ARTIGO 19

Quando corpos se tornam dados: tecnologias biométricas e liberdade de expressão

Edição Brasileira: 2022

Publicado pela primeira vez pela ARTIGO 19 Internacional em abril de 2021.

A ARTIGO 19 trabalha para um mundo em que todas as pessoas em todos os lugares possam se expressar livremente e se engajar ativamente na vida pública sem medo de discriminação. Fazemos isso trabalhando com duas liberdades interconectadas, que fornecem as bases de todo o nosso trabalho. A Liberdade de Falar diz respeito ao direito de todos de expressar e divulgar opiniões, ideias e informações por qualquer meio, assim como discordar e questionar os detentores do poder. A Liberdade de Saber diz respeito ao direito de exigir e receber informações dos detentores do poder em prol da transparência, da boa governança e do desenvolvimento sustentável. Quando qualquer uma dessas liberdades está ameaçada, pela falha de detentores do poder em protegê-las adequadamente, a ARTIGO 19 fala a uma só voz através dos tribunais, de organizações globais e regionais e da sociedade civil, onde quer que estejamos presentes.

comunicacao@artigo19.org
www.artigo19.org
@artigo19
@artigo19
@artigo19brasil

Índice

Sumário executivo

Neste informe, a ARTIGO 19 apresenta sua posição acerca dos efeitos do desenvolvimento e da implementação de tecnologias biométricas sobre o direito à liberdade de expressão.

Esta publicação é motivada pela preocupação com o rápido e crescente uso das tecnologias biométricas não apenas pelo setor privado, mas também por órgãos públicos, em contextos que vão desde a proteção de fronteiras até o desbloqueio de *smartphones*, e pelo fato de elas estarem sendo naturalizadas pela sociedade. Tais tecnologias estão sendo utilizadas para analisar o modo como se age, aparenta e se expressa nas esferas pública e privada, e têm o poder de mudar a forma como as pessoas se comportam nos espaços públicos, ameaçando, portanto, a própria existência do espaço cívico, um pilar essencial da democracia, que permite a participação pública e o exercício dos direitos humanos.

Nesse contexto, os atores estatais ou privados que concebem, projetam, desenvolvem e implementam tecnologias biométricas devem fazê-los conforme uma abordagem de direitos humanos, a fim de proteger os direitos fundamentais das pessoas. Em particular, a ARTIGO 19 destaca as seguintes preocupações:

- O aumento das práticas de vigilância biométrica em massa dos espaços públicos, usando tecnologias biométricas como o reconhecimento facial e o reconhecimento de emoções, criará, sem dúvidas, um grave efeito inibidor[1] na liberdade de expressão e na participação pública.
- Os Estados e o setor privado estão desenvolvendo e implementando tecnologias biométricas sem considerar os danos que elas podem causar à vida das pessoas e seu efeito prejudicial ao exercício dos direitos humanos. Trata-se de um quadro preocupante, pois esses atores podem usar esses tipo de tecnologias de forma altamente intrusiva, violando os direitos à liberdade de expressão e à privacidade e não protegendo adequadamente os dados pessoais. É relevante destacar que, no caso do Brasil, há a preocupação específica com o uso dessas tecnologias para a reprodução de preconceitos de raça, classe e gênero, especialmente em casos de violações e repressões por parte de forças de segurança pública e agentes privados. Isso porque o uso de tecnologias biométricas e o tratamento desse tipo de dado podem resultar na identificação de falsos positivos e negativos por meio de vieses raciais nos algoritmos. Além disso, considerando a seletividade penal e criminalização de corpos suscetíveis à discriminação racial – o que é diuturnamente denunciado por movimentos sociais e organizações da sociedade civil –, o uso desse tipo de tecnologia de forma massiva em espaços públicos pode catalisar e potencializar a seleção dessas pessoas pelas forças de segurança, por meio de abordagens policiais e ajuizamento de processos criminais indevidos.

- Há uma grave ausência de responsabilização, prestação de contas e obrigações públicas relativas à transparência (*accountability*). Os atores estatais ou privados não criaram mecanismos efetivos para que as potenciais vítimas possam reivindicar reparação adequada pelas violações de seus direitos. Se, por exemplo, pessoas sofrerem discriminação por causa do uso do reconhecimento facial, não está público e evidente o modo como tal questão seria tratada, se seriam feitas reparações adequadas e como isso seria realizado.
- Por último, o fato de uma tecnologia biométrica específica (ou qualquer tecnologia) estar disponível não deve servir de justificativa automática para seu respectivo uso. A própria maneira pela qual essas tecnologias são concebidas e projetadas indica que elas são propícias a usos abusivos, estão sujeitas a falhas de segurança e podem proporcionar vieses discriminatórios, sendo que preocupações relativas a estes últimos devem ser especialmente levadas em consideração no Brasil, em que há condições sociais estruturais relativas a opressão de raça e gênero. A pressão em desenvolver ferramentas e produtos por si só falha essencialmente na tarefa de colocar a tecnologia a serviço do ser humano ou de projetar soluções que de fato resolvam problemas existentes.

Por esses motivos, a ARTIGO 19 alerta contra o uso de tecnologias biométricas, especialmente sob os argumentos relacionados à segurança pública, sem que haja uma estrutura legislativa suficiente para proteger os direitos humanos. Consideramos que uma abordagem baseada nos direitos humanos deve ser incorporada desde a concepção, o projeto e o desenvolvimento de qualquer tecnologia. Pedimos, portanto, uma moratória no desenvolvimento e na implementação de todas as tecnologias biométricas tanto pelos Estados como por atores privados até que eles possam garantir a proteção total da liberdade de expressão e o pleno cumprimento das normas internacionais de direitos humanos.[2]

Esta publicação está dividida em cinco partes. Primeiro, apresentamos as principais informações e terminologias relativas à tecnologia biométrica. Depois, abordamos as normas internacionais relevantes sobre liberdade de expressão e aplicáveis à tecnologia biométrica. Subsequentemente, há uma seção que discorre sobre como a utilização e o abuso dessas tecnologias impedem que as pessoas exerçam seus direitos humanos, com foco particular no direito à liberdade de expressão e ao acesso à informação. Em seguida, analisamos dois estudos de caso: um sobre como o reconhecimento facial limita a liberdade de expressão e o outro sobre como o reconhecimento de emoções pode ter esse mesmo impacto. Ao final, listamos recomendações abrangentes dirigidas a Estados, empresas privadas e demais partes interessadas.

Resumo das recomendações:

1. Os Estados devem banir a vigilância biométrica em massa.
2. Os Estados devem banir a concepção, o projeto, o desenvolvimento e o uso de tecnologias de reconhecimento de emoções.
3. Os atores públicos e privados que concebem, projetam, desenvolvem e utilizam tecnologias biométricas devem respeitar os princípios de legitimidade, proporcionalidade e necessidade.
4. Os Estados devem estabelecer um marco legislativo adequado para a concepção, o projeto, o desenvolvimento e o uso de tecnologias biométricas.
5. As autoridades governamentais devem assegurar que a concepção, o projeto, o desenvolvimento e o uso de tecnologias biométricas estejam sujeitos à transparência e abertos ao debate público.
6. Os requisitos de transparência devem ser impostos e implementados de forma ampla tanto pelo setor público como pelo privado.
7. Os Estados devem garantir responsabilização, prestação de contas e obrigações públicas relativas à transparência (accountability) e o acesso a reparações adequadas por violações de direitos humanos decorrentes de tecnologias biométricas.
8. O setor privado deve conceber, projetar, desenvolver e implementar sistemas biométricos de acordo com as normas aplicáveis de direitos humanos.

Introdução

Em todo o mundo, governos e atores privados que utilizam sistemas de identificação e verificação se baseiam cada vez mais em dados biométricos – desde impressões digitais e amostras de DNA até tecnologias biométricas mais avançadas que visam a identificar pessoas com base em suas características físicas, comportamento ou condutas[3]. Os setores público e privado atualmente empregam essas tecnologias em vários ambientes para mensurar e analisar em tempo real aparências, vozes, comportamentos e deslocamentos das pessoas. Tais tecnologias são cada vez mais aplicadas em áreas como controle de fronteiras, segurança pública, publicidade e *marketing*,[4] e são comumente utilizadas pelas pessoas para desbloquear *smartphones*, acessar contas bancárias online ou mesmo acessar espaços físicos e outros espaços *online*.[5] Seu uso massivo, no entanto, não está necessariamente limitado à identificação pessoal. Ele também resulta e na caracterização e categorização das pessoas com base em idade, sexo, cor da pele e no controle sobre o que estão fazendo, com quem o fazem, como estão se sentindo e até mesmo como provavelmente se comportarão no futuro.

As tecnologias biométricas desenvolveram-se rapidamente nos últimos anos, principalmente em razão de dois fatores. O primeiro é a disponibilidade de um número sem precedentes de bases de dados **gigantescas,** sendo esses dados coletados sobretudo pelo setor privado com base em modelos de negócios cada vez mais orientados por dados e apoiados em narrativas alarmantes conectadas à segurança pública e/ou a medidas de combate ao terrorismo. O segundo fator é a disponibilidade crescente, a preços mais baixos, do *machine learnin*g, isto é, do aprendizado de máquina, tanto em termos de *hardware* (infraestrutura e capacidade computacional) quanto de *software* (incluindo a disponibilização de mais financiamento e de pessoal qualificado para aprendizado de máquina). Ambos os fatores estão fortemente inter-relacionados, já que o último precisa do primeiro para funcionar. Esses avanços permitiram uma vasta difusão dos sistemas de vigilância e uma transição de um mundo onde sistema de rastreamento e identificação eram exceções para um mundo onde eles estão se tornando a norma.

Ainda que essas tecnologias tenham evoluído e se popularizado cada vez mais, os marcos legislativos relevantes não evoluíram na mesma velocidade. Embora muitos países tenham emitido marcos regulatórios específicos para o uso de tecnologias biométricas de "primeira geração", o mesmo não pode ser dito sobre as desenvolvidas mais recentemente, uma vez que a maioria delas opera sem base legal específica. Trata-se de algo altamente problemático, pois o mau uso/abuso das tecnologias biométricas afeta a vida das pessoas de várias maneiras. São tecnologias especialmente intrusivas, e seu emprego viola frequentemente os direitos humanos à privacidade e à proteção de dados,[6] à dignidade humana,[7] à não discriminação,[8] à autodeterminação e ao direito de acesso a uma reparação adequada.

O uso crescente, difundido e muitas vezes invisível das tecnologias biométricas pelos setores público e privado, bem como sua capacidade de identificar e rastrear pessoas e comportamentos, também impede que as pessoas exerçam seu direito à liberdade de expressão, particularmente a possibilidade de permanecerem anônimas. Essas aplicações também têm prejudicado o espaço cívico, sendo essa a esfera onde os indivíduos exercitam seus direitos, participam, se expressam, se reúnem e se informam. Como o espaço cívico é um pilar fundamental da democracia, a difusão e o uso de tecnologias biométricas põem em risco a própria existência dos processos democráticos.[9] Somado a isso, há uma grave falta de transparência sobre os agentes que desenvolvem e implementam tais tecnologias, sobre a maneira por meio da qual isso é feito e sobre o porquê de elas estarem sendo desenvolvidas, o que impede um debate público e aberto sobre seu uso por parte dos setores público e privado.

Recentemente, a **pandemia de Covid-19** reforçou um apelo por soluções tecnológicas e deu um impulso adicional aos agentes públicos e privados para que desenvolvam e implementem tecnologias biométricas como ferramentas "centrais" nas medidas de prevenção e contenção da pandemia.[10] Estas incluem vários aplicativos de quarentena ou de rastreamento de contatos[11], bem como o uso de capacetes de vigilância pela polícia para escanear as pessoas com febre (um dos sintomas da Covid-19) enquanto elas transitam em espaços públicos.[12] Preocupantemente, tanto agentes públicos quanto privados têm adotado uma narrativa que coloca os direitos humanos em oposição à saúde pública[13] e estão forçando as populações a aceitar um nível de vigilância em massa sem precedentes. Embora as medidas para proteger as pessoas da Covid-19 sejam importantes e possam ser simplificadas por meio do uso de tecnologias biométricas em um contexto estritamente emergencial e que não propicie o estabelecimento de monitoramento e controle constante, é improvável que tais tecnologias sejam a solução, como é frequentemente anunciado, para os mais diversos problemas que a sociedade contemporânea enfrenta. Em qualquer caso, como elas podem ser usadas para se inserir na vida privada das pessoas, o uso dessas tecnologias deve ser sempre controlado e estar de acordo com as normas internacionais, e nunca ser naturalizado.

