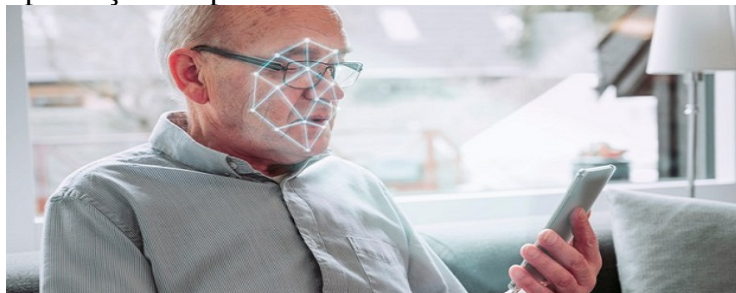


Uso do reconhecimento facial na segurança pública

No cenário contemporâneo, a rápida evolução da tecnologia tem desempenhado um papel crucial na transformação das estratégias de segurança pública em todo o mundo. Uma das inovações mais notáveis nesse contexto é a tecnologia de reconhecimento facial (FRT), que se destaca como um instrumento de vigilância invasivo e polêmico na busca por eficiência e segurança.

Os algoritmos de reconhecimento estão se aprimorando, lidando melhor com desafios como envelhecimento, iluminação inadequada e rostos mascarados, enquanto os bancos de dados de rostos crescem com a proliferação de câmeras de segurança e a coleta de imagens de várias fontes. Não podemos ignorar que tal expansão é alimentada também pela crescente submissão a escaneamentos faciais, extração de imagens de redes sociais e coleta de dados por meio de aplicativos e autoridades.

Reprodução/Serpro



Na China, a FRT foi utilizada pelo governo para fiscalizar o cumprimento pela população da rigorosa política de *lockdown* adotada ao longo da pandemia de covid-19. Com milhares de câmeras de monitoramento biométrico espalhados pelo país, as autoridades governamentais realizam um controle

implacável sobre a população, permitindo identificar os focos de disseminação do vírus, determinar o isolamento social das pessoas infectadas e penalizar os infratores do regime de quarentena.

Outro país asiático que tem se destacado pelo uso da FRT é o Japão. As Olimpíadas de 2020, que seriam sediadas em Tóquio, foram adiadas para 2021 devido à pandemia de Covid-19, motivo pelo qual quando da sua efetiva realização foram implementadas medidas de segurança avançadas, e parte disso incluiu o uso de FRT. A técnica foi empregada em diferentes aspectos dos Jogos Olímpicos, desde a recepção no aeroporto internacional, controle de acesso a locais de competição até a segurança em áreas públicas, como meio de identificação e rastreamento de pessoas, contribuindo para a segurança do evento.

Desde 2017, o Reino Unido também tem se apoiado na utilização da FRT na segurança pública e, ano a ano, vem intensificando a aplicação da ferramenta, especialmente com intuito de fiscalizar e prevenir ocorrências em grandes eventos. Exemplos em que se verificou o uso da ferramenta pela polícia britânica são o show da Beyonce, a coroação do Rei Charles e o Grande Prêmio da Grã-Bretanha de Fórmula 1. Nessas ocasiões, foram realizados escaneamentos de milhares de rostos ao vivo, sendo eles comparados por inteligência artificial com a imagem de indivíduos procurados pela polícia que compunham uma lista de observação, a fim de identificar e deter os suspeitos que correspondessem ao registro policial.

O Brasil não está fora disso. Nos últimos meses, temos acompanhado de perto a discussão acerca da legalidade da instalação de câmeras de FRT no metrô de São Paulo. De um lado, a Companhia do Metropolitano de São Paulo justifica a adoção do novo sistema de monitoramento eletrônico para



garantir a segurança dos usuários e auxiliar na localização de pessoas desaparecidas; De outro lado, um grupo de entidades, composto pelas defensorias públicas da União e do Estado, coletivo de advocacia em direitos humanos (CADHu) e Instituto Brasileiro de Defesa do Consumidor (Idec), tem acionado a Justiça para impedir o uso deste sistema por suposto viés discriminatório do software no tratamento de dados, bem como por violação da Lei de Proteção de Dados Pessoais (LGPD).

O uso da FRT é um tema em voga, porém sua regulamentação ainda é bastante incipiente e esparsa. Embora o gênero “proteção de dados pessoais” seja objeto de grande preocupação nos últimos anos e tenha impulsionado a construção de diretrizes legais a respeito em vários países, o tratamento de dados biométricos obtidos em espaços públicos por FRT ainda carece de uma normatização mais detalhada e restritiva que impeça o abuso, cometimento de discriminação e invasão de privacidade dos seus titulares pelo Estado controlador dos dados.

