidade para então ligar o rosto coletado *(input)* com a sua identidade no mundo real *(output).* Procuram responder a seguinte problemática: "A qual pessoa pertence esse rosto coletado"? É o que se denomina de reconhecimento facial em sentido estrito, ou seja, o reconhecimento apenas da identidade. Por outro lado, a análise automatizada de expressão facial tenta controlar os diversos significados que uma face individual pode transmitir para identificar sinais afetivos, expressões, emoções, humor, etc. Mesmo com objetivos finais diferentes, os primeiros passos da análise automatizada de expressão facial são os mesmos do reconhecimento facial em sentido estrito: detectar uma face e a extração de características (GATES, 2011).

Então, a face humana é, para essas tecnologias, tanto um marco de identidade quanto um local de expressão. Nos últimos anos, há um esforço para investir em computadores, softwares, que possam fazer os dois, isto é, que reconheçam tanto a face humana quanto as expressões faciais, fazendo isso tão bem ou até melhor que os humanos.

A controvérsia sobre se os computadores podem identificar faces e expressões faciais melhores que os humanos reacendem questões filosóficas sobre a própria natureza da visão e da percepção visual, e motivam debates teóricos até hoje no campo da IA. A questão central do teste de Turing "as máquinas podem pensar?" focava na habilidade da máquina de manipular linguagem natural. Hoje, uma pergunta similar podia ser "uma máquina pode ver?". A resposta depende muito do que se considera como "ver".

O processo de enxergar é obviamente um processo fisiológico, mas também uma prática cultural, moldada a partir de elementos culturais e históricos. O que nos leva a outro questionamento, se máquinas podem ver elas necessariamente incorporam modos particulares de ver? ou há um universal, despersonificado, objetivo modo de ver, fora de qualquer estrutura social? Em resumo, a pergunta é: o reconhecimento facial é completamente objetivo ou incorpora formas particulares de ver?

A propaganda veiculada por aqueles que comercializam os softwares é de que essas tecnologias são precisas, objetivas, e que funcionam de forma mais eficiente que a percepção humana. Contudo, esses dispositivos e softwares não nascem espontaneamente, no vácuo. Há um investimento humano para criar essas tecnologias, para fazer com que os computadores vejam. É necessário desenvolver algoritmos que possam digitalizar o mundo analógico dos rostos; criar e desenvolver vastos bancos de imagens faciais para servir de base para a memória visual do computador; desenvolver métodos eficientes de recuperação de imagens; marcar bilhões de imagens com *metadata* para fazer delas algo mais fácil de ser achado; instalar hardwares em espaços físicos; desenvolver interfaces para os usuários dos softwares etc. Sistemas visuais dos computadores são muito limitados pelos propósitos do seu design, **e** sugerir que o modelo de visão computacional é objetivo, oculta as intenções e o trabalho por trás do design, assim como os interesses de quem os produzem (GATES, 2011). Refletir sobre os interesses e objetivos por trás das tecnologias de reconhecimento facial suscita questões complexas, cujas respostas demandariam análises que estão além do panorama deste trabalho. Contudo, tal observação já indica a necessidade de analisá-las de maneira crítica, especialmente levando em consideração os impactos que elas podem gerar na vida das pessoas. A maioria da população ainda tem pouca noção dessa complexa rede de vigilância sutil, e de como ela pode estar mais perto do que se imagina. Há, por exemplo, uma outra forma de fazer com que rostos cheguem como *inputs* para os softwares de reconhecimento: as fotos e selfies nos smartphones.

Vivemos na era das selfies. Elas tornaram-se um elemento corrente no dia de muitas pessoas. Presente em publicações, *stories* ou *status*, as selfies focalizam justamente no rosto dos usuários e estão sendo muito utilizadas junto com filtros. Filtros que dizem qual personagem de um filme você é; que reconhecem seu rosto para aparecer para aplicar cor, tonalidade, arte; quantos anos você tem; e até mesmo qual sua orientação sexual. Assim, o fato é que o reconhecimento facial já se tornou bem difundido nas principais redes sociais. Desafios online como o "*10 year challenge*" têm sido acusados de treinar mecanismos de reconhecimento facial (MOGNON, 2019). O Facebook, recentemente, havia começado a

utilizar mecanismos de reconhecimento para identificar o usuário da plataforma em fotos não marcadas. Funcionava assim: se o software de reconhecimento identificasse seu rosto em uma foto postada, e você não estivesse marcado nela, o Facebook lhe enviava automaticamente uma notificação de aviso com uma mensagem similar a "você supostamente aparece nessa foto, deseja realizar marcação?" ou antes mesmo da pessoa postar a foto, a plataforma já identificava o rosto e realizava a marcação.