A ARTIGO 19 considera importante contribuir para os debates atuais sobre a possibilidade de mitigar abusos da crescente tendência de uso de tecnologias biométricas ou a respeito da possibilidade de proibição por completo do uso dessas tecnologias por órgãos estatais e entes privados. Neste estudo, examinamos como o mau uso/abuso das tecnologias biométricas impede as pessoas de exercer plenamente seu direito à liberdade de expressão e ao acesso à informação e fazemos recomendações aos Estados, atores privados e todas as partes interessadas sobre como proteger e promover a liberdade de expressão.

Nesse contexto, a estrutura do presente documento é a seguinte:

- primeiramente, estabelecemos algumas definições, terminologias e conceitos básicos em torno do uso de tecnologias biométricas;
- em segundo lugar, delimitamos as normas internacionais de direitos humanos que se aplicam ao uso dessas tecnologias;
- em terceiro lugar, avaliamos o impacto das tecnologias biométricas sobre o direito à liberdade de expressão;
- em quarto lugar, realizamos dois estudos de caso específicos de biometria e liberdade de expressão: um sobre reconhecimento facial e o outro sobre reconhecimento de emoções;
- e, finalmente, fazemos recomendações aos Estados, a atores privados e a outras partes interessadas sobre como garantir a proteção da liberdade de expressão na concepção, no projeto, no desenvolvimento e no uso de tecnologias biométricas.

Nossas recomendações para os Estados, os agentes privados e todas as outras partes interessadas unem-se a um apelo sincero para não excluir do debate público uma das batalhas mais importantes para definir a liberdade de expressão e a própria existência de um espaço cívico para a nossa geração e as próximas.

Tecnologias biométricas: contexto

Terminologia-chave

O termo **biometria** geralmente descreve as características fisiológicas e comportamentais das pessoas, como impressões digitais, voz, formato do rosto, padrões de retina e da íris, geometria da mão, maneira de caminhar ou perfis genéticos.

Dados biométricos foram definidos pelo Parlamento Europeu como "dados pessoais resultantes de processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais de uma pessoa natural, que permitem ou confirmam a identificação única dessa pessoa natural, tais como imagens faciais ou dados dactiloscópicos (impressões digitais)".[14] Os dados biométricos alteram irrevogavelmente a relação entre corpo e identidade, pois tornam as características do corpo humano "legíveis por máquina" e passíveis de serem usadas posteriormente[15].

A Lei Geral de Proteção de Dados – LGPD brasileira (Lei no 13.709/2018) não define o que seriam dados biométricos em si, mas classifica, em seu artigo 5º, inciso II, esse tipo de dado como "dado pessoal sensível".[16] A lei ainda traz uma seção específica que determina critérios mais restritos, se comparados com os adotados em relação a dados pessoais não sensíveis, para o tratamento desse tipo de dado. O tratamento[17] de dados biométricos segundo a LGPD ocorre com base no consentimento do titular ou de seu responsável legal ou sob outras bases legais nas hipóteses listadas pelo dispositivo, nas quais o fornecimento do consentimento pode ser afastado.

O termo **tecnologia biométrica** refere-se então a uma variedade de tecnologias que medem e analisam características humanas únicas, tais como DNA, impressões digitais, padrões de voz, medidas das mãos, retinas ou íris, além de frequência cardíaca[18]. Mais recentemente, as tecnologias biométricas passaram a incluir, entre outros sistemas, a biometria multimodal, a biometria comportamental, o reconhecimento dinâmico da face, o reconhecimento remoto da íris e várias outras aplicações em diferentes estágios de desenvolvimento.[19]

O termo **reconhecimento facial** se enquadra em uma categoria mais ampla de tecnologias biométricas e pode ser definido como "processamento automático de imagens digitais que contêm as faces de indivíduos para autenticação, identificação ou categorização"[20].

O **reconhecimento de emoções** é uma tecnologia biométrica que utiliza o machine learning na tentativa de identificar os estados emocionais das pessoas e classificá-las em categorias específicas como raiva, surpresa, medo, felicidade etc. Os dados de entrada podem incluir rostos, movimentos corporais, tonalidades vocais, palavras faladas ou digitadas e sinais fisiológicos (por exemplo, frequência cardíaca, pressão arterial e frequência respiratória).[21]

Confiabilidade de algumas tecnologias biométricas

A precisão e a confiabilidade da aplicação de tecnologias biométricas para o reconhecimento de emoções e comportamentos ainda não foram comprovadas. Uma vasta quantidade de estudos científicos adverte que expressões faciais e outros comportamentos externos não são indicadores confiáveis de estados emocionais internos.[22] Essas pesquisas advertem que as imprecisões levam à discriminação de minorias raciais,[23] étnicas ou outras minorias[24] e destacam as premissas racistas que formam a base dessas tecnologias.[25]

Deve-se destacar que muitas dessas tecnologias e aplicações dependem de uma percepção histórica inaugurada pelos estudos sobre fenótipos, inspirados pela classificação racial e por premissas racistas (ângulo facial, cranioscopia/frenologia, fisionomia, antropometria).[26] Tais técnicas foram criadas para estabelecer o chamado "racismo científico" aplicado ao mundo colonial.[27] Embora a validade científica de tais métodos nunca tenha sido comprovada, a aplicação dessas técnicas marcou a evolução dessa linha de estudo, principalmente em sua aplicação para a caracterização, classificação e identificação de estereótipos a serem utilizados na antropologia criminal e em parâmetros eugênicos.[28] A história social das tecnologias biométricas é, portanto, fundamental para compreender os desafios relacionados ao modo como elas são utilizadas hoje. Assim, mesmo que sua precisão seja aprimorada, a discriminação e as questões legais que emergem dessas tecnologias permaneceriam sem solução.

Isso significa que a aceitabilidade da utilização da biometria tem de ser conectada estreitamente a um exercício de equilíbrio que considere, por um lado, o interesse legítimo do uso da tecnologia e, por outro, a necessidade de garantir a proteção aos direitos humanos.

Os principais usos e as narrativas dominantes por trás da implementação de tecnologias biométricas

Os governos e agentes privados utilizam atualmente as tecnologias biométricas de várias maneiras, alegando que, com isso, atingiriam diversos objetivos. As reivindicações mais proeminentes incluem as listadas a seguir.

- **Proteção da segurança nacional, medidas antiterroristas e de segurança pública** são algumas das justificativas dadas para a implementação de tecnologias biométricas em vários ambientes nas últimas duas décadas; seu uso abrange desde controles e gestão de fronteiras[29] e controle de embarque em aeroportos[30] até sistemas nacionais de identificação.[31] Além das narrativas de segurança e proteção, órgãos de segurança pública têm utilizado a tecnologia de reconhecimento facial como uma ferramenta para ajudar a prevenir e detectar crimes, garantir a segurança pública e processar supostos infratores,[32] prevenir fraudes e roubos e seguir movimentos de grupos formados por minorias[33].
- As tecnologias biométricas também têm sido utilizadas por autoridades para a gestão e o acesso a várias funções e **prestações de serviços públicos**[34], como sistemas eletrônicos de saúde e registros eleitorais.[35] Elas também são empregadas no **desenvolvimento de projetos de "cidades inteligentes"**, transporte público, acesso a escolas ou a espaços físicos e *online*[36] privados ou geridos pela iniciativa privada.

A implementação de tecnologias biométricas é normalmente justificada por uma série de vantagens que elas supostamente ofereceriam, como o acesso rápido e sem necessidade de contato, soluções de redução de custos, maior precisão e confiabilidade, maior segurança e bem-estar. Entretanto, a maioria dessas vantagens não é comprovada ou, quando tais promessas são analisadas, não se levam devidamente em consideração as vastas contrapartidas, como a violação aos direitos humanos e a ameaça de perpetuação de um contexto de controle e vigilância pelo poder público e por empresas privadas.

Esse rol de justificativas corrobora o argumento amplamente adotado de que a disponibilidade de uma tecnologia é suficiente para justificar seu uso. Devemos resistir fortemente a essa abordagem e, além disso, ter em vista que a concepção, o projeto, o desenvolvimento e a implementação de tecnologias biométricas não podem ser assumidos como neutros. Em nível técnico, a biometria baseia-se na realização de suposições e em premissas previamente estabelecidas; em nível institucional, ela é utilizada por meio de expedientes essencialmente discriminatórios e que aprofundam desigualdades socioestruturais e discriminações históricas. De maneira geral, as tecnologias biométricas funcionam como sistemas sociotécnicos que refletem valores e suposições e que, como discutido neste informe, estão longe de alcançar a proteção dos direitos humanos ou são totalmente incompatíveis com ela.[37]

Normas internacionais de direitos humanos e tecnologias biométricas

Normas de direitos humanos aplicáveis

Não há normas internacionais explícitas que tratem diretamente de tecnologias biométricas. Sua implementação e seu uso, no entanto, afetam a capacidade das pessoas de exercer uma série de direitos humanos, em particular os citados a seguir.

- A **liberdade de expressão**, protegida pelo artigo 19 da Declaração Universal dos Direitos Humanos (DUDH)[38] e reforçado juridicamente pelo artigo 19 do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP),[39] bem como em tratados regionais de direitos humanos.[40] Segundo as normas internacionais de direitos humanos, as restrições ao direito à liberdade de expressão só são permitidas sob circunstâncias muito específicas (o chamado teste tripartite);[41] todas as restrições devem ser rigorosas e estritamente adaptadas e não podem pôr em risco o próprio direito.[42]
- **O direito ao acesso à informação,** reconhecido como um elemento do direito à liberdade de expressão. O Comitê de Direitos Humanos da ONU, órgão encarregado de interpretar o PIDCP, analisou o escopo e os limites do direito à informação em 2011 e declarou que o artigo 19 do citado tratado garante o direito à informação detida pelos órgãos públicos. A interpretação determina que os Estados proativamente divulguem informações de interesse público e que o acesso a elas seja "fácil, rápido, eficaz e prático".[43] O Comitê também estipulou que os Estados devem promulgar "procedimentos necessários", como legislações para efetivar o direito à informação, que as taxas de acesso devem ser limitadas, que as respostas aos pedidos devem ser fornecidas em tempo adequado, que as autoridades devem apresentar explicações para a não concessão de informações e que os Estados devem estabelecer mecanismos de recurso.[44]
- **A liberdade de associação e reunião pacífica,** garantida pelo artigo 20, parágrafo 1, da Declaração Universal dos Direitos Humanos (DUDH) e reforçada no artigo 21 do PIDCP, no artigo 5(d) da Convenção sobre a Eliminação da Discriminação Racial[45] e em tratados regionais.[46] Sob tais normas, os requisitos para restrições admissíveis devem obedecer ao mesmo teste tripartite para as restrições à liberdade de expressão.[47]
- **O direito à privacidade,** garantido pelo artigo 12 da DUDH e pelo artigo 17 da PIDCP e em tratados regionais.[48] Sob tais normas, a privacidade é um conceito amplo relacionado à proteção da autonomia individual e à relação entre um indivíduo e a sociedade, incluindo governos, empresas e outros indivíduos. O direito à privacidade é comumente reconhecido como um direito fundamental que sustenta a dignidade humana e outros valores. As restrições à privacidade também devem atender às exigências do teste tripartite.[49]

- **O direito à não discriminação e o direito à igualdade,** protegidos pelo artigo 2 e pelo artigo 7 da DUDH e garantido por meio dos artigos 2 e 26 do Pacto Internacional dos Direitos Econômicos, Sociais e Culturais (Pidesc), bem como por tratados e instrumentos regionais.[50] O direito à igualdade implica que todas as pessoas devem receber "sem discriminação alguma, a igual proteção da Lei. A (...) lei deverá proibir qualquer forma de discriminação e garantir a todas as pessoas proteção igual e eficaz contra qualquer discriminação por motivo de raça, cor, sexo, língua, religião, opinião política ou de outra natureza, origem nacional ou social, situação econômica, nascimento ou qualquer outra situação".[51]
- **A liberdade de locomoção,** prevista no artigo 13 da DUDH e também no artigo 12 do PIDCP. Comumente é considerada o "direito de ir e vir" e diz respeito a circular livremente nas fronteiras de um Estado. Ainda segundo o artigo 12 do PIDCP, esses direitos "não poderão constituir objeto de restrições, a menos que estejam previstas em lei e no intuito de proteger a segurança nacional e a ordem, saúde ou moral públicas, bem como os direitos e liberdades das demais pessoas, e que sejam compatíveis com os outros direitos reconhecidos no presente Pacto".