Quando nos debruçamos sobre a questão da proteção de dados pessoais na União Europeia, precisamos examinar dois instrumentos principais: a Convenção 108 para a proteção das pessoas em relação ao tratamento automatizado de dados pessoais e o Regulamento Geral de Proteção de Dados (GDPR).

A Convenção 108, vinculativa para os Estados-membros do Conselho Europeu, é o primeiro instrumento jurídico sobre proteção de dados pessoais. Seu artigo 6º proíbe o tratamento automático de dados reveladores de origem racial, opiniões políticas, crenças religiosas, saúde ou vida sexual, a menos que a legislação nacional estabeleça salvaguardas adequadas. No entanto, o artigo 9º da mesma convenção permite exceções para proteger a segurança do Estado, segurança pública, interesses financeiros do Estado, repressão de infrações penais ou para proteger os direitos e liberdades de terceiros. Assim, embora a convenção valorize a dignidade humana, reconhece a relativização desse direito em prol da segurança em determinadas circunstâncias.

Em 2018, o Conselho da Europa deu início a um processo de modernização visando adequar a Convenção 108 aos desafios e oportunidades decorrentes do rápido avanço das tecnologias de informação e comunicação. Essa versão modernizada, conhecida como Convenção 108+, foi adotada em 2023 e tem previsão de entrar em vigor em junho de 2024. Além de abordar questões emergentes, como a análise de grandes volumes de dados, a inteligência artificial e o tratamento de dados pessoais no contexto do ambiente de trabalho fortalecem os mecanismos de aplicação da convenção e incentivam a cooperação internacional em assuntos relacionados à proteção de dados.

Já a GDPR, que entrou em vigor em 25 de maio de 2018, visa a fortalecer e unificar as regras de proteção de dados para todos os cidadãos da UE, estabelecendo diretrizes rigorosas sobre como os dados pessoais devem ser coletados, processados, armazenados e protegidos, garantindo maior controle e privacidade aos indivíduos sobre suas informações pessoais.

As informações obtidas por meio da FRT são designadas como dados biométricos. Conforme explicitado no artigo 4 (14) da GDPR, dados biométricos referem-se a dados pessoais provenientes de um processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais de um indivíduo, permitindo ou confirmando sua identificação única, tais como imagens faciais ou impressões digitais. Devido à sua característica inerentemente resistente à eliminação ou alteração e à sua capacidade distintiva de identificação, a manipulação de dados biométricos é proibida, a menos que



obtenha o consentimento explícito do titular dos dados ou ocorra por necessidade de interesses públicos específicos, conforme estipulado no artigo 9 (2) do GDPR ou em outras circunstâncias delineadas no mesmo dispositivo legal.

Em outubro de 2021, o Parlamento Europeu emitiu uma decisão não vinculativa pedindo a proibição do uso policial de FRT em locais públicos e no policiamento preditivo, assim como a criação de bancos de dados privados para esse fim.

Em 12 de maio de 2022, o Conselho Europeu de Proteção de Dados, encarregado de aplicar o Regulamento Geral de Proteção de Dados e promover a cooperação entre as autoridades de proteção de dados da UE, emitiu as Diretrizes 05/2022 sobre o uso de FRT. O conselho considera que o tratamento de dados biométricos em espaços públicos para identificação não equilibra adequadamente os interesses privados e públicos, representando uma interferência desproporcional nos direitos dos titulares dos dados. Ao analisar o monitoramento de transeuntes em espaços públicos, o conselho destacou que tal prática compromete gravemente a expectativa razoável das pessoas de permanecerem anônimas, contrariando os princípios de autodeterminação e participação livre em uma sociedade democrática. Em outras palavras, como regra, a FRT não seria recomendável para aplicação em locais públicos.

Nos Estados Unidos, a proteção da privacidade e a manutenção da segurança pública emergem como temas caros aos cidadãos norte-americanos, gerando debates acalorados sobre a implementação de FRT em espaços públicos pela polícia. Inicialmente, nos anos de 2019 e 2020, observou-se uma inclinação para proibir o uso dessa tecnologia em vários estados dos Estados Unidos. No entanto, recentemente, alguns estados têm adotado uma abordagem mais flexível, ajustando as regulamentações para permitir o emprego dessa ferramenta em circunstâncias específicas, visando à proteção da população.

Atualmente, não há uma lei federal que regule a matéria, porém, em novembro de 2023 foi apresentada o *Facial Recognition Act*, de autoria do deputado Ted Lieu, à Câmara dos Representantes. O referido projeto regulamenta o uso da FRT pela polícia e se baseia na experiência de alguns estados, reflete os apelos dos defensores do direito à privacidade e direito digital, estabelecendo limites amplos ao uso de vigilância por reconhecimento facial pela aplicação da lei.