Contudo, em setembro de 2019, o próprio Facebook anunciou que as sugestões de *tags* automáticas foram desativadas, sendo a ferramenta de reconhecimento facial uma opção a ser utilizada ou não pelo usuário[6]. A desativação do mecanismo ocorreu após o 9º Tribunal de Apelações dos Estados Unidos ter decidido que o Facebook enfrentaria uma ação coletiva sobre essa suposta violação da privacidade. A rede social também teve problemas durante a investigação realizada pela Federal Trade Commission (FTC) sobre as práticas de privacidade da empresa. Em 2019, a empresa acordou com a FTC uma multa recorde de US$5 bilhões e novas salvaguardas de privacidade, incluindo a exigência de que o Facebook obtenha consentimento afirmativo dos usuários antes de usar a tecnologia de reconhecimento facial (BIRNBAUM, 2019).

Em que pese essa funcionalidade do Facebook estar agora como opcional aos usuários, ela mostra que os mecanismos de reconhecimento facial não estão mais limitados às câmeras de vigilância. Os *smarthphones, tablets*, tvs, e todos aqueles dispositivos com capacidade de captura de imagem e vídeo, se adaptados com o software certo, ou com a funcionalidade de determinada plataforma, podem transformar-se em aparelhos vigilantes da face humana. Além disso, funções disponíveis como filtros no Instagram mostram que o reconhecimento não se limita mais a softwares completos, difíceis de manusear. Estão cada vez mais próximo dos usuários, presentes no dia-a-dia. Vejamos alguns exemplos recentes de tecnologias de reconhecimento facial.

3. USOS E APLICAÇÕES RECENTES

3.1 Amazon Rekognition

Como um das maiores *marketplaces* do mundo, a Amazon disponibiliza comercialmente seu software de reconhecimento facial chamado "*Amazon Rekognition*". O software é um entre

[6] Publicação do próprio Facebook na sua página: https://about.fb.com/news/2019/09/update-face-recognition/.

os muitos serviços disponibilizados pela Amazon Web Services, plataforma da empresa especializada em serviços de computação e dados. Sobre o Rekognition, a Amazon garante:

> [...] O Amazon Rekognition consegue analisar atributos como olhos abertos ou fechados, humor, cor do cabelo e geometria visual do rosto. Esses atributos de detecção são cada vez mais úteis para clientes que precisam organizar ou pesquisar milhões de imagens por segundo usando tags de metadados (por exemplo, feliz, óculos, faixa etária) ou identificar alguém (ou seja, reconhecimento facial usando uma imagem de origem ou um identificador exclusivo). Os rostos são comparados com base na geometria visual, incluindo as proporções entre os olhos, o nariz, as sobrancelhas, a boca e outras características faciais. Quando as imagens são analisadas pelo Amazon Rekognition, é criado um contorno ao redor do rosto chamado de caixa delimitadora. Ela define a única parte da imagem que o Rekognition analisa. Depois disso, a análise cria números de notação de objeto para a imagem, indicando a "localização" dos principais elementos do rosto. Quando os clientes realizam uma pesquisa de rosto, a tecnologia compara os dados da imagem original com cada uma das imagens pesquisadas. Por meio disso, o serviço atribui uma pontuação de similaridade a cada rosto da imagem. Essa abordagem garante que o Amazon Rekognition não retenha qualquer informação sobre a identidade da pessoa, somente o cálculo de semelhança entre um rosto e outro.

De acordo com a classificação de Gates (2011) o software da Amazon possui dupla função: a do reconhecimento facial em sentido estrito e da análise automatizada da expressão facial. Isso porque consegue determinar a identidade de um rosto, assim como, identificar expressões como humor. Sobre a primeira função, de reconhecimento em sentido estrito, a Amazon afirma que é criado um contorno ao redor do rosto chamado caixa delimitadora, a qual define a única parte da imagem analisada pelo Rekognition. Depois são criados números de notação, indicando a localização dos principais elementos do rosto. A partir daí, comparam-se os dados, e atribui-se uma pontuação de similaridade, fazendo um cálculo de semelhança entre o rosto que se quer identificar e aqueles do banco de dados.

Algumas considerações importantes que podemos extrair das informações da Amazon: a primeira refere-se ao salto evolucional desses softwares. Se pensarmos nos primeiros mecanismos de reconhecimento, onde a maior dificuldade ainda era separar o rosto dos outros elementos da imagem, o avanço é gigantesco. A segunda refere-se ao cálculo de semelhança, que mostra que esses softwares trabalham com cálculos matemáticos operadas por algoritmos complexos e eficientes. O que não quer dizer que sejam infalíveis. Erros podem aparecer no cálculo de semelhança, sendo que mesmo com a indicação de uma pontuação alta de similaridade, a identificação pode não estar correta.

