Movimento por banir uso de reconhecimento facial cresce no mundo

Vigilância generalizada coloca o conjunto da sociedade sob observação e, na verdade, sob suspeita

Ricardo Abramovay

***Folha de S. Paulo,* 15.12.2019**

Vigilância generalizada coloca o conjunto da sociedade sob observação e, na verdade, sob suspeita

[RESUMO] Cresce no mundo todo o movimento por banir ou limitar o uso de reconhecimento facial. Mais do que avanço da biometria, tecnologia é um instrumento de vigilância contínua.

A Cnil (Comissão Nacional de Informática e Liberdades) da França proibiu que um colégio de Nice e outro de Marselha usassem reconhecimento facial para controlar o acesso dos alunos aos estabelecimentos.

Os colégios alegavam a possibilidade de economizar tempo dos funcionários e redução de fraudes com as novas tecnologias. Após análise cuidadosa, a Cnil chegou à conclusão de que tais procedimentos são contrários aos princípios de proporcionalidade e de minimização de dados, uma das bases da legislação europeia que regulamenta a coleta, o armazenamento e a análise de informações pessoais obtidas por meio de dispositivos digitais.

Não se trata de idiossincrasia francesa. A autoridade sueca de proteção de dados pessoais baniu o uso de reconhecimento facial em escolas e multou um estabelecimento que utilizava a técnica, apesar do consentimento dos pais dos alunos.

Exagero? Nos Estados Unidos, as câmaras municipais de Berkeley, San Francisco e Oakland, na Califórnia, e de Summerville, em Massachusetts, baniram o uso por autoridades públicas de imagens coletadas por dispositivos de reconhecimento facial.

No início de outubro, o governador da Califórnia assinou uma lei que institui moratória de três anos no uso de câmeras nos uniformes dos policiais do Estado. Parlamentares de lados opostos do espectro, como a democrata Alexandria Ocasio-Cortez e o republicano Jim Jordan, uniram-se para pedir regulamentação legal dessas câmeras antes que seu uso fique "fora de controle".

Em 2017, Satya Nadella, CEO da Microsoft, chegou a citar a obra de George Orwell para referir-se ao risco de que câmeras de vigilância contribuam para a emergência de um Estado totalitário. Embora o Google tenha feito da "inteligência artificial em primeiro lugar" (AI first) seu lema, a empresa recusou-se, ano passado, a desenvolver um sistema de reconhecimento facial que seus clientes pudessem adaptar facilmente a seus dispositivos.

Um grupo de acionistas da Amazon manifestou preocupação de que o Rekognition, plataforma de reconhecimento facial da empresa, abrisse caminho à violação de direitos humanos e civis. Em causa estão não só o viés e as distorções do dispositivo (mais preciso na identificação de homens brancos do que de mulheres negras, por exemplo), mas também o perigo de que o Rekognition seja vendido a governos autoritários e se transforme em obstáculo ao avanço da democracia no mundo.

Setenta organizações da sociedade civil obtiveram a assinatura de 150 mil pessoas contra esse dispositivo nos Estados Unidos. Em 2018, o Washington Post publicou editorial alertando

contra os riscos de um Estado orwelliano que resultaria da vigilância generalizada a que estes equipamentos abrem caminho.

Essas informações suscitam uma constatação importante: o reconhecimento facial não é um instrumento apenas de Estados ditatoriais como a China. Londres hoje tem mais dispositivos de reconhecimento facial por habitante do que Pequim. Nos Estados Unidos, o FBI dispõe de 641 milhões de imagens de americanos não suspeitos de qualquer crime.

Trata-se de um dos mais prósperos e promissores negócios da economia contemporânea. A China, onde há 176 milhões de câmeras de segurança, detém 46% do faturamento em reconhecimento facial no mundo e tem a ambição de que o setor chegue a US$ 150 bilhões por ano em 2030.

Além de seu emprego sistemático por autoridades policiais, a tecnologia é a base do sistema de pagamentos no varejo e dos empréstimos "peer to peer", altamente difundidos no país. Nos Estados Unidos esse mercado cresce 20% ao ano desde 2016.

Embora o Brasil não seja protagonista das inovações tecnológicas trazidas pela revolução digital, aqui também o reconhecimento facial avança celeremente.

Esse crescimento deve intensificar-se com o decreto que instituiu o Cadastro Base do Cidadão, que envolve não apenas foto, digitais e CPF, mas também dados biométricos como retina, íris, formato da face, voz e maneira de andar. Todos esses dados poderão ser compartilhados por diferentes órgãos governamentais, e a gestão desse sistema será feita por um comitê formado por sete representantes do governo, sem qualquer participação da academia, do mercado ou da sociedade civil.