A liberdade de expressão e a privacidade são direitos que se reforçam mutuamente, especialmente na era digital.[52] A privacidade é um pré-requisito para o exercício da liberdade de expressão; sem ela, os indivíduos não têm espaço para pensar, falar e ter suas vozes escutadas. Ocorre que, quando os Estados desenvolvem ou utilizam a biometria de uma forma que interfere no direito à privacidade, esse uso deve estar sujeito ao teste tripartite, que analisa sua legalidade, sua necessidade e sua proporcionalidade.

Além disso, a **proteção de dados pessoais** é reconhecida pelo Comitê de Direitos Humanos da ONU como parte fundamental da privacidade.[53] A Resolução de 1990 da Assembleia Geral da ONU sobre diretrizes para a proteção de dados de informações pessoais mantidas em bancos de dados informatizados[54] estabelece seis princípios básicos de proteção de dados com base em *Fair Information Practices*.[55] Em nível regional, a proteção de dados pessoais também é garantida na Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108),[56] na Carta da UE,[57] nos termos da Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais (Convenção da UA sobre o Crime Cibernético)[58] e nos termos dos Princípios sobre Privacidade e Proteção de Dados Pessoais da Organização dos Estados Americanos (OEA).[59]

Leis internacionais de direitos humanos também reconhecem que os indivíduos que querem saber se e por que foram submetidos ao uso de tecnologias biométricas pela administração pública têm o direito de fazê-lo sob a lei de proteção de dados. Entre esses direitos está o de ser informado sobre a coleta e o uso de seus dados pessoais, o que leva a uma gama de obrigações de disponibilização de informação por parte de

quem controla esses dados[60]. Em seu Comentário Geral nº 16, o Comitê de Direitos Humanos da ONU observou que esse direito é necessário para garantir o respeito do direito à privacidade.[61] Além disso, tal direito foi amplamente incorporado no direito internacional, bem como nos principais acordos regionais sobre proteção de dados.[62] Nos termos do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR, na sigla em inglês), cada indivíduo tem o direito a ser informado, havendo distinção entre duas situações: se os dados pessoais são obtidos diretamente pela pessoa (artigo 13) e caso não ocorra essa hipótese (artigo 14).[63]

A importância de garantir fortes salvaguardas para impedir o acesso ilegal aos dados e preservar a transparência foi enfatizada na União Europeia pela Agência dos Direitos Fundamentais (FRA, em inglês), com especial referência à coleta de dados pessoais, incluindo impressões digitais de requerentes de asilo e de visto, bem como de migrantes em situação irregular.[64] Alguns Estados também estabeleceram a proteção desses direitos e salvaguardas de privacidade em sua legislação nacional.[65]

Organismos internacionais de direitos humanos também avançaram no sentido de reconhecer o **direito ao anonimato** como um aspecto importante do direito à liberdade de expressão e à privacidade. Isto tem implicações para as tecnologias biométricas utilizadas para identificar indivíduos em suas casas e em espaços públicos. A interferência do Estado no anonimato deve estar sujeita, portanto, ao teste tripartite: legalidade, necessidade e proporcionalidade, como qualquer outra interferência nesse direito.[66]

Normas de direitos humanos sobre tecnologias biométricas

Embora não existam normas internacionais que regulem explicitamente tecnologias biométricas, há um grupo emergente de normas relevantes para o desenvolvimento e a implementação dessas tecnologias.

Em primeiro lugar, os órgãos de direitos humanos reconhecem cada vez mais as maneiras pelas quais novas formas de processamento de dados impedem a capacidade das pessoas de exercer seus direitos humanos. Com relação ao perfilamento, por exemplo, que pode envolver o uso de sistemas biométricos para auferir, inferir ou prever informações sobre indivíduos com o propósito de avaliá-los ou avaliar algum aspecto sobre eles, o Conselho de Direitos Humanos da ONU observou com preocupação, em março de 2017, que:

> O processamento automático de dados pessoais para a elaboração de perfis individuais pode levar à discriminação ou a decisões que, de outra forma, poderiam afetar o exercício dos direitos humanos, incluindo os direitos econômicos, sociais e culturais.[67]

Em segundo lugar, especificamente em relação a dados biométricos, a Convenção Modernizada do Conselho da Europa para a Proteção de Indivíduos no que diz respeito ao Tratamento Automatizado de Dados Pessoais (a Convenção 108+) prevê que o tratamento de dados biométricos que identificam uma pessoa de forma única só será permitido quando salvaguardas apropriadas forem consagradas em lei, complementando as da Convenção 108.[68]

O GDPR proíbe o processamento de dados biométricos para fins de identificação única de uma pessoa natural, ressalvado um número limitado de exceções.[69] Além disso, a normativa europeia define os dados biométricos utilizados para fins de identificação como "dados de categoria especial", o que significa que são considerados mais sensíveis e que necessitam de maior proteção. A mesma abordagem é adotada nas Normas de Proteção de Dados Pessoais para os Estados Ibero-americanos[70] e pela LGPD, que os categoriza como dados sensíveis, demandando uma proteção mais rígida devido a seu potencial discriminatório.

A Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais requer autorização preliminar da autoridade nacional de proteção de dados para o processamento de dados pessoais envolvendo dados biométricos.[71]

Outros instrumentos internacionais fornecem diretrizes úteis sobre como avaliar o impacto do uso de tecnologias biométricas sobre a capacidade de as pessoas exercerem seus direitos humanos. Por exemplo, a Alta Comissária da ONU para os Direitos Humanos, em seu relatório sobre o direito à privacidade na era digital, destacou as preocupações sobre o uso de dados biométricos, sobre o potencial de eles serem objetos de "graves violações" e sobre os Estados que embarcam em projetos baseados em biometria sem "salvaguardas legais e processuais adequadas".[72] O relatório recomenda que os Estados, entre outras medidas:

> Assegurem que os sistemas que utilizam uma grande quantidade de dados, incluindo os que envolvem a coleta e a retenção de dados biométricos, só sejam implementados quando os Estados puderem demonstrar que eles são necessários e proporcionais para atingir um objetivo legítimo.[73]

Além disso, três mandatos de direitos humanos já alertaram sobre os sistemas biométricos:

- Em 2019, o Relator Especial da ONU sobre Liberdade de Reunião e Associação Pacífica declarou em seu relatório que "deve ser proibido o uso de técnicas de vigilância para fins de vigilância indiscriminada e não direcionada daqueles que exercem seu direito de reunião e associação pacífica, tanto em espaços físicos quanto digitais".[74]
- O Relator Especial da ONU sobre o Direito à Privacidade colocou em questão a necessidade e a proporcionalidade do uso de sistemas biométricos.[75]
- O Relator Especial da ONU sobre Liberdade de Expressão levantou preocupações semelhantes sobre o impacto dos sistemas biométricos sobre defensores de direitos humanos, jornalistas, políticos e investigadores da ONU.[76]

A jurisprudência de determinados organismos internacionais e tribunais regionais e nacionais também fornece indicações gerais sobre as normas a serem aplicadas nos casos de uso de tecnologias biométricas. Em particular, a Corte Europeia de Direitos Humanos (CEDH) destacou a necessidade de encontrar um equilíbrio entre a proteção dos direitos fundamentais e o desenvolvimento de novas tecnologias, e considerou a retenção "geral e indiscriminada" de dados biométricos uma "interferência desproporcional" no direito à privacidade, por não satisfazer às exigências da CEDH e não poder ser vista como "necessária em uma sociedade democrática"[77].

Uma abordagem parcialmente diferente parece ter sido adotada no campo do combate ao terrorismo. Em 2017, o Conselho de Segurança da ONU decidiu que os Estados devem desenvolver e implementar sistemas para coletar e compartilhar dados biométricos para fins de combate ao terrorismo.[78] Da mesma forma, o Adendo de 2018 aos Princípios Orientadores de Madri observa a utilidade dos dados biométricos.[79] Como resultado, os sistemas biométricos são adotados como uma ferramenta legítima para a identificação de suspeitos/as de terrorismo.

Entretanto, mesmo quando o objetivo é combater o terrorismo, o uso de tecnologias biométricas deve estar de acordo com as normas internacionais, e em particular com os princípios de necessidade e proporcionalidade. O Compêndio das Nações Unidas de práticas recomendadas para o uso responsável e compartilhamento da biometria no combate ao terrorismo poderia ser considerado um primeiro passo para uma abordagem mais centrada nos direitos humanos, apesar de não ser uma estrutura suficientemente adequada.[80]

Responsabilidades do setor privado em matéria de direitos humanos

Embora o direito internacional dos direitos humanos imponha obrigações aos Estados para a proteção, a promoção e o respeito aos direitos humanos, há o amplo reconhecimento de que o setor privado também tem a responsabilidade de respeitar os direitos humanos.[81]

Os Princípios Orientadores sobre Empresas e Direitos Humanos fornecem um ponto de partida para articular o papel do setor privado na proteção dos direitos humanos na Internet.[82] Eles reconhecem a responsabilidade das empresas de respeitar os direitos humanos, independentemente das obrigações do Estado ou da implementação dessas obrigações, e recomendam às empresas que adotem várias medidas.[83] Trata-se de parâmetros que incluem a incorporação de salvaguardas de direitos humanos desde a concepção e planejamento do projeto para mitigar os impactos adversos sobre as pessoas e as comunidades, desenvolver poder de influência e propiciar sua aplicação conjunta a fim de fortalecer seu poder frente a autoridades governamentais; e disponibilização de reparações adequadas para impactos adversos sobre os direitos humanos que sejam identificados.

Várias partes interessadas solicitaram a regulamentação. De maneira limitada, isso também se aplica a empresas de tecnologia que, após responder inicialmente a apelos para a adoção de normas sobre tecnologias biométricas “éticas” ou “confiáveis”, começaram a reconhecer que era necessário dar um passo além, também pedindo regulamentação. No entanto, propostas de regulação feitas por empresas de tecnologia, seja no campo da ética, seja no campo jurídico, raramente mostram-se adequadas. Além disso, essas são medidas não vinculantes, e não marcos regulatórios apropriados para a proteção de direitos humanos no contexto das tecnologias biométricas.[84]

Por fim, há um reconhecimento crescente de que as normas e os protocolos técnicos devem ser fundamentados em uma abordagem de direitos humanos, pois podem ter um impacto substancial no exercício destes últimos[85]. No entanto, apesar desse reconhecimento crescente, os direitos humanos não são explicitamente nem adequadamente abordados nos processos políticos de muitas organizações técnicas ou empresariais, embora esses agentes estejam rapidamente representando meios de entrada e mediadores do exercício da liberdade de expressão e da liberdade de associação, uma vez que desenvolvem a maioria dos sistemas de tecnologias biométricas. Ainda que iniciativas como os Princípios de Inteligência Artificial do Google[86] possam ser lidas como um passo nessa direção, elas têm demonstrado muitas falhas e, até agora, não conseguiram garantir níveis suficientes de responsabilização, prestação de contas e cumprimento de obrigações públicas relativas à transparência (*accountability*) das empresas.

Tecnologias biométricas e o direito à liberdade de expressão e informação

Tecnologias biométricas e direitos humanos: desafios gerais

Antes de discutir os desafios trazidos pelo mau uso ou abuso das tecnologias biométricas para o exercício do direito à liberdade de expressão e acesso à informação, a ARTIGO 19 destaca, a seguir, alguns problemas que essas tecnologias apresentam do ponto de vista dos direitos humanos em geral.

Coleta, armazenagem e retenção de dados

O desenvolvimento e a implementação de tecnologias biométricas implicam a coleta e a geração de grandes quantidades de dados pessoais sensíveis. Os dados biométricos são uma categoria especial de dados pessoais que, devido à sua capacidade de revelar informações íntimas sobre uma pessoa (impressões digitais, varreduras oculares, origem racial ou étnica, sexo etc.), exigem salvaguardas adicionais e maior proteção. Desde o princípio, portanto, a tecnologia biométrica é projetada para ser muito invasiva. Além disso, as bases de dados são frequentemente construídas a partir de métodos problemáticos de coleta – por exemplo, amostras de dados podem não ser representativas da população em geral e apresentar vieses que refletem os padrões discriminatórios sociais previamente existentes.[87]

Igualmente problemática é a prática difundida de retenção indiscriminada de dados biométricos que não atende aos critérios de necessidade e proporcionalidade.[88] Em outras palavras, agentes de tratamento de dados frequentemente mantêm os dados biométricos por mais tempo do que necessitam tão somente com o objetivo de retê-los, sem justificativas adequadas.