Por fim, os softwares mais avançados deixam de ter a face como único ponto de análise. Por exemplo, os recursos do Rekognition que focam no rosto são: *detecção e análise de faces*, *pesquisa e confirmação de faces* e *reconhecimento de celebridades.* Mas além da face, o Rekognition já possui recursos de rótulos para identificar objetos (por exemplo, bicicletas, telefones, edifícios) e cenas (estacionamento, praias, cidades).

O Rekognition é um serviço pago, possuindo uma tabela de valores a depender do tipo de utilização do software. Por isso, algo a se ponderar, principalmente em relação aos softwares de reconhecimento facial, é qual o público-alvo dessas tecnologias. Pelo valor cobrado, estima-se que o público seja pessoas, organizações governamentais, empresas de médio a alto poder aquisitivo. Como divulgado no próprio site, alguns dos clientes do Rekognition são NFL, CBS, PopSugar e o Washington County Sheriff Office[7]. Sendo um dos softwares mais conhecidos, o Rekognition sofre duras críticas, principalmente em relação à sua resposta a determinados gêneros e etnias.

No começo de 2019, pesquisadores do MIT constataram que o Rekognition falhava em determinar com segurança o sexo de rostos femininos e de peles mais escuras, em cenários específicos. Os autores do estudo afirmaram que, em experimentos realizados em 2018, a análise facial do Rekognition identificou erroneamente fotos de mulheres como homens em 19% das vezes, e mulheres de pele mais escura como homens em 31% das vezes. Em comparação, o software da Microsoft determinou mulheres de pele mais escura classificadas como homens em apenas 1,5% das vezes (WIGGERS, 2019). No documento com a íntegra do estudo, Raji e Buolamwini (2019), ressaltam a importância de se realizar essas auditorias algorítmicas com vistas a expor desvios sistemáticos nesses softwares. Destacam:

> [...] outside of the capitalist motivations of economic benefit, employee satisfaction, competitive advantage, social pressure, and recent legal developments like the EU General Data Protection Regulation, corporations still have little incentive to disclose details about their systems (DIAKOPOULOS; BURRELL, 2016; WACHTER; RUSSELL, 2018 *apud* RAJI; BUOLAMWINI, 2019, p. 01)[8].

[7] Nos Estados Unidos, a primeira agência policial a utilizar o Rekognition foi o Washington County Sheriff Office, em 2017. Em três anos de utilização, surgiram questionamentos sobre o custo dos gastos públicos com tal serviço, a ausência de uma regulação específica para o uso de algoritmos na atividade policial e principalmente as graves consequências de um reconhecimento errôneo. Em junho de 2020, o Washington County Sheriff Office anunciou pausa na aplicação do software.

[8] Tradução livre: fora das motivações capitalistas de benefício econômico, satisfação dos funcionários, vantagem competitiva, pressão social e desenvolvimentos legais recentes como o Regulamento Geral de Proteção de Dados da UE, as empresas ainda têm pouco incentivo para divulgar detalhes sobre seus sistemas (Diakopoulos; Burrell, 2016; Wachter; Russell, 2018 *apud* Raji; Buolamwini, 2019, p. 01).

De fato, as empresas de tecnologia consideram os seus algoritmos como verdadeiros segredos industriais. E sob o argumento de que a abertura para análise pode gerar riscos à segurança, as empresas têm tido pouco incentivo para permitir auditorias algorítmicas. Em um discurso que demonstra essa noção, um detetive da equipe do Washington County Office afirmou que "(...) assim como qualquer uma de nossas técnicas de investigação, nós não contamos para as pessoas como nós as pegamos"[9], se referindo aos questionamentos sobre a agência só ter anunciado oficialmente nove prisões relacionadas a utilização do software da Amazon (HARWELL, 2019).

No Brasil, o movimento ainda é em direção à aquisição desse tipo de software, sobre promessas, principalmente, de melhorar a segurança pública nos grandes centros urbanos, conforme se verifica na seção a seguir.

3.2 Agências de Segurança: polícia estadunidense e polícia brasileira

Notícia sobre uso de tecnologias de reconhecimento facial pela polícia brasileira:

> No carnaval de 2019 o sistema de reconhecimento facial da polícia baiana localizou e prendeu um criminoso fantasiado de mulher no circuito Dodô. A polícia do Rio de Janeiro, em 2018, contratou o sistema britânico "Facewatch" com o propósito de identificar 1.100 criminosos ao cruzarem as câmeras de segurança; (...). Inúmeros casos têm sido relatados globalmente sobre erro de identificação, alguns com danos relevantes como o recente caso no Rio de Janeiro (julho/2019): uma mulher foi detida por engano em Copacabana e levada à delegacia do bairro, após as câmeras de reconhecimento facial darem positivo. A potencial ameaça à privacidade tem suscitado fortes reações contrárias. Em 14 de maio último, São Francisco tornou-se a primeira cidade dos EUA a proibir o uso dessa tecnologia pela política e outros órgãos da administração (KAUFMAN, 2019).