Mas, se é um negócio tão próspero e virtualmente tão útil no comércio, na educação e na segurança pública, por que razão vem suscitando tanta apreensão e tantos protestos?

É difícil acreditar que se trate de uma espécie de doença infantil que atingiria tecnologias incipientes, quando alguns dos mais importantes ícones da revolução digital e empresas como a Microsoft e o Google manifestam publicamente o temor de uma expansão não regulamentada dessas tecnologias. Do que é acusado o reconhecimento facial?

O problema central é que ele muda a natureza da biometria pela qual os indivíduos são identificados.

Um dos Objetivos do Desenvolvimento Sustentável (o ODS 16.9) é que até 2030 todos os habitantes do mundo possuam uma identidade verificável, base para o exercício de sua cidadania não só no voto mas na obtenção de benefícios de políticas sociais. Hoje 502 milhões de pessoas na África Subsaariana e 357 milhões na Ásia do Sul não possuem identificação oficial.

Mas o reconhecimento facial contemporâneo não se limita a baratear e tornar mais rápida a obtenção deste direito universal à identificação. Ele traz ao menos duas mudanças preocupantes na ideia de biometria.

A primeira delas é que, até o início do século 21, a biometria se apoiava no recolhimento de informações individualizadas e cuja obtenção exigia o conhecimento e a cooperação das pessoas. Quando você renova sua carteira de habilitação, você sabe que suas digitais são captadas eletronicamente. É o que Laura Donohue, do Centro de Direito da Universidade de Georgetown, qualifica de "identificação biométrica imediata". Você está presente fisicamente no ato que o identifica e não tem como ignorá-lo.

O reconhecimento facial inaugura outra modalidade, que Donohue chama de "identificação biométrica remota". Como as câmeras de identificação são interligadas e conectadas a

dispositivos que contêm gigantesca base de dados (big data), elas podem localizar e identificar as pessoas em qualquer situação sem que elas tenham a menor ideia de que estão sob escrutínio.

Hoje, é perfeitamente possível identificar indivíduos numa multidão. Não é por outra razão que tanto em Hong Kong como em Santiago os manifestantes tentavam despistar as imagens das câmeras, apontando raios laser em sua direção.

Sob o ângulo jurídico, essa forma de identificação pervasiva fere um dos mais importantes preceitos constitucionais americanos, a Quarta Emenda, segundo a qual o cidadão só pode ser investigado se houver uma suspeita bem fundamentada de que ele tenha feito algo errado.

A vigilância generalizada coloca o conjunto da sociedade sob observação e, na verdade, sob suspeita. À medida que o indivíduo sabe que, de forma remota, pode ser reconhecido e catalogado como participante de uma manifestação pública, é difícil dizer que sua própria liberdade de expressão não está comprometida.

Mas isso não se refere apenas a manifestações políticas: é a vida cotidiana, a interação social, a sociabilidade humana que se transformam como resultado da identificação biométrica remota.

Uma cidade inteiramente monitorada e cujos dados são permanentemente processados por algoritmos que interpretam as imagens coletadas perde uma das características mais importantes do próprio conceito de cidade: o anonimato, a possibilidade de não ser identificado em locais públicos. Os espaços públicos tornam-se territórios de vigilância.

A entrada numa igreja, num bar, o cruzamento dos dados da entrada no bar com aquilo que o indivíduo consumiu (e que foi pago também por reconhecimento facial), a ida a um psiquiatra, a um ginecologista, em suma toda a movimentação referente à vida privada e à própria intimidade das pessoas ganha uma dimensão pública que, ao longo do tempo, acaba por interferir em seus comportamentos, já que elas sabem que estão sob observação.

O movimento global pelo banimento ou ao menos pela moratória na expansão das tecnologias de reconhecimento facial ganha força.

A possibilidade de que governos com inclinação autoritária usem o argumento da segurança e da economia para reprimir manifestações públicas, constranger indivíduos e impor condutas coerentes com sua visão de mundo é uma ameaça à democracia muito maior que a dos serviços secretos convencionais.

E o emprego dessas técnicas pelo setor privado traz igualmente o risco de impor a toda a sociedade comportamentos em que os indivíduos vão agir como quem sabe que está sendo permanentemente vigiado.

O tema pode parecer distante, mas é uma realidade que está em franca implantação e sobre a qual é essencial uma séria discussão pública que vá além do mantra de que isso é incontornável —como se o rumo tomado pelas tecnologias fosse independente da capacidade de interferência dos indivíduos e das organizações da sociedade civil.

Ricardo Abramovay é professor sênior do Instituto de Energia e Ambiente da USP e autor de ‘Muito Além da Economia Verde’ (Planeta Sustentável/Abril).