Além disso, esses bancos de dados gigantescos podem ser facilmente utilizados por agentes estatais ou privados para outros fins que não aqueles originalmente previstos. Essa possibilidade levanta o debate sobre o potencial de expansão da aplicação dessas tecnologias para a coleta de dados e/ou a execução de funções que não foram originalmente aprovadas. Já existem evidências de que bancos de dados biométricos que foram criados para um propósito foram reutilizados para outro.[89] Nesses casos, mesmo que as pessoas tenham consentido o uso de seus dados biométricos para o propósito inicial, seu consentimento não cobre o outro uso, que deve, então, ser considerado ilegal.[90]

Possíveis falhas de segurança

As violações de segurança dos bancos de dados biométricos são de difícil detecção e de reparação extremamente dispendiosa. A procura de reparação para violações decorrentes desses incidentes é ainda mais difícil para indivíduos que foram por eles

atingidos. Os dados biométricos não são como senhas, que podem ser alteradas em caso de vazamento. Pelo contrário, eles podem ser usados para identificar e rastrear um indivíduo por toda a vida. Os riscos de segurança são maiores no caso de bancos de dados grandes e centralizados e afetarão particularmente as comunidades que já são marginalizadas. Por esse motivo, bancos de dados centralizados só devem ser considerados em caso de necessidade absoluta e somente quando não houver alternativa viável disponível.[91]

Por último, os riscos de segurança são mais elevados em países onde a indústria tecnológica e a infraestrutura de segurança de dados não existem ou estão insuficientemente desenvolvidas. Nesse contexto de desconfiança, torna-se profundamente preocupante que o governo ou outros agentes retenham os dados biométricos dos indivíduos. Ainda nesse sentido, além de haver a necessidade do reforço de segurança da informação em órgãos públicos retentores de bases de dados, é importante levar em consideração que o respectivo enfraquecimento institucional ou a privatização torna a proteção de dados nesse âmbito ainda mais vulnerável.

O "problema da caixa-preta"

As novas aplicações das tecnologias biométricas estão cada vez mais baseadas no aprendizado de máquina, o que levanta o "problema da caixa preta".[92] A impenetrabilidade desses processos e sistemas é um desafio fundamental para a responsabilização, a prestação de contas e as obrigações públicas relativas à transparência (*accountability*) e para reparações que se façam necessárias no contexto da tomada automatizada de decisões. Dado um significativo viés automatizado em favor de decisões tomadas por máquinas, somado a sistemas técnicos imperfeitos e muitas vezes ultrapassados, a definição de perfis e a correspondência tornam-se difíceis ou impossíveis de contestar, particularmente quando a lógica e os pressupostos por meio dos quais as decisões são tomadas não são claros. Como consequência, torna-se difícil, senão inviável, para os tribunais julgar a veracidade das provas e dos argumentos que forem alegados. A utilização de sistemas informáticos fechados, proprietários e que impedem auditoria e verificação podem ser um obstáculo à transparência dessas tecnologias. *Softwares* de código-fonte aberto devem ser disponibilizados livremente e auditáveis sempre que possível, para que se ofereça à sociedade o conhecimento sobre sua operação, especialmente em aplicações estratégicas e autorizadas ou em parceria com o poder público.

Escala

As tecnologias biométricas estão atualmente implementadas em uma escala sem precedentes e têm, potencialmente, suscitado um estado de vigilância em massa em várias áreas do mundo. Dos aeroportos às praças públicas, das câmeras térmicas aos sistemas de identificação das veias dos dedos, o uso dessas tecnologias para identificar e monitorar indivíduos está se tornando cada vez mais difundido.[93]

Marcos legais nacionais inadequados ou inexistentes

A inadequação ou a inexistência de marcos legais nacionais para o desenvolvimento e a implementação de tecnologias biométricas é um grave problema. A legislação de proteção de dados (caso exista), embora necessária, pode não ser suficiente para lidar com todos os problemas decorrentes desses panoramas. Para tanto, as legislações devem conter regras claras sobre consentimento, legalidade do processamento, limitação de propósito, entre outros pontos. Além disso, vários marcos normativos de proteção de dados apresentam exceções quando se trata do processamento de dados pessoais para o cumprimento da lei. Essas exceções são muitas vezes moldadas em termos vagos e amplos, sem garantias suficientes para a proteção de dados pessoais. Um marco legislativo adequado, em conformidade com as normas internacionais, é necessário para o desenvolvimento e o uso de tecnologias biométricas tanto por agentes públicos quanto por agentes privados. No caso brasileiro, a LGPD apresenta regras mais rígidas para o tratamento de dados pessoais sensíveis, incluindo dados biométricos, como já destacado anteriormente. Todavia, o tratamento desses dados para segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais foge ao escopo da lei, de acordo com seu artigo 4º, III. Assim, são necessárias novas normativas que regulamentem o tratamento de dados nestes âmbitos. No caso específico da segurança pública, uma comissão de juristas já elaborou um anteprojeto de lei (chamada de "LGPD Penal"), que foi apresentado à Câmara dos Deputados[94] e aguarda o prosseguimento da tramitação.

Necessidade e proporcionalidade

Estados e atores privados estão desenvolvendo e implementando tecnologias biométricas para uma lista cada vez maior de finalidades. A disponibilidade da tecnologia é frequentemente considerada uma razão suficiente para seu uso, sem que haja uma avaliação adequada da legitimidade dos seus objetivos. O desenvolvimento e a implementação dessas tecnologias para fins que atingem a dignidade humana – por exemplo, para o monitoramento digital massivo, humilhação ou manipulação – nunca devem ser permitidos.[95] Mesmo quando é identificado um propósito legítimo para o uso da biometria, sua implementação nem sempre atende aos critérios de necessidade e proporcionalidade de forma estrita: a tecnologia tem de ser absolutamente necessária para atingir o escopo e devem inexistir outros meios menos invasivos para fazê-lo. Se tal teste não for realizado, o uso da tecnologia não deve ser permitido, independentemente de sua disponibilidade ou apelo.[96]

Falta de reparação adequada em casos de violações de direitos humanos

Atores públicos e privados que lidam com tecnologias biométricas ainda não disponibilizam reparações adequadas caso ocorram violações de direitos humanos. Por exemplo, se o uso da tecnologia biométrica tiver um resultado discriminatório, não está claro como esse tipo de situação será tratada. Da mesma forma, se a polícia utiliza a tecnologia biométrica para rastrear indivíduos envolvidos em grupos políticos,

religiosos ou outras categorias de expressão protegidas, não está evidente a reparação adequada que será colocada à disposição desses indivíduos. De qualquer maneira, uma premissa para o direito de uma reparação adequada é que as pessoas estejam cientes de que seus dados biométricos estão sendo tratados ou de que uma decisão que a elas interesse foi tomada com base no uso de tecnologias biométricas, o que não ocorre na grande maioria das situações.

Tecnologias biométricas e desafios para a liberdade de expressão e informação

Alguns dos desafios colocados pelo uso de tecnologias biométricas à capacidade das pessoas de exercer seus direitos à liberdade de expressão e informação são semelhantes àqueles trazidos pelas tecnologias previamente existentes. Uma parte desses problemas, entretanto, tem origem em características específicas da biometria e incluem o seguinte:

Efeito inibidor da vigilância em massa na liberdade de expressão

Embora os parâmetros de direitos humanos tenham evoluído para reconhecer que proteções contra vigilância em massa ilegal ou arbitrária são principalmente garantidas pelo direito à privacidade,[97] há um crescente reconhecimento de que a vigilância em massa também tem um efeito inibidor na liberdade de expressão.[98] Se as tecnologias biométricas são usadas para fins de identificação ou perfilamento em espaços públicos, como a utilização de tecnologias de reconhecimento facial para processar imagens faciais capturadas por câmeras de videomonitoramento em ruas, praças, metrôs, estádios ou salas de concertos, elas negam a capacidade dos indivíduos de se comunicarem com confiança e anonimato quando transitam ou exercem outros tipos de atividades em espaços públicos. Da mesma forma, eles impedem diretamente a forma como as ONGs operam com relação à proteção de suas fontes, bem como interferem no papel fiscalizador que essas entidades têm frente aos diferentes poderes que se relacionam na sociedade, principalmente o Estado.[99] Estudos mostram que a consciência de ser vigiado e rastreado pode levar as pessoas a não participarem de reuniões públicas ou da vida social e cultural e a não se expressar e manifestar livremente seus pensamentos, corpos, consciência e crenças religiosas em espaços públicos.[100]

Impacto na liberdade de expressão de grupos específicos

O uso de tecnologias biométricas pode ter um impacto mais severo no direito à liberdade de expressão de minorias ou de grupos que podem se tornar alvo por exercerem esse direito. Como já destacado anteriormente, há evidências de que o reconhecimento facial apresenta diversos vieses de raça, gênero e idade, o que gera violações de liberdade de expressão mais graves para pessoas negras, mulheres, pessoas trans e crianças, por exemplo. Ademais, jornalistas poderiam ser desencorajados/as a conduzir investigações ou estabelecer contatos com suas fontes

de informação se soubessem que poderiam ser monitorados/as, espionados/as e identificados/as pelas tecnologias biométricas em espaços públicos ou privados.[101] O medo de serem rastreados/as e vigiados/as pode ter um forte efeito inibidor sobre esses/as profissionais, o que, por sua vez, impediria o exercício de jornalismo de qualidade e impactaria reportagens investigativas, frustrando o papel que a mídia desempenha na sociedade. Ativistas e opositores políticos podem ter receios semelhantes e, portanto, os mesmos incentivos à autocensura. Eles e elas poderiam ser dissuadidos de exercer seu direito de protesto se, como conseqüência do uso de tecnologias biométricas pelo Estado, lhes forem atribuídas classificações específicas, tais como "manifestantes habituais"[102] ou similares. [103]

Necessidade de transparência e acesso à informação

A utilização generalizada de tecnologias biométricas e a criação de extensos bancos de dados, juntamente com uma falta geral de transparência sobre sua implementação e uso, também levantam desafios para o direito de acesso à informação por parte da população. Quando os governos coletam e armazenam grandes quantidades de dados biométricos, é crucial que o público também tenha o direito de saber o que o governo está fazendo com tais informações. Isso é especialmente um problema quando agentes públicos ou privados aplicam tecnologias de identificação e monitoramento em espaços públicos.

Não há informações acessíveis suficientes sobre quem está desenvolvendo tecnologias biométricas, sobre o tipo de tecnologia que está sendo desenvolvida, sobre quem as está implementando, como e para quais propósitos. Também não se sabe se os desenvolvedores/as e vendedores/as realizam a devida diligência para avaliar o histórico de direitos humanos de quem compra.[104]

Agentes estatais e privados atuam de maneira próxima nos mercados de tecnologias biométricas. Entretanto, o conteúdo e os termos das parcerias público-privadas (PPPs) e dos contratos públicos (por meio dos quais as autoridades públicas compram as tecnologias da indústria) não são tornados públicos. Em geral, os Estados não divulgam suas relações com os desenvolvedores/as, incluindo os critérios para a avaliação das propostas e as atribuições contratuais. Este ambiente opaco e sigiloso faz com que tecnologias biométricas sejam compradas e utilizadas sem o devido escrutínio público, com fracas salvaguardas processuais e supervisão ineficaz. De forma semelhante, as autoridades públicas que lidam com tecnologias biométricas parecem não conduzir avaliações de impacto ou de risco adequadas, que são componentes importantes da responsabilização, da prestação de contas e das obrigações públicas relativas à transparência (*accountability*).[105]

Leis de liberdade e/ou acesso à informação são ferramentas legais poderosas que cidadãs e cidadãos, jornalistas e ativistas podem utilizar para melhorar a transparência governamental e para compreender o uso de dados biométricos pelo governo.[106]

No entanto, as tentativas de acessar informações de órgãos públicos sobre o uso de tecnologias biométricas por meio dessas leis têm se mostrado um desafio.[107] Considerando o grande número de pessoas de quem os dados biométricos são coletados, parece indiscutível que o público em geral tem interesse nos sistemas projetados para armazenar e manipular quantidades significativas de tais dados.[108] Independentemente disso, os órgãos públicos frequentemente falham em publicar proativamente informações sobre tais sistemas de identificação. De maneira geral, essas informações só são divulgadas após acionamento do sistema judicial para questionar negativas de acesso à informação. Os recursos judiciais são normalmente longos e caros na maioria das jurisdições e as e os solicitantes, incluindo jornalistas, cientistas e ativistas, frequentemente desistem de recorrer a eles.