O uso das tecnologias de reconhecimento facial pelas agências de segurança talvez seja a utilização mais controversa. Em partes porque errar na identificação de uma celebridade em um filme é bem menos nocivo que imputar um crime a alguém com base em um reconhecimento errôneo. Desde a década de noventa algumas agências policiais estadunidenses começaram a adquirir e implantar os softwares de reconhecimento comercialmente disponíveis à época. Contudo, hoje se vê um movimento muito mais de desconfiança e proibição do uso desse tipo de equipamento.

[9] Tradução de: "(...) just like any of our investigative techniques, we don't tell people how we catch them" (Harwell, 2019).

Em 2019, por exemplo, São Francisco, Oakland e Califórnia proibiram o uso de reconhecimento facial pelas agências públicas, e em junho de 2020, o Washington County Sheriff Office anunciou pausa na aplicação do software. Tal desconfiança deve-se às questões de privacidade, ao gasto público com tal equipamento, aos erros noticiados, e em geral à própria consciência quanto à complexidade e perigos dos sistemas de vigilância sutil.

No Brasil, o movimento ainda é em direção à aquisição desse tipo de software, sobre promessas de melhorar a segurança pública, especialmente nos grandes centros urbanos. Perguntas como "de que maneira está sendo adquirido e implantado esses softwares? quais bancos de dados estão sendo utilizados? quais os resultados e o acesso para possíveis auditorias?" fazem parte de uma inquietação que devem ser trabalhadas nos próximos anos. Mas não é só.

Muito se tem argumentado que, devido às consequências que poderão advir do seu uso na segurança pública, é necessário haver uma análise humana posterior ao reconhecimento. Isso significa que, em casos em que a tecnologia reconhece determinada pessoa como suspeito ou acusado, é indispensável que haja uma revisão humana posterior, para evitar que o reconhecimento autônomo seja prova finalística.

O Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR/EU/2016/679) prevê, em seu artigo 22, o direito do titular dos dados de não estar sujeito a uma decisão baseada apenas no processamento automatizado, e destaca a figura do controlador como aquele que, prioritariamente, deve realizar a intervenção humana. Além disso, destaca que em casos que envolvam dados biométricos, por se tratar de um dado de categoria especial, o direito à revisão não pode ser afastado. Os softwares de reconhecimento facial trabalham justamente com a categoria de dados biométricos. Por isso, não se pode afastar de alguém, que, eventualmente, sinta-se prejudicado pelos efeitos de decisão tomada por um mecanismo automatizado de reconhecimento, a possibilidade de pedir sua revisão.

No entanto, diferentemente do Regulamento Europeu, a Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD, Lei nº 13.709/2018)[10] não prevê o direito de revisão humana das decisões baseadas no processamento automatizado. Na redação originária da LGPD (2018), o art. 20 era composto por um parágrafo terceiro, que determinava, expressamente, que a revisão

[10] De forma geral, a LGPD (2018) enumera as regras que devem ser observadas para o tratamento de dados pessoais no Brasil, tanto por pessoas naturais ou por pessoas jurídicas de direito público ou privado e define dados pessoais como todas as informações relacionadas a uma pessoa natural, identificada ou identificável. Sendo o tratamento qualquer operação realizada com esses dados, como coleta, transmissão, processamento, arquivamento, avaliação, eliminação, reprodução, entre outras.

de decisões automatizadas deveria ser feita por uma pessoa natural e não por um algoritmo. Sucede que tal dispositivo foi vetado pela Presidência da República e seu veto mantido pelo Congresso Nacional. A LGPD (2018) também categoriza dados biométricos como dado pessoal sensível[11]. Assim, de acordo com os parâmetros estabelecidos pela LGPD, a operação realizada pelas tecnologias de reconhecimento facial na Bahia e no Rio de Janeiro podem ser consideradas como tratamento de dados pessoais sensíveis, uma vez que coletam e analisam dados biométricos ligados a uma pessoa natural. No que diz respeito aos dados sensíveis, Bioni (2020) lembra que seu conteúdo oferece uma especial vulnerabilidade: a discriminação.

E não há no Brasil (até a edição deste trabalho), o direito do titular de solicitar a revisão humana da decisão automatizada de reconhecimento, mesmo diante dessa especial vulnerabilidade. Isso implica que, determinado cidadão, ao ser reconhecido pelo software, se desejar questionar o reconhecimento, não há a obrigatoriedade da agência de segurança de realizar uma revisão humana. Adota-se, pois, uma decisão tão potencialmente tautológica, quanto meramente formal: a revisão de decisão proferida por uma máquina pode ser feita por outra máquina, que, em rigor, poderá ter sido concebida pelas mesmas pessoas e dentro dos mesmos critérios e vieses presentes nos algoritmos que produziram a primeira decisão desfavorável. Essa ausência de revisão impede que o titular do dado exerça o seu direito de autodeterminação informativa.