Em linhas gerais, os pontos principais da *Facial Recognition Act* dizem respeito às restrições ao emprego da FRT, como exigência de mandado demonstrando a causa provável de que um indivíduo cometeu um crime violento grave, proibição de utilização da FRT como única base para estabelecer causa provável para busca, prisão ou outra ação de aplicação da lei e proibição de utilização de FRT para criar um registro que documente como um indivíduo exerce direitos constitucionais, como protestar legalmente, por exemplo. Além disso, o projeto prevê o dever de transparência e proteção os direitos dos réus, como previsão de direito de ação privada para indivíduos prejudicados pelo uso da FRT, e exigência de notificação pelas autoridades policiais de indivíduos sujeitos à busca de FRT.

Embora ainda esteja em tramitação no Congresso americano, o projeto é considerado um avanço nas discussões envolvendo a regulamentação do uso da FRT no país, na medida em que estabelece requisitos claros e específicos para o uso da tecnologia, visando a proteger os direitos dos cidadãos e garantir a segurança pública.



No Brasil, em que pese a promulgação da LGPD, não há legislação que regule especificamente o uso da FRT como medida de segurança pública. Contudo, existem projetos de lei em tramitação, tanto em nível federal como estadual, tanto favoráveis como desfavoráveis à utilização do instrumento pelo poder público.

O Projeto de Lei 3069/22, que tramita na Câmara dos Deputados, regulamenta o uso da FRT por forças de segurança pública e define como reconhecimento facial o “procedimento biométrico automatizado com fim de identificação humana, realizado a partir da captura de uma imagem facial”. Segundo o idealizador do projeto, deputado Gonzaga, “a utilização de resultado obtido unicamente por meio de FRT deve ser absolutamente evitada sob pena do cometimento de erros graves de identificação”. Contudo, dada a grande utilidade da ferramenta no âmbito da segurança pública, embora não seja infalível, o sistema facial serviria como um primeiro filtro, devendo seu uso ser associado “com a etapa de revisão pericial humana, ou por meio de confirmação multibiométrica papiloscópica”.

Já em nível estadual, verificamos diversos projetos de lei vinculados à campanha #SaiDaMinhaCara, que articulou 50 parlamentares de diferentes partidos e apresentou projetos de lei banindo o uso da FRT em espaços públicos, dos quais destacamos o Projeto de Lei nº 5240/2021, submetido por Dani Monteiro, Waldeck Carneiro, Luiz Paulo, Flavio Serafini, Mônica Francisco, Enfermeira Rejane, Carlos Minc, Renata Souza e Eliomar Coelho, apresentado no Estado do Rio de Janeiro, e o Projeto de Lei nº 385 /2022, submetido por Leci Brandão (PCdoB), Isa Penna (PCdoB) e Érika Malunguinho (PSOL), apresentado no Estado de São Paulo.

Ambos de idêntico conteúdo, os projetos são contrários à adoção da tecnologia em qualquer circunstância, vedando ao Poder Público: obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial ou informações derivadas de uma FRT; celebrar contrato com terceiro com a finalidade ou objetivo de obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial, informações derivadas de uma FRT ou manter acesso à FRT; celebrar contrato com terceiro que o auxilie no desenvolvimento, melhoria ou expansão das capacidades da FRT ou forneça ao terceiro acesso a informações que o auxiliem a fazer isso; instruir pessoa jurídica de direito público ou privado a adquirir ou usar tecnologias de reconhecimento facial em seu nome; permitir que pessoa jurídica de direito público ou privado use tecnologias de reconhecimento facial em áreas urbanas, rurais ou mistas de sua circunscrição; implantar ou operacionalizar tecnologias de reconhecimento facial nos espaços públicos e privados do Estado.

No contexto regulatório, enquanto a União Europeia, com base no GDPR, sinaliza uma postura cautelosa e restrições severas ao reconhecimento facial em locais públicos, os Estados Unidos estão enfrentando debates internos, culminando no projeto de lei *Facial Recognition Act*. No Brasil, a discussão está em estágio inicial, com diferentes propostas legislativas, refletindo a necessidade urgente de uma legislação abrangente para orientar o uso ético e responsável da tecnologia. A questão central permanece: como podemos equilibrar a segurança pública com a proteção dos direitos fundamentais em um mundo cada vez mais dominado pela FRT? Essa resposta demandará uma abordagem colaborativa e multissetorial para criar um ambiente regulatório que promova a segurança sem comprometer os valores democráticos fundamentais.

Meta Fields