Vale mencionar que algumas iniciativas abordaram a falta de transparência no uso de tecnologias biométricas, reconhecendo que as necessidades políticas devem ser conciliadas com preocupações éticas e que a implementação de tais medidas deve ser baseada em abertura e transparência.[109]

Tecnologias biométricas e liberdade de expressão: estudos de caso

Reconhecimento facial

Propósitos e uso de tecnologias de reconhecimento facial

O reconhecimento facial é o processamento automático de imagens faciais digitais dos indivíduos para três propósitos principais:

- **Verificação**: é a comparação de dois modelos biométricos para determinar se a pessoa exibida nos dois modelos é a mesma (comparação um para um).
- **Identificação**: é a comparação do modelo de uma pessoa com vários modelos de um banco de dados para averiguar se essa pessoa está nesse banco (comparação um para muitos). Quando o reconhecimento facial é usado para este fim em tempo real, também é referido como "reconhecimento facial automatizado ou em tempo real" (AFR ou LFR, nas siglas em inglês). Embora tanto a autenticação um para um como a autenticação um para muitos apresentem problemas[110], o uso do reconhecimento facial para fins de identificação um para muitos prejudica de forma mais grave o exercício do direito à liberdade de expressão das pessoas.
- **Categorização**: é utilizada para traçar o perfil e categorizar pessoas com base em suas características pessoais, tais como sexo, idade e origem étnica[111].

A utilização do reconhecimento facial tem aumentado de forma constante nos últimos anos. Vários governos ao redor do mundo estão discutindo e aplicando regras que preveem a implementação em massa de reconhecimento facial em espaços públicos para fazer cumprir a lei[112]. Em alguns países, recorre-se amplamente ao argumento de segurança pública para justificar a vigilância cada vez maior dos espaços públicos.[113]

O reconhecimento facial também é utilizado pelo setor privado para os mais diversos fins. Internacionalmente são frequentes os casos de varejistas que se valem do reconhecimento facial, por exemplo, para verificar a presença de potenciais criminosos/as em suas lojas.[114] Alguns foram além e adotaram o reconhecimento facial para monitorar as reações de clientes aos itens na loja[115] ou como um sistema para os clientes fazerem compras[116]. Empresas de entretenimento aplicam o reconhecimento facial para identificar as pessoas que já adquiriram ingressos e facilitar seu acesso a serviços ou locais. Empresas de transporte implementaram sistemas de reconhecimento facial em painéis publicitários localizados em estações de metrô para identificar as reações das pessoas aos anúncios (o mecanismo reconheceria se elas estariam felizes, insatisfeitas, surpreendidas ou neutras) e supostamente relacioná-las com suas características fisiológicas (idade e sexo)[117]. Além disso, empresas que controlam aplicativos de transporte individual de passageiro apoiam-

se no reconhecimento facial como uma salvaguarda contra fraudes e para verificar a identidade de seus e suas motoristas.[118,119] Por fim, como mencionado anteriormente, vários desenvolvedores de *smartphones* permitem que usuários desbloqueiem seu telefone usando o recurso de reconhecimento facial.[120]

Devido aos problemas já relatados e a essa utilização em massa, algumas cidades, especialmente nos Estados Unidos, estão indo na direção oposta e banindo ou impondo moratórias para o uso do reconhecimento facial para determinados fins.[121] Da mesma forma, recentemente, vários desenvolvedores e desenvolvedoras de tecnologias de reconhecimento facial tomaram medidas (ainda que insuficientes) para limitar ou suspender seu desenvolvimento e sua implementação.[122] O escopo desses compromissos ainda não está claro, mas essas medidas podem ser vistas como um sinal das crescentes pressões para limitar ou banir o uso indiscriminado do reconhecimento facial para o cumprimento da lei. Destaca-se, no entanto, que essa não é a situação atual em outras partes do mundo, como a América Latina, que parece estar indo na direção contrária, adotando tecnologias de reconhecimento facial de maneira ampla e elaborando leis para justificá-las.[123] Ademais, poucas vozes parecem levantar essas preocupações e atribuir igual peso aos perigos da implementação de sistemas de reconhecimento facial por agentes privados.[124] Essa falta de preocupação contrasta fortemente com o uso – não só pontual como também mais amplo – cada vez maior dessa tecnologia por tais agentes.[125]

A pandemia de Covid-19 chamou ainda mais a atenção para as tecnologias de reconhecimento facial. Desenvolvedores/as têm aproveitado a emergência de saúde pública para impulsionar novos e mais amplos usos do reconhecimento facial, tanto por agentes públicos quanto por agentes privados. Governos ao redor do mundo estão implementando a cada dia mais esse tipo de tecnologia para fins de monitoramento, para impor quarentenas ou rastrear rotas de infecção.[126] O impulso para o uso de tecnologias de reconhecimento facial é tão grande que os desafios técnicos levantados pelo uso obrigatório ou recomendado de máscaras faciais já foram superados.[127] Algumas empresas, por exemplo, começaram a desenvolver algoritmos de reconhecimento "periocular" que detectam e reconhecem rostos com base apenas na região dos olhos entre as maçãs do rosto e as sobrancelhas.[128] Ainda assim, a tecnologia de reconhecimento facial está sendo proposta como uma solução para a Covid-19 sem que haja uma análise ampla e aprofundada dos seus impactos, devendo-se levar também em consideração a probabilidade de ocorrência de mais erros de identificação quando se toma como referência somente uma parte dos rostos. Ao contrário, tais iniciativas emergem como parte de um esforço maior para estabelecer uma infraestrutura de vigilância em constante expansão sob o pretexto de uma resposta à pandemia.[129]

Desafios trazidos pelo reconhecimento facial ao exercício dos direitos humanos

Todos os usos da tecnologia de reconhecimento facial – seja pelo setor público, seja pelo privado – têm um impacto na capacidade das pessoas de exercer seus direitos humanos. Por vezes, o reconhecimento facial é mais danoso quando utilizado por agentes privados. Nesse contexto, os/as consumidores/as são frequentemente convencidos/as a adotar essa tecnologia em sua esfera privada (em casa, em seus relacionamentos com a família e os amigos ou no trabalho) para objetivos cada vez mais fúteis, nenhum dos quais sendo justificável ou proporcional à violação dos direitos humanos que advém dela.

Muitas preocupações sobre a implementação e o uso do reconhecimento facial são semelhantes àquelas listadas anteriormente para outras tecnologias biométricas. Essa tecnologia é frequentemente utilizada sem uma base legal, na ausência de qualquer marco legislativo específico ou qualquer salvaguarda adequada para os direitos humanos e também sem consulta pública prévia. Entretanto, devido a suas características específicas, as tecnologias de reconhecimento facial impõem desafios específicos ao exercício dos direitos humanos e da liberdade de expressão. Isso porque o reconhecimento facial tem duas particularidades em relação a outros dados biométricos: por um lado, pode ser realizado sem que a pessoa esteja ciente disso; por outro, pode distinguir características protegidas pelo direito internacional (raça, religião, sexo e outras).

Nesse sentido, as seguintes preocupações devem ser consideradas:

- **Consentimento**: as tecnologias de reconhecimento facial não precisam de contato e nem de um comportamento ativo por parte das pessoas cujos dados são coletados. Por essa razão, os atores que empregam o reconhecimento facial podem facilmente submeter os alvos a ele sem seu conhecimento ou consentimento.[130] Por exemplo: o Facebook, um dos primeiros desenvolvedores de tecnologias de reconhecimento facial, tem utilizado amplamente as imagens faciais dos usuários e usuárias para treinar seu sistema de reconhecimento facial, sem informá-los/as ou pedir o consentimento deles/as.[131] E, mesmo quando o uso do reconhecimento facial é descoberto, pode ser difícil estabelecer quando o consentimento fornecido é válido. Estudos têm argumentado que, de qualquer maneira, o uso do reconhecimento facial do Facebook não atende aos padrões de consentimento, obscurecendo seus riscos e corroendo a autonomia coletiva.[132]
- **Falta de transparência**: embora a falta de transparência no uso de tecnologias biométricas seja uma preocupação geral, o reconhecimento facial levanta preocupações ainda maiores por ser mais invasivo. Como explicado anteriormente, uma imagem facial pode ser capturada sem que o alvo esteja ciente disso ou ainda sem que seja informado sobre o uso da tecnologia

em determinado espaço. Esse fato, aliado à falta de transparência sobre a utilização dessas tecnologias tanto por agentes públicos quanto por agentes privados, deixa os indivíduos sem acesso suficiente às informações adequadas e totalmente expostos a abusos.

- **Precisão**: semelhante a outras tecnologias biométricas, o reconhecimento facial é baseado em uma estimativa estatística da correspondência entre os elementos comparados. Portanto, é intrinsecamente falível e não está livre de reproduzir discriminações sociais, carregando intrinsecamente os vieses de seus programadores e programadoras e da base de dados nas quais são treinados[133]. Apesar de o discurso que favorece a sua aplicação frequentemente defender a objetividade desses sistemas, numerosos estudos demonstram que o reconhecimento facial falha em termos de precisão, particularmente para grupos marginalizados, vítimas de preconceitos estruturais, sub-representados ou historicamente desfavorecidos[134,135]. Para que o reconhecimento facial esteja livre de vieses, a qualidade dos dados e a abrangência dos bancos de dados de treinamento são essenciais. Se a qualidade dos dados não for assegurada ou se os bancos de dados de teste forem sobre ou sub-representativos de certas características, o reconhecimento facial está muito longe de ser confiável,[136] o que é especialmente problemático em casos de vieses raciais discriminatórios.[137] A precisão dos sistemas de reconhecimento facial é extremamente importante, já que o reconhecimento equivocado é bem mais do que um inconveniente, podendo resultar em graves consequências. Um falso negativo em uma busca um para um pode impedir que um indivíduo tenha acesso a serviços ou instalações. Um falso positivo em uma busca um para muitos pode ocasionar prisões equivocadas ao inserir incorretamente pessoas em determinadas listas de pessoas em contextos que mereceriam maior escrutínio ou baseados em rótulos prévios não necessariamente adequados. Uma vez que isso acontece, parece difícil, senão impossível, reverter a situação.[138] Essa tendência intrínseca de vieses não é sanada por correções ou ajustes nos sistemas tecnológicos, até mesmo porque há o risco de, sob este argumento, recolherem-se mais dados para justificar análises mais acuradas. Da mesma forma, não é possível remediar o problema ou aceitar a implementação dessas tecnologias sob argumento de um eventual aprimoramento do sistema de reconhecimento facial, contexto no qual é imprescindível uma análise de necessidade e proporcionalidade na sua retenção e utilização.
- **Pouca ou nenhuma supervisão**: salvo algumas exceções, órgãos cujo papel é fazer cumprir a lei têm pouca ou nenhuma supervisão no que se refere ao uso do reconhecimento facial em vários países. Na maioria dos lugares, nada explicitamente impede as autoridades de utilizar o reconhecimento facial em câmeras de videomonitoramento ao vivo, transformando os/as transeuntes em participantes desavisados/as de processos de reconhecimento pessoal virtual.[139] Soma-se a isso o fato de não haver regras sobre a retenção dos dados coletados por meio do uso de reconhecimento facial. Essas preocupações são igualmente relevantes ao avaliar-se a forma como agentes

privados usam o reconhecimento facial: na ausência de supervisão apropriada, as empresas aplicam o reconhecimento facial para fins e de maneiras que violam os padrões de direitos humanos.