Este direito tem origem na proteção da intimidade[12]. Do ponto de vista tradicional o direito à intimidade protege a capacidade de autodeterminação pessoal e familiar, garantindo a não interferência de terceiros nos espaços privados e no plano de vida dos indivíduos (PÉREZ, 2008). Contudo, a partir do momento em que as sociedades se tornaram mais complexas, especialmente com o avanço das tecnologias, a possibilidade de exposição da intimidade a níveis e formas antes inconcebíveis fez surgir a necessidade de uma nova compreensão do que seria o íntimo.

A intimidade não poderá mais ser entendida apenas em seu aspecto negativo, clássico, ou seja, como "direito ao isolamento, ao confinamento a si mesmo, ao poder de retirar-se virtual e provisoriamente do mundo e pôr-se dentro de si", como assevera Morente (1935, *apud* LUÑO, 2005, p. 355), ou mesmo a "pretensão, liberdade, poder e imunidade de dispor de um âmbito

[11] Art. 5º, II da LGPD (BRASIL, 2018).
[12] O presente trabalho adota as expressões privacidade e intimidade como expressões cujo âmbito normativo é equivalente, ou cuja diferença sutil não justifica tratá-los como algo diverso. Isso dizer que, mesmo quando a distinção é feita, ela não consegue se revelar materialmente relevante, sendo apenas uma questão de aprofundamento material.

de vida pessoal subtraído de qualquer tipo de intromissão perturbadora ou, simplesmente, indesejadas", no dizer de Hohfeld (1913, *apud* LUÑO, 2005, p. 356).

A tal aspecto negativo, é mister que se inclua uma concepção ativa ou dinâmica, pelo que a intimidade também passa a abranger o direito de conhecer, acessar e controlar as informações que dizem respeito, que são relevantes a cada pessoa (LUÑO, 2005). Trata-se do núcleo da autodeterminação informativa, o qual já se encontra previsto como fundamento específico da disciplina de proteção de dados pessoais no Brasil, conforme art. 2º, II, da LGPD, enquanto aspecto básico da intimidade.

O conceito diz respeito à capacidade do indivíduo de gerenciar seus próprios dados, especialmente em casos de graves consequências, como investigações ou persecuções criminais que envolvam identificação de um indivíduo pelo reconhecimento facial. Entre os requisitos citado por SOLOVE (2013) está justamente a (i) a exigência de transparência do sistema de registro dos dados, (ii) o direito de corrigir os dados e a (iii) responsabilização dos utilizadores dos dados, em caso de uso indevido. Devendo-se pensar também na exigibilidade de uma devida reparação e ratificação das identificações realizadas de forma errônea.

O STF (2020), por ocasião do julgamento das ADIs propostas em face da Medida Provisória 954/2020 incorporou a necessidade de tutela eficiente da autodeterminação informativa. A MP 954/2020 determinava o compartilhamento de dados pessoais de brasileiros ao IBGE para a finalidade de produção estatística. No julgamento, o STF conclui que a MP 954/2020 não observou os limites constitucionais e legais de proteção à intimidade e ao direito à autodeterminação informativa, à medida que não indicou os mecanismos protetivos necessários ao compartilhamento, assim como não forneceu aos usuários de telefonia a opção de autorizar ou não a transferência dos dados para o IBGE. A decisão que cessou os efeitos da MP já indicou o status fundamental das garantias relativas à proteção de dados pessoais e estabelece um novo horizonte paradigmático para eventuais casos de reconhecimento errôneo automatizado.

O paradigma é de que cada vez mais, seja reconhecido a importância do direito à autodeterminação informativa, especialmente considerando o direito das pessoas de controlarem não só a captura de seus dados, mas o uso, a avaliação, e quaisquer outras operações de tratamento, especialmente se estas são resultantes de procedimentos de vigilância sutil.

3.3 Caso Hering e igrejas

O âmbito privado também tem sido objeto de utilização das tecnologias de reconhecimento facial, principalmente no mercado consumidor. Em 2019, a Hering foi investigada por possível coleta de dados de clientes sem autorização prévia via tecnologia de reconhecimento facial. Conforme notícia jornalística (SILVA, 2019):

> O processo (...) avalia o uso inadequado dessas informações a partir de recursos de personalização presentes na loja Hering Experience, inaugurada no fim de 2018 em São Paulo. Ao que tudo indica, uma das habilidades do sistema seria usar reconhecimento facial para exibir a reação dos clientes diante de roupas, calçados e acessórios vendidos pela marca. Assim, a empresa poderia monitorar esses detalhes para promover publicidade segmentada futuramente. Procurada para demais esclarecimentos, a Hering negou a acusação e declarou que "não realiza reconhecimento facial, mas sim detecção facial, por meio da qual estima apenas o gênero, a faixa etária e o humor dos consumidores de forma anônima". Ainda ressaltou que os dados não seriam tratados, armazenados ou compartilhados de modo externo, sendo considerados como meramente estatísticos.

Não é correto afirmar que não se realiza "reconhecimento facial e sim detecção facial". Analisar o gênero e a faixa etária dos consumidores encontra-se dentro do reconhecimento facial em sentido estrito. Já a análise do humor dos clientes estaria dentro da análise automatizada de expressão facial. Ademais, a ressalva de que os dados não seriam "tratados" não condiz com a perspectiva de tratamento adotada tanto pelo GDPR quanto pela LGPD, uma vez que a simples coleta já é considerada dentro da operação de tratamento devendo ser respeitado todos os direitos e proteções especiais aos dados, principalmente em se tratando de dados sensíveis como os biométricos[13]. E segundo a LGPD, em seu art. 11, I, o tratamento de dados sensíveis somente pode ocorrer com o consentimento específico e destacado do titular, o que não era realizado pelos consumidores da Hering. O serviço de análise automatizada de expressão facial também tem sido oferecido para igrejas:

> Em outubro, foi realizada a 15ª ExpoCristã em São Paulo. Entre shows, simulações virtuais e editoras, duas empresas se destacaram com produtos tecnológicos semelhantes. A Kuzzma, empresa (...) estrangeira, e a brasileira Igreja Mobile apresentaram a ideia de reconhecimento facial para igrejas. A tecnologia utiliza uma câmera comum para registrar as imagens e enviar para um computador capaz de reconhecer rostos e mais informações pessoais. "Conseguimos definir a assiduidade do usuário, contagem de pessoas, humor do usuário", explicou o diretor de desenvolvimento da Igreja Mobile, Luís Henrique Sabatine. (PRETA, 2019).

[13] Nesse sentido, veja-se o art. 5o, incisos II e X, da LGPD e o art. 4º, da GDPR.

O oferecimento de serviços de análise automatizada da expressão facial está intrinsicamente ligado aos métodos de personalização. Para personalizar serviços, produtos ou plataformas é necessário conhecer as pessoas (usuários, consumidores, fiéis etc.). Conhecer suas emoções, seus comportamentos. Em ambas as notícias, o conhecimento é produzido por meio do software de reconhecimento facial. Assim, a personalização já não se limita às ofertas de propaganda. Ela encontra-se nos mais diversos ambientes, físicos ou virtuais. É uma parte da própria finalidade do contexto de vigilância sutil.

Schneier (2020) afirma que, em regra, os sistemas modernos de vigilância de massa operam com três dinâmicas: identificação, correlação e discriminação. E os três casos citados anteriormente não fogem desta asserção. Apesar da LGPD já vigorar no Brasil, é necessário que haja regras mais claras sobre como o indivíduo exercerá efetivamente seu direito de acesso, o controle da movimentação de seus dados, à luz de um direito a autodeterminação informativa.

E sobre o panorama regulatório, no contexto da América Latina, o Brasil não está tão desigual. Em um estudo sobre reconhecimento facial na América Latina (Argentina, Brasil, Chile, Colômbia, Costa Rica, México, Nicarágua, Panamá, Peru, República Dominicana, Uruguai), Franqueira, Hartmann e Silva (2021) concluíram que predominantemente, nesses países, a regulação de sistemas de reconhecimento facial é exclusivamente com base na previsão normativa sobre proteção de dados, e que não há regras distintas para cada área. Por exemplo, segurança pública, âmbito privado e/ou de consumo, trabalhista/corporativo etc. Esses e outros ambientes, virtuais ou não, estão sob as mesmas exigências gerais.

Apesar do Legislativo, estar na vanguarda do tema, é fundamental que o Judiciário, e outros órgãos como Ministério Público e Defensoria Pública, promovam medidas de enfrentamento e debate sobre os riscos desse tipo de tecnologia, especialmente frente aos casos de discriminação. Em especial, é preciso que esse debate seja contextualizado para que indivíduos de grupos vulnerabilizados estejam devidamente protegidos da atuação invasiva, errônea ou discriminatória de entes públicos e privados. Tais contextualizações incluem também discussões amplas sobre quais locais estão sendo colocadas essas tecnologias e até como viabilizar o acesso do cidadão que deseja questionar o uso de seus dados biométricos.

CONCLUSÃO

Alguém acorda e pega o celular desbloqueando-o por meio do reconhecimento facial. Sai na rua e é observado por câmeras de vigilância. Acessa o transporte público e utiliza a biometria facial. Entra em uma loja, gosta de determinada roupa e seu humor é coletado por câmeras. Essa é a realidade contemporânea das tecnologias reconhecimento facial. Mais do que uma representação mística de objetos em um Estado totalitário vigilante, os mecanismos de reconhecimento fazem parte da realidade das pessoas, inclusive no Brasil.