- **Falta de padrões:** as normas e as melhores práticas para a implementação do reconhecimento facial ainda estão em processo de elaboração.[140] Destaca-se, também, a existência de apelos para a elaboração de um código de conduta estatutário[141]. Apesar da falta de normas, a tecnologia de reconhecimento facial continua a ser utilizada tanto em espaços públicos quanto em espaços privados em todo o mundo. Trata-se de uma preocupante lacuna que não pode ser preenchida simplesmente por apelos ao uso ético: as preocupações éticas devem ser tratadas por uma estrutura regulatória adequada que esteja de acordo com os padrões internacionais de direitos humanos.[142]
- **Dupla finalidade**: a grande maioria dos sistemas de reconhecimento facial comercializados por atores privados pode ser utilizada para fins diferentes daqueles para os quais eles foram projetados ou previstos. Em outras palavras, o potencial de abuso é alarmante. A falta de um marco regulatório que apresente garantias contra o tratamento de dados para outros propósitos, que atribua responsabilidade e preveja reparações adequadas caso isso aconteça amplia drasticamente os riscos. No caso brasileiro, devem-se destacar os princípios de finalidade e adequação, presentes na LGPD, no caso de tratamento de dados pessoais, os quais também devem ser respeitados por legislação futura que regule o tratamento de dados pessoais para as exceções presentes no art. 4º, III, como a segurança pública.
- **Falta de necessidade e proporcionalidade**: muitos casos de uso de tecnologias de reconhecimento facial já foram considerados falhos no teste de necessidade e proporcionalidade. O uso dessa tecnologia nas escolas com o objetivo de controlar o acesso de estudantes, entre outros exemplos, foi condenado tanto por autoridades de proteção de dados quanto por tribunais em determinados países.[143]

Desafios trazidos pelo reconhecimento facial para a liberdade de expressão e informação

Do ponto de vista da liberdade de expressão, a implementação e o uso da tecnologia de reconhecimento facial provocam os seguintes problemas adicionais:

- **Direito de permanecer anônimo**: o uso do reconhecimento facial (e especialmente do reconhecimento facial em tempo real) em espaços públicos é um desafio notório ao anonimato. Ele limita a possibilidade de se locomover anonimamente e o uso anônimo de serviços e, em termos mais gerais, a possibilidade de permanecer incógnito/a. Proteger o espaço público para o exercício dos direitos e liberdades fundamentais, em particular o direito à liberdade de expressão, é crucial. Se aplicada extensivamente, por exemplo em câmeras de videomonitoramento ou naquelas utilizadas em uniformes policiais, a tecnologia de reconhecimento facial pode redefinir

significativamente a natureza do espaço público,[144] com usos que não passam no teste da necessidade e proporcionalidade. O uso indiscriminado e não direcionado do reconhecimento facial que leva à vigilância em massa nos espaços públicos nunca deve ser permitido.[145]

- **Direito de protesto**: o uso de tecnologias de reconhecimento facial durante os protestos pode desencorajar as pessoas a participar desse tipo de movimentação, tendo evidentes implicações negativas em relação ao funcionamento eficaz da democracia participativa.[146] Mesmo se aplicado para coibir violência policial em protestos, o reconhecimento facial pode ainda afetar aqueles manifestantes que não se envolvem em violência, além de demais transeuntes. Em outras palavras, a aplicação do reconhecimento facial pode gerar um efeito inibidor nos indivíduos e fazê-los alterar seu comportamento e se abster de exercer seus direitos de protesto. Assim, as pessoas podem ser desencorajadas de encontrar indivíduos ou organizações, frequentar reuniões ou participar de certas manifestações. Da mesma forma, o reconhecimento facial em tempo real em espaços públicos pode ser utilizado para atingir jornalistas, causando um efeito inibidor nos indivíduos e sociedades no tocante ao acesso à informação sobre protestos.
- **Liberdade religiosa**: o uso de tecnologias de reconhecimento de rostos pode interferir na liberdade religiosa das pessoas.[147] Isso pode acontecer, por exemplo, se as pessoas forem obrigadas a descobrir seus rostos em espaços públicos de maneira contrária à sua liberdade de expressão cultural e religiosa e/ou se estiverem sujeitas a multas ou outras consequências negativas caso não o façam.

Reconhecimento de emoções

Propósitos e uso das tecnologias de reconhecimento de emoções

A tecnologia de reconhecimento de emoções pretende inferir o estado afetivo interno de um indivíduo com base em características tais como movimentos musculares faciais, tonalidades vocais, movimentos corporais e outros sinais biométricos. Essa tecnologia é projetada para usar o aprendizado de máquina para analisar expressões faciais e outros dados biométricos e, subsequentemente, inferir o estado emocional de uma pessoa. O setor privado está utilizando estas tecnologias para direcionar sua publicidade, atrair a atenção de clientes e influenciar suas escolhas, entre outros propósitos. Ela também é extremamente atraente para governos e órgãos cujo papel é fazer cumprir a lei e manter a ordem, já que pretendem antever atividades criminosas, eliminar ameaças terroristas e policiar espaços públicos e privados.[148]

Assim como ocorre com outras tecnologias biométricas, o uso do reconhecimento de emoções envolve a coleta em massa de dados pessoais sensíveis de forma invisível e sem responsabilização, sem prestação de contas e obrigações públicas relativas à transparência (*accountability*), permitindo o rastreamento, o monitoramento, a categorização, a pontuação ou a criação de perfis de indivíduos, muitas vezes em tempo real. Essa tecnologia é usada em vários ambientes, por patrulhas de fronteira ou policiais, para identificar aparentes "comportamentos suspeitos" ou "terroristas".[149] Tanto os Estados como as empresas privadas testam e empregam tecnologias de reconhecimento de emoções, o que tem consequências de larga abrangência, muitas vezes decorrentes do trabalho conjunto desses agentes.[150]

Eficácia das tecnologias de reconhecimento de emoções

Há duas premissas fundamentais que sustentam as tecnologias de reconhecimento das emoções: a primeira é que é possível conhecer as emoções internas de uma pessoa a partir de suas expressões externas, e a segunda é que as emoções internas são expressadas globalmente de forma discreta e uniforme. Esta ideia, conhecida como Teoria Básica das Emoções (BET, na sigla em inglês), sugere que os seres humanos de quaisquer culturas poderiam discernir de forma confiável os estados emocionais com base em expressões faciais, que supostamente seriam universais.[151] A BET tem sido extremamente influente, até mesmo inspirando programas populares de televisão e filmes.[152] No entanto, ao longo dos anos os cientistas investigaram, contestaram e rejeitaram em grande parte a validade dessas afirmações e desacreditaram o argumento de universalidade da expressão das emoções[153].

Tecnologias de reconhecimento de emoções para identificar, monitorar, rastrear e classificar indivíduos em diversas categorias são, portanto, fundamentalmente problemáticas. Não por funcionarem, mas porque as partes interessadas na construção e utilização dessas tecnologias afirmam que elas funcionam.[154] Mesmo diante disso, pesquisas acadêmicas e aplicações no mundo real continuam a ser embasadas nas premissas básicas da universalidade da expressão de emoções, apesar de estas estarem conectadas a estudos científicos duvidosos e a uma história de pseudociência desacreditada e racista.[155]

Desafios trazidos aos direitos humanos por tecnologias de reconhecimento de emoções

Muitas preocupações sobre a utilização de tecnologias de reconhecimento de emoções são similares às mencionadas anteriormente em relação a tecnologias biométricas e reconhecimento facial. Esse outro tipo de tecnologia também está sendo desenvolvido e implementado de maneira invisível, opaca e sem limitações, mecanismos de supervisão ou consultas públicas. Além disso, destacamos as seguintes preocupações:

- As tecnologias de reconhecimento de emoções se baseiam em **premissas pseudocientíficas com falhas e argumentos há muito desacreditados**. Como mencionado anteriormente, baseiam-se no pressuposto de que as expressões são universais, de que os estados emocionais podem ser desvendados nas expressões faciais e de que tais inferências são suficientemente confiáveis para serem utilizadas na tomada de decisões. Trata-se de três premissas que têm sido desacreditadas por cientistas de todo o mundo há décadas, mas isso parece não impedir a realização de experimentações e a venda dessas tecnologias. Embora existam crescentes preocupações técnicas sobre tecnologias de reconhecimento de emoções por parte de desenvolvedores privados, a maioria dessas críticas aborda as preocupações técnicas da indústria de vigilância em detrimento de implicações dos direitos humanos para aqueles que estão sendo monitorados/vigiados ou para vítimas de falsos positivos.[156]

Desafios trazidos pelas tecnologias de reconhecimento de emoções para a capacidade das pessoas de exercer sua liberdade de expressão

O uso de tecnologias de reconhecimento de emoções apresenta desafios semelhantes aos do reconhecimento facial. A concepção, o projeto e a implementação do reconhecimento de emoções acrescentam uma camada de obstáculos e arbitrariedade a uma tendência já preocupante dadas a falta de uma base legal, a ausência de salvaguardas e a natureza extremamente intrusiva dessas tecnologias.

Utilizando o argumento de que elas inferem os “verdadeiros” estados internos das pessoas para proceder a tomadas de decisões baseadas nessas inferências, a implementação de tecnologias de reconhecimento de emoções faz com que presunções **arbitrárias e unilaterais** sobre os indivíduos sejam assumidas como verdades, o que tem duas implicações significativas. Em primeiro lugar, isso dá espaço a um significativo efeito inibidor na capacidade dos indivíduos de exercer seu direito à liberdade de expressão. Isso porque a ciência de não apenas ser visto/a e identificado/a, mas também **julgado/a e classificado/a**, funciona como um mecanismo de intimidação

que faz com que os indivíduos se adaptem a formas de autoexpressão classificadas socialmente como “corretas” para que não sejam classificados como “suspeitos/as” ou “perigosos/as”, a depender dos usos específicos aplicados. Em segundo lugar, dada a ampla gama de aplicações atuais, esses usos podem naturalizar a vigilância em massa como parte da vida cotidiana das pessoas, particularmente em locais de participação cívica. Nesse sentido, é importante ressaltar que a liberdade de expressão inclui o direito de não falar ou não se expressar.[157]

A natureza dessas tecnologias também está em desacordo com a ideia de proteção da dignidade humana e constitui um método totalmente desnecessário para alcançar os supostos objetivos de segurança nacional, ordem pública, entre outros. Enquanto as normas internacionais de direitos humanos estabelecem a segurança nacional e a ordem pública como justificativas legítimas para a restrição de direitos humanos, incluindo restrições à liberdade de expressão e à privacidade, essas critérios não dão aos Estados liberdade para adquirir e usar arbitrariamente tecnologias que impeçam as pessoas de exercer seus direitos humanos, nem permitem aos Estados a violação de direitos sem fornecer justificativas afuniladas e razões válidas e específicas para fazê-lo.

Há também uma surpreendente **falta de transparência** por parte dos Estados e de empresas no contexto da concepção, do projeto, do desenvolvimento e do uso de tecnologias de reconhecimento de emoções. Embora tanto *startups* quanto empresas de tecnologia já bem estabelecidas sejam impelidas a desenvolver esse tipo de sistema, preocupações relevantes estão muito pouco ou nunca presentes no debate público. Isso ocorre em relação à justificativa das autoridades para comprar e incentivar esses produtos, informações sobre mecanismos de supervisão, salvaguardas a serem consideradas em períodos de teste e considerações sobre a proteção de dados. Dadas as múltiplas formas por meio das quais as tecnologias de reconhecimento de emoções ameaçam os direitos humanos, os Estados que as utilizam e compram têm a obrigação de assegurar a devida responsabilidade, a segurança jurídica e a transparência processual e legal sobre as respectivas aquisição e implementação.[158] As empresas também estão sujeitas a obrigações de transparência segundo os Princípios Orientadores sobre Empresas e Direitos Humanos, o que exige que elas tenham processos que permitam a reparação adequada de quaisquer impactos adversos aos direitos humanos que causem ou para os quais contribuam.[159]

Recomendações da ARTIGO 19

Tendo em vista o que foi exposto, a ARTIGO 19 sugere que as partes interessadas devem adotar uma abordagem baseada nos direitos humanos para a concepção, o projeto, o desenvolvimento e a implementação de tecnologias biométricas, além de cumprir as recomendações listadas a seguir.

É importante que, até que estas recomendações sejam implementadas, haja uma moratória para o desenvolvimento e o uso de todas essas tecnologias, tanto pelos Estados como pelos atores privados.

Recomendação 1:
A vigilância biométrica em massa deve ser banida

Os Estados devem proibir o uso de tecnologias biométricas para o processamento indiscriminado e não direcionado de dados biométricos em espaços públicos e de acesso público, tanto offline como online. Os Estados também devem interromper o financiamento para programas e sistemas de processamento biométrico que possam contribuir para a vigilância em massa em espaços públicos e privados, quando acessados pelo público em geral.

Recomendação 2:
A concepção, o projeto, o desenvolvimento e o uso de tecnologias de reconhecimento de emoções devem ser banidos

Por princípio, as tecnologias de reconhecimento de emoções são essencialmente falhas e se baseiam em métodos discriminatórios e contestados por pesquisadores dos campos da computação afetiva e da psicologia. Elas nunca cumprem estritamente os testes de necessidade, proporcionalidade, legalidade e legitimidade. Portanto, seus desenvolvimento, venda, transferência e uso devem ser proibidos.

Os Estados também devem incorporar e aplicar normas internacionais que proíbam a concepção, o projeto, o planejamento, o desenvolvimento, a implementação, a venda, a exportação e a importação dessas tecnologias, em reconhecimento à sua fundamental incompatibilidade com os direitos humanos.

Recomendação 3:
A concepção, o projeto, o desenvolvimento e o uso de tecnologias biométricas devem respeitar os princípios de legitimidade, proporcionalidade e necessidade

Tanto os Estados como os atores privados devem realizar uma avaliação adequada caso a caso sobre a legitimidade do uso de tecnologias biométricas para um determinado fim. A simples disponibilidade de uma tecnologia nunca deve se tornar motivo suficiente para sua implementação e uso. A concepção, o projeto, o desenvolvimento e o uso dessas tecnologias devem ser restritos a fins lícitos que sejam consistentes com as normas de direitos humanos e que não violem a dignidade humana.