Com a estrutura difusa e generalizada de aparelhos conectados à internet, a vigilância tornou-se muito mais sutil, operando sem alardes e "aparentemente" sem intervenções físicas. A capacidade e a inteligência computacional foram ampliadas o que possibilitou a criação de softwares complexos capazes de reconhecer rapidamente um rosto, de identificar objetos, padrões e cenários.

Entender essa nova realidade e suas implicações demanda pesquisas em áreas multisetoriais, onde as perspectivas técnica e humana possam dialogar, especialmente nos casos em que o uso tecnologia possa implicar em decisões e restrições sociais. Esforços devem ser feitos, por governos e empresas, para que os indivíduos sejam protegidos do uso predatório e enviesado de seus dados pessoais, especialmente os sensíveis. Esforços devem ser feitos também para viabilizar a realização de auditorias algorítmicas, como o importante trabalho citado dos pesquisadores do MIT. Tais auditorias possibilitarão a crítica e a revisão desses mecanismos para padrões mais justos.

Ademais, como se sabe, a tecnologia é fruto de operações estritamente racionais e objetivas de um plano abstrato e, nessa qualidade, atende interesses sociais e econômicos, contextos e padrões daqueles que a produzem, assim como daqueles que a consomem.

Por isso, uma inquietação que deve se tornar uma questão de pesquisas futuras é de como essas tecnologias estão sendo utilizadas e adaptadas no Brasil? Os bancos e operações de dados estão respeitando os padrões nacionais e internacionais?

Além disso, os estudos brasileiros são quase uníssonos em admitir que se excluem dos usuários cotidianos da tecnologia milhões de pessoas que ainda tem acesso precário à internet e aos equipamentos tecnológicos. As próprias tecnologias de reconhecimento facial têm mais predominância no cenário urbano, onde a própria estrutura de rede e de internet permite essa propagação.

Assim, necessário avaliar, criticamente, as tecnologias de reconhecimento facial, especialmente frente aos seus riscos sociais.

REFERÊNCIAS

AMAZON REKOGNITION. Disponível em: https://aws.amazon.com/pt/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/. Acesso em: 20 de janeiro de 2020.

BARRICHELLO, Eugenia Maria Mariano da Rocha, MOREIRA, Elizabeth Huber. A análise da vigilância de Foucault e sua aplicação na sociedade contemporânea: estudo de aspectos da vigilância e sua relação com as novas tecnologias de comunicação. **Intexto**. Porto Alegre. UFGRS, PPGCOM, n. 33, p. 64-75. 2015. Disponível em: https://seer.ufrgs.br/intexto/article/view/50075. Acesso em: 20 de janeiro de 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento**.** 2ª Ed. Rio de Janeiro: Editora Forense, 2020.

BIRNBAUM, Emily. **Facebook ends facial recognition photo tagging suggestions.** Disponível em: https://thehill.com/policy/technology/459771-facebook-ends-facial-recognition-photo-tagging-suggestions. Acesso em: 19 de janeiro de 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 13 julho 2020.

BRASIL. **Medida provisória nº 954,** de 11 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 11 de abril de 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 19 agosto 2020.

EGGERS, Dave. **O Círculo**. São Paulo: Editora Companhia das Letras, 2014.

FIALHO, Yrana Miranda. **Big Brother is watching you: Do "1984" de George Orwell às câmeras de vigilância presentes na contemporaneidade.** Artigo disponível em: http://www.pucrs.br/direito/wp-content/uploads/sites/11/2018/03/yrana_fialho_20172.pdf. Acesso em: 16 de janeiro de 2020.

GATES, Kelly A. **Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance**. New York: New York University Press, 2011.

Hardwell, Drew. **Oregon became a testing ground for Amazon's facial-recognition policing. But what if Rekognition gets it wrong?** The Washigton Post, 2019. Disponível

em: Amazon's facial-recognition AI is supercharging police in Oregon. But what if Rekognition gets it wrong? - The Washington Post. Acesso em: 13 março de 2020.

INIOLUWA, Deborah Raji; BUOLAMWINI, Joy. **Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products.** Disponível em: https://www.media.mit.edu/publications/actionable-auditing-investigating-the-impact-of-publicly-naming-biased-performance-results-of-commercial-ai-products/. Acesso em: 20 de janeiro de 2020.

KAUFMAN, 2019. **Alerta: as tecnologias de reconhecimento facial estão nos ameaçando.** Disponível em: https://epocanegocios.globo.com/colunas/IAgora/noticia/2019/10/alerta-tecnologias-de-reconhecimento-facial-estao-nos-ameacando.html. Acesso em: 20 de janeiro de 2020.

LE DANDA, Manuel. **War in the of Intelligent Machines**. New York: Zone Books, 1991.

LEE-MORRISON. Lila. **Portraits of Automated Facial Recognition: On Machinic Ways of Seeing the Face.** Transcript Verlag, 2019. Ebook. Disponível em: https://www.transcript-verlag.de/978-3-8376-4846-1/portraits-of-automated-facial-recognition/. Acessado em: 16 de janeiro de 2020.

LUÑO, Antonio Enrique Perez. **Derechos Humanos, Estado de Derecho y Constituicion.** Madrid: Tecnos, 2005.

MAGRANI, Eduardo. **A internet das coisas**. 1ª edição. Rio de Janeiro: Editora FGV, 2018.

MARX, Gary T. **Soft Surveillance: Mandatory Voluntarism and the Collection of Personal Data.** Dissent, Fall 2005, v. 52, n. 4, p. 36-43.

MOGNON, Mateus. **Desafio dos 10 anos' pode treinar sistemas de reconhecimento facial.** Disponível em: https://www.tecmundo.com.br/ciencia/137950-desafio-10-anos-treinar-sistemas-reconhecimento-facial.htm. Acessado em: 22 de janeiro de 2020.

MOREIRA, André. **Sobre o Direito e a Inteligência Artificial (e Robótica)**. Disponível em: https://www.oscorp.com.br/single-post/2017/01/26/Sobre-o-Direito-e-a-Intelig%C3%AAncia-Artificial-Rob%C3%B3tica---Parte-I. Acesso em: 22 de janeiro de 2020.

ORWELL, George. 1984. São Paulo: Editora Companhia das Letras, 2009.
PARISER, Eli. **O filtro invisível: O que a Internet está escondendo de você**. 1ª Edição. Editora Zahar, 2012.

PEDRO, Rosa Maria Leite Ribeiro; SZAPIRO, Ana Maria; RHEINGANTZ, Paulo Afonso. Dispositivos de vigilância e as cidades: tecnologia, política e vida cotidiana. **Rev. Polis Psique**, Porto Alegre, v. 5, n. 3, p. 26-44, dez. 2015. Disponível em http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S2238-152X2015000200003&lng=pt&nrm=iso. Acesso em: 22 de janeiro de 2020.

PÉREZ, Xiomara Lorena Romero. El alcance del derecho a la intimidad em la sociedade atual**. Revista Derecho del Estado**, Bogotá n. 21, v. 1, p. 209-222, dezembro 2008. Disponível em: https://revistas.uexternado.edu.co/index.php/derest/article/view/499. Acesso em: 28 de junho 2020.

PRETA, Guilherme. **Igrejas usam reconhecimento facial em fiéis.** Disponível em: https://olhardigital.com.br/noticia/igrejas-usam-reconhecimento-facial-em-fieis/92998. Acesso em: 21 de janeiro de 2020.

PUGLIESE, Joseph. **Biometrics: Bodies, Technologies, Biopolitics.** New York: Routledge, 2010.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS. (GDPR/EU/2016/679). Disponível em: **https://gdpr-info.eu/.** Acesso em: 20 de janeiro de 2020.

SILVA, Camila Cássia. **Hering é investigada por uso de dados de clientes via reconhecimento facial.** Disponível em: https://www.tecmundo.com.br/seguranca/145544-hering-investigada-uso-dados-clientes-via-reconhecimento-facial.htm. Acesso em: 20 de janeiro de 2020.

SOLOVE., Daniel J. **Nothing to Hide:** The False Tradeoff Between Privacy and Security. New Heaven: Yale University Press, 2013.

STF. **MEDIDA CAUTELAR NA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 6.387 DISTRITO FEDERAL**. Rel. Ministra Rosa Weber, DJ 24/05/2020. STF, 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf. Acesso em 18 out 2020.

STF. **Pleno - Dados de usuários de telefonia**. Youtube, [S. l], 2020. (170 min). Disponível em: https://www.youtube.com/watch?v=84M0nOQhQXo. Acesso em 08 out 2020.

WAYMAN, James. **The Scientific Development of Biometrics over the last 40 years. *In:* The History of Information Security: A comprehensive Handbook.** Amsterdam: Editora Elsevier, 2007, págs. 263-274.

WIGGERS, Kyle. MIT researchers: **Amazon's Rekognition shows gender and ethnic bias (updated)**. Disponível em: https://venturebeat.com/2019/01/24/amazon-rekognition-bias-mit/. Acessado em: 20 de janeiro de 2020.

ZUBOFF, Shoshana. Big Other: Capitalismo de Vigilância e perspectivas para uma civilização de informação. *In*: Bruno, Fernanda; Cardoso, Bruno; Kanashiro, Marta; Guilhon, Luciana; Melgaço, Lucas (Orgs.). **Tecnopolíticas de Vigilância: perspectivas da margem.** 1ª edição. São Paulo: Boitempo, 2018, p. 17-68.

Recebido – 13/04/2021
Aprovado – 12/12/2021