No que concerne a tecnologias mais invasivas como o **reconhecimento facial**, o ponto de partida para a avaliação é reconhecer que, devido a essa característica intrínseca, a tecnologia nunca é inofensiva. Por essa razão, os Estados devem considerar a proibição do uso do reconhecimento facial como regra e a possibilidade de torná-lo uma exceção, que deve ser justificada e vinculada a um propósito específico.

Quando um propósito legítimo para o uso da biometria é identificado, seu desenvolvimento e sua implementação devem atender ao teste de necessidade e proporcionalidade de forma estrita: a tecnologia deve ser absolutamente necessária para atingir o objetivo e devem inexistir outros meios menos invasivos de fazê-lo. Quando não se caracterizar uso massivo, os Estados devem evitar o uso generalizado de tecnologias biométricas e, especialmente, de reconhecimento facial, em espaços públicos. A aplicação dessas tecnologias em espaços públicos limita a capacidade dos indivíduos de se expressar e de participar da vida social. É da maior importância que os Estados resistam à naturalização da vigilância, preservem o papel do espaço público para a democracia e, portanto, garantam os direitos dos indivíduos de permanecer anônimos, de protestar e de se expressar em tal espaço.

Os Estados devem garantir que tanto eles quanto agentes privados jamais utilizem tecnologias biométricas para atingir indivíduos ou grupos que desempenham papéis significativos na promoção dos valores democráticos, como jornalistas e ativistas.

Recomendação 4:
Os Estados devem estabelecer marcos legislativos adequados para a concepção, o projeto, o desenvolvimento e o uso de tecnologias biométricas

Para os usos legítimos que atendam ao teste de necessidade e proporcionalidade, os Estados devem desenvolver um marco legislativo adequado para o desenvolvimento e a implementação de tecnologias biométricas. Essa estrutura deve incluir, no mínimo:

- regras sobre coleta, tratamento e armazenamento que protejam adequadamente os dados biométricos dos indivíduos e forneçam garantias suficientes contra violações de segurança;
- requisitos relativos à qualidade dos dados utilizados para a programação das tecnologias e a implementação obrigatória de auditorias internas, testes de precisão e de identificação de vieses raciais e de gênero;
- a obrigação de realizar avaliações prévias de impacto de proteção de dados e avaliações de impacto sobre os direitos humanos, sujeitas a revisão contínua;
- a obrigação, tanto para desenvolvedores/as como para usuários/as, adaptada ao nível dos riscos identificados, de prevenir e minimizar os riscos correspondentes;
- código de conduta vinculante para utilização por órgãos cujo papel é fazer cumprir a lei;
- disposições específicas para evitar a utilização dos sistemas biométricos para outros propósitos diferentes daqueles originalmente declarados, tanto por atores públicos quanto privados.

Além disso, os Estados devem estabelecer parâmetros em seus marcos regulatórios dedicados a traçar limites à biometria.

Recomendação 5:
A concepção, o projeto, o desenvolvimento e o uso de tecnologias biométricas devem ser objeto de um debate público, aberto e transparente

Como o uso de tecnologias biométricas afeta cada vez mais os valores democráticos e múltiplos processos sociais críticos, sua concepção, seu projeto, sua implementação e seu desenvolvimento só devem ser permitidos após um debate público e amplo. É essencial que redes e coalizões da sociedade civil e de outros especialistas participem adequadamente desse debate. Isso impedirá que os direitos e liberdades individuais sucumbam aos interesses econômicos de qualquer indústria e também representará obstáculo para que os governos utilizem argumentos de segurança vagos e excessivamente abrangentes para naturalizar a vigilância em massa.

Recomendação 6:
Os requisitos de transparência devem ser impostos e implementados integralmente por cada setor

Os Estados devem divulgar publicamente todas as atividades existentes e planejadas e os usos de tecnologias biométricas. Deve haver também uma obrigação específica de realizar consultas públicas sobre questões como as consequências para os direitos humanos das compras dessas tecnologias e ainda sobre se as tecnologias em questão serão eficazes para atingir os objetivos pretendidos.

Os Estados devem assegurar o mais alto nível de transparência e supervisão pública dos processos de compras públicas para a aquisição, o desenvolvimento e o uso de tecnologias biométricas. A transparência deve incluir os critérios para a avaliação das propostas, os termos das parcerias público-privadas, o conteúdo dos contratos públicos e relatórios públicos regulares sobre aprovações, compras e uso.

Os Estados devem garantir o direito de acesso às informações relacionadas à concepção, ao projeto, ao desenvolvimento e à implementação de tecnologias biométricas de acordo com os parâmetros internacionais. Adicionalmente, os Estados devem considerar as informações sobre tecnologias biométricas como “informação pública” no âmbito das leis de acesso à informação e publicá-las proativamente, bem como fornecê-las mediante pedidos de acesso.

Os Estados e atores privados devem publicar regularmente as respectivas avaliações de impacto sobre a proteção de dados, avaliações de impacto sobre os direitos humanos e relatórios de avaliação de risco, juntamente com uma descrição das medidas tomadas para mitigar os riscos e proteger os direitos humanos dos indivíduos. Essas publicizações não devem ocorrer somente de maneira protocolar, mas, sim, devem ser realizadas de forma a permitir e a facilitar o *feedback* e o diálogo, bem como resistências a possíveis implementações.

Recomendação 7:
A responsabilização e o acesso à reparação adequada devem ser garantidos

Os marcos legislativos para o desenvolvimento e a implementação de tecnologias biométricas devem prever estruturas claras de responsabilização, prestação de contas e obrigações públicas relativas à transparência (*accountability*) e também medidas de auditoria independentes. Os Estados devem condicionar a participação do setor privado nas tecnologias biométricas utilizadas para fins de vigilância – desde a pesquisa e o desenvolvimento até a comercialização, a venda, a transferência e a manutenção – à devida diligência e a um histórico de cumprimento das normas de direitos humanos.

Os parâmetros legislativos também devem assegurar o acesso a reparações adequadas aos cidadãos e cidadãs cujos direitos forem violados pelo uso de tecnologias biométricas.

Recomendação 8:
O setor privado deve conceber, projetar, desenvolver e implementar sistemas biométricos de acordo com os padrões de direitos humanos

As empresas envolvidas na concepção, no projeto, no desenvolvimento, na venda, na distribuição e na implementação de tecnologias biométricas devem:

- garantir a **proteção e o respeito às normas de direitos humanos**, adotando, para isso, uma abordagem centrada no ser humano e realizando uma avaliação prévia de impacto aos direitos humanos;
- estabelecer procedimentos adequados e contínuos de **avaliação de riscos** a fim de identificar riscos aos direitos e liberdades das pessoas (em particular, o direito à privacidade e à liberdade de expressão) decorrentes do uso de tecnologias biométricas, bem como adotar uma abordagem de minimização de riscos;
- Fornecer **reparações adequadas e eficazes** em caso de violação dos direitos humanos das pessoas.

Notas

1 O efeito inibidor – em inglês, "*chilling effect*" – ocorre quando pessoas não exercem legitimamente seus direitos pela ameaça de algum tipo de sanção. No caso da utilização de reconhecimento facial em espaços públicos, por exemplo, as liberdades de expressão e de associação podem ser limitadas quando se sabe que há monitoramento em curso, mesmo quando o ato for protegido pelo Direito.

2 A moratória aqui referida diz respeito a usos que possam atender aos critérios de legalidade, necessidade e proporcionalidade – conforme requerem os padrões internacionais de direitos humanos. Para usos que já demonstraram não cumprir esses critérios, como, por exemplo, a utilização de tecnologias biométricas que permitam vigilância em massa, discriminatória e enviesada, a ARTIGO 19 já tem posicionamento pelo respectivo banimento. Ver: Organizações sem unem em chamada para banimento global de usos de reconhecimento facial e biométrico, 09 de junho de 2021.

3 Ver: Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data, Direção Geral dos Direitos Humanos e Assuntos Legais do Conselho da Europa, janeiro 2014, 44p. Federações Desportivas internacionais também incluem reconhecimento facial ou remoto da íris, antropometria (medição da morfologia corporal) ou *medidas fisiológicas* (medição de funções corporais como a frequência cardíaca, pressão arterial e outros).

4 Ver: S. Hood, Biometric Marketing: What Is Biometric Technology and How Can Marketers Use It?, Hitsearch, 15 de outubro de 2018.

5 Ver: Caso Rosenbach versus Six Flags Entertainment Corporation (2019 IL 123186), da Suprema Corte de Illinois (EUA).

6 Ver: Painel de especialistas a pedido da Comissão Europeia, Ethics and data protection, 14 de novembro de 2018.

7 Ver: Parecer 4/2015 da Autoridade Europeia para a Proteção de Dados, Towards a new digital ethics, data dignity and technology, 11 de setembro de 2015.

8 Ver: Centre for Data and Ethics and Innovation, Interim report: Review into bias in algorithmic decision-making, julho de 2019.

9 Ver: Documento do Alto Comissariado das Nações Unidas para os Direitos Humanos: Practical recommendations for the creation and maintenance of a safe and enabling environment for civil society, based on good practices and lessons learned, A/HRC/32/20, 11 de abril de 2016.

10 Na China, por exemplo, o Estado está usando um aplicativo para controlar o acesso das pessoas aos espaços públicos, enviando seus dados à polícia. Ver: New York Times, In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, 1 de março de 2020.

No Reino Unido, o governo estava planejando acrescentar funcionalidades de reconhecimento facial no aplicativo patrocinado pelo NHS para rastreamento de contatos, e anunciou que este reconhecimento facial poderia ser a base para a emissão de passaportes de imunidade. Ver: The Telegraph, NHS app adds face-scanning sign ups in step towards immunity certificates, 19 de maio de 2020.

Em Liechtenstein, parte da população agora usa pulseiras eletrônicas que monitoram a temperatura da pele, pulsação e outros dados biométricos. O governo planeja lançar o esquema de pulseiras para todo o país. Ver: L. Cendrowicz, Coronavirus Testing: Liechtenstein tracks virus with pioneering biometric bracelets, iNews.co.uk, 16 de abril de 2020.

11 Ver: BBC News, Coronavirus: NHS app paves the way for immunity passports, 27 de maio de 2020.

12 Atualmente, o uso destes capacetes de vigilância está confirmado na China, Dubai e Itália. Ver: Business Insider, Police in China, Dubai, and Italy are using these surveillance helmets to scan people for COVID-19 fever as they walk past and it may be our future normal, 17 de maio de 2020.

13 Ver: V. Marda, Papering over the crack: on privacy versus health, em Data Justice and Covid-19: Global Perspectives, 2020.

14 Ver: Regulamento 2018/1725 do Parlamento Europeu e do Conselho, 23 de outubro de 2018.

O Regulamento acima versa sobre a proteção de pessoas naturais a respeito do processamento de dados pessoais pelos órgãos, escritórios, agências e instituições da UE e a livre circulação de tais dados, e a revogação do Regulamento (EC) No 45/2001 e da Decisão No 1247/2002/EC, Artigo 3(18). Ver: Diretiva 2016/680 do Parlamento Europeu e do Conselho, 27 de abril de 2016.

Ela se refere à proteção de pessoas naturais a respeito do processamento de dados pessoais pelas autoridades competentes para os fins de prevenção, investigação, detecção ou processos criminais ou a execução de sanções penais, e sobre a livre circulação de tais dados e a revogação da Decisão 2008/977/JHA (Diretiva para cumprimento da lei) do Council Framework Decision, Artigo 3 (13). Ver: Regulamento 2016/679 do Parlamento Europeu e do Conselho, 27 de abril de 2016.

O referido Regulamento aborda a proteção de pessoas naturais a respeito do processamento de dados pessoais e da livre circulação de tais dados, e revogação da Diretiva 95/46/EC (do GDPR), Artigo 4(14).

15 Ver: Opinion 3/2012 on developments in biometric technologies, do Article 29 Data Protection Working Party.

16 No dispositivo, a LGPD determina que dado pessoal sensível seria aquele "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

17 Ainda segundo o art. 5º, inciso X da LGPD, o tratamento é "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".

18 Ver: D. Hambling, The Pentagon has a laser that can identify people from a distance–by their heartbeat, MIT Technology Review, 27 de junho de 2019.

19 Ver: E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer Netherlands, 2019.

20 Ver: Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192, Brussels, 22 de março de 2012, p. 2.

21 ARTIGO 19, Emotional Entanglement: Freedom of Expression Implications of China's Emotion Recognition Market, 2020.

22 Ver: Association for Psychological Science, Corrigendum: Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, 2016; e L. Feldman Barrett et al., Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest, 20(1) , 2019.

23 Ver: Levantamento realizado pela Rede de Observatórios de Segurança. Novembro de 2019. Segundo o levantamento, 90,5% das pessoas presas por monitoramento facial no Brasil eram negras. A pesquisa considerou dados sobre prisões e abordagem com uso de reconhecimento facial desde março daquele ano em cinco estados do Brasil.

24 A organização brasileira Coding Rights realizou pesquisa divulgada no início de 2021 na qual chama atenção para riscos de discriminação de pessoas trans e não binárias por sistemas de reconhecimento facial utilizados pelo governo federal do Brasil.

25 Ver: A. Korte, Facial recognition technology cannot read emotions, scientists say, American Association for the Advancement of Science, 16 de fevereiro de 2020; ou S. Porter, Secrets and Lies: Involuntary Leakage in Deceptive Facial Expressions as a Function of Emotional Intensity, Journal of Nonverbal Behavior, 36(1), 23-37, Março de 2012.

26 Ver: A. M'charek, Tentacular Faces: Race and the Return of the Phenotype in Forensic Identification, American Anthropologist, 6 de maio de 2020.

27 Ver: R. Wevers, Unmasking biometrics' biases: Facing gender, race, class and ability in biometric data collection, Tijdschrift voor Mediageschiedenis, TMG Journal for Media History, 21(2), 89-105, 2018.

28 Ver: S. Fussel, An Algorithm That 'Predicts' Criminality Based on a Face Sparks a Furor, Wired, 24 de junho de 2020; K. Amjad & A.A. Malik, A Technique and Architectural Design for Criminal Detection based on Lombroso Theory Using Deep Learning,LGURJCSIT, 4(3), 2020.

29 Ver: Interpol, Biometrics for Frontline Policing; ou The Brussels Times, The Brussels Airport to be equipped with facial recognition cameras, 9 de julho de 2019.

30 Sob justificativas relacionadas à segurança, um sistema de reconhecimento facial em aeroportos do Brasil começou a ser testado no final de 2020, no âmbito do projeto "Embarque Seguro". Posteriormente, em junho de 2021, o projeto foi testado pela primeira vez simultaneamente em dois aeroportos, mais especificamente na ponte aérea entre Rio de Janeiro e São Paulo. Entretanto, vale destacar que, em anos anteriores, tecnologias de reconhecimento facial já haviam sido utilizadas em aeroportos brasileiros, também com finalidade de segurança.

31 Ver: o programa Aadhaar na Índia, o sistema nacional de carteiras de identidade da África do Sul, PYMNTs; ou Deep Dive: Digital ID Developments From Around The World, 27 de fevereiro de 2019.

No primeiro trimestre de 2021, foi noticiada a celebração de um acordo do Tribunal Superior Eleitoral (TSE) com o governo federal com a finalidade de que bases de dados de biometria fossem integradas para facilitar a implementação de um sistema de Identificação Civil Nacional (ICN) no Brasil. A ideia é que a gestão da ICN seja realizada pelo TSE no futuro e que esse novo sistema de identificação funcione como uma identidade digital.

32 Ver: Metropolitan Police e NPL, Metropolitan Police Service Live Facial Recognition Trials. Fevereiro de 2020. O projeto "O Panóptico" realiza o monitoramento da utilização de reconhecimento facial por forças de segurança pública e disponibiliza um mapa online indicando a implementação dessas tecnologias em diferentes lugares no Brasil.

33 Ver: V. Marda & S. Narayan, Data in New Delhi's predictive policing system, 2020; ou A. Daly, Algorithmic oppression with Chinese characteristics: AI against Xinjiang's Uyghurs, 2019.

34 O crescente uso da biometria pelos Estados para prestar serviços públicos, juntamente com os riscos desta abordagem, foram assinalados pelo Relator Especial da ONU para pobreza extrema e direitos humanos em seu Relatório de 2019 à Assembleia Geral, Relatório Especial da ONU sobre pobreza extrema, tecnologias digitais, proteção social e direitos humanos. Ver: A/74/493, Outubro de 2019.

35 Por exemplo, os sistemas eleitorais Thales em listas eleitorais. De acordo com o site da empresa, os países incluem a República Democrática do Congo, Gabão, Omã, Burkina Faso, Benin, Filipinas e Suécia. Desde 2008, o Tribunal Superior Eleitoral (TSE) vem conduzindo o cadastramento biométrico das impressões digitais dos eleitores brasileiros. O cadastramento é obrigatório e o TSE planeja cadastrar todo o eleitorado até 2022. Nas eleições locais de 2020, a verificação biométrica não foi realizada por conta de questões sanitárias.

36 Ver: Suprema Corte de Illinois, Rosenbach versus Six Flags Entertainment Corporation, 2019 IL 123186

37 Observações semelhantes são feitas pelo Relator Especial da ONU para extrema pobreza, já citado anteriormente.

38 Somente por meio de sua adoção em uma resolução da Assembleia Geral da ONU, a DUDH não tem caráter vinculante para os Estados. No entanto, considera-se que muitos de seus dispositivos tenham adquirido força normativa como direito internacional consuetudinário desde sua adoção em 1948. Ver: Filartiga v. Pena-Irala, 630 F. 2d 876.1980. 2º Tribunal de Recursos.

39 Assembleia Geral da ONU, Pacto Internacional dos Direitos Civis e Políticos, 16 de Dezembro de 1966, UN Treaty Series, vol. 999, p. 171.

40 Ver: Artigo 10 da Convenção Europeia de Direitos Humanos (Convenção Europeia), 4 de setembro de 1950; Artigo 9 da Carta Africana dos Direitos Humanos e dos Povos (Carta de Banjul), 27 de junho de 1981; Artigo 13 da Convenção Americana de Direitos Humanos (Convenção Americana), 22 de novembro de 1969; e Artigo 11 da Carta dos Direitos Fundamentais da União Europeia (Carta da UE).

41 A jurisprudência interamericana desenvolveu um teste tripartite, a partir do disposto no art. 19 do PIDCP e no art. 13 da Convenção Interamericana de Direitos Humanos "que é utilizado para determinar se as restrições a esse direito são aceitáveis sob os parâmetros da Convenção Americana. Esse padrão exige que as restrições sejam previstas de modo claro e preciso na lei, que sejam direcionadas à realização de objetivos imperiosos reconhecidos pela Convenção, e que sejam necessárias em uma sociedade democrática". Ver: C. B. Marino, Marco Jurídico Interamericano sobre o Direito à Liberdade de Expressão. Relatoria Especial para a Liberdade de Expressão, Comissão Interamericana de Direitos Humanos (2014), Acesso em 28 jun. 2021.

42 Ver: Comitê de Direitos Humanos da ONU, Belichkin v. Belarus, Com. No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

43 Ver: Comitê de Direitos Humanos da ONU, Comentário Geral n. 34, Artigo 19: Liberdade de Opinião e Expressão, CCPR/C/GC/34, para 18.

44 Ibid., para 19. A mesma linguagem é repetida em convenções de direitos humanos regionais, mais notavelmente o Artigo 13 da Convenção Americana, Artigo 9 da Carta Africana, Artigo 10 da Convenção Europeia e Artigo 23 da Declaração dos Direitos Humanos da ASEAN.

45 Ver: Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, 21 de dezembro de 1965, UN Treaty Series, vol. 660, p. 195.

46 Ver: Artigo 11 da Convenção Europeia, Artigo 12 da Carta da UE, Artigo 15 da Convenção Americana e Artigo 11 da Carta Africana.

47 Ver: Comitê de Direitos Humanos da ONU, Comentário Geral n. 37, Artigo 21: direito de reunião pacífica, CCPR/C/ GC/37, 27 de julho de 2020, para 36.

48 Ver: Artigo 11 da Convenção Americana; e Artigo 8 da Convenção Europeia.

49 Ver: Comitê de Direitos Humanos da ONU, Comentário Geral n. 16: Artigo 17 (Direito à privacidade), The Right to Respect of Privacy, Family, Home, and Correspondence, and Protection of Honour and Reputation, 8 de abril 1988, para 3; International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles), Princípio 1.

50 Ver: Convenção Europeia, op. cit., Artigo 14; Carta da UE, op. cit., Artigo 21; Carta Africana, op. cit., Artigos 2 e 3; Convenção Americana, op. cit., Artigo 24.

51 Ver: PIDCP, Artigo 26.

52 Ver: ARTIGO 19, The Global Principles on Protection of Freedom of Expression and Privacy, 2017.

53 Ver: Comentário Geral nº 16, op.cit., para 10.

54 Ver: Guidelines for the Regulation of Computerized Personal Data Files, GA Res. 45/95, 14 de dezembro de 1990.

55 As legislações ao redor do mundo que regulam o tratamento de dados pessoais atualmente são em sua maioria baseadas nos Fair Information Practices (FIP). Estes princípios foram elaborados nos anos 1970 pelo U.S. Department of Health, Education and Welfare (HEW) para que dados pessoais fossem tratados de maneira justa, respeitando a privacidade e a segurança dos dados (U.S. Department of Health, Education and Welfare - HEW). Ver: Records, Computers and the Rights of Citizens: report of the secretary's advisory committee on automated personal data systems. Washington, 1973.

56 Ver: Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, ETS No.108.

57 Segundo o artigo 1º da Carta da UE, a dignidade humana é o fundamento de todos os direitos fundamentais nela garantidos. Portanto, os dados biométricos devem ser coletados e processados de forma a proteger adequadamente a dignidade humana. Ver: CJEU, C-377/98, Holanda v. Parlamento Europeu e do Conselho, 9 de outubro de 2001, paras. 70-77.

Adicionalmente, de acordo com o Artigo 52 (1) da Carta da UE, qualquer limitação aos direitos fundamentais deve: (i) estar prevista em lei. Esta condição requer uma base jurídica adequada que atenda à exigência qualitativa: a regra deve ser pública, precisa e previsível; (ii) atender verdadeiramente a objetivos de interesse geral reconhecidos pela União ou à necessidade de proteger os direitos e liberdades de terceiros; (iii) respeitar a essência do direito; (iv) ser necessária e proporcional. A Autoridade Europeia para a Proteção de Dados (AEPD) fornece orientações rigorosas sobre como demonstrar a necessidade e a proporcionalidade. A Agência dos Direitos Fundamentais (FRA, na sigla em inglês) considera que o uso do reconhecimento facial pode violar a dignidade humana, fazendo com que as pessoas evitem locais ou eventos importantes através de formas excessivamente enérgicas/ coercivas de coleta de dados e através de "comportamento policial inadequado". Ver: França, Facial recognition technology: fundamental rights considerations in the context of law enforcement, Viena, 2020, p. 20.

58 Ver: African Union Convention on Cyber Security and Personal Data Protection, 2014. A ARTIGO 19 observa que, segundo seu ponto de vista, as sanções penais e os regulamentos baseados no conteúdo

presente na Convenção estão em desacordo com os padrões de restrições admissíveis à liberdade de expressão segundo outros instrumentos vinculantes de direitos humanos.

59 Ver: OEA, Principles for Privacy and Personal Data Protection in the Americas, 2015. Atualmente, encontra-se em revisão. As revisões incluem referências específicas a dados biométricos, como, por exemplo, em documentos de 2015 e 2020.

60 Ver: Comitê de Direitos Humanos da ONU, Comentário Geral n. 16, (Artigo 17 PIDCP). 8 de abril de 1988, para 10, no qual o Comitê observou que o direito é necessário para garantir o respeito do direito à privacidade.

61 Ibid.

62 Ver: Corte Europeia, Gaskin v. the United Kingdom, 7 de julho de 1989, Series A no. 160, para 49; M.G. v. the United Kingdom, App. No. 39393/98. 24 de setembro de 2002, para 27; Odièvre v. France [GC], App. No. 42326/98, ECHR 2003III), para 41-47; Guerra e Others v. Italy, App. No. 14967/89, 19 fevereiro de 1998.

63 Ver: GDPR, op.cit.

64 Ver: FRA, Opinions Biometrics, 2019.

65 Ver: a Lei de Privacidade de Informações Biométricas do estado de Illinois, que reconheceu que "uma maioria esmagadora da população está cansada do uso da biometria quando tais informações estão vinculadas a finanças e outras informações pessoais"; Illinois Compiled Statutes 740 ILCS 14/1 Biometric Information Privacy Act, Sec 5 (d).

66 Ver: Relatório sobre criptografia, anonimato e a estrutura dos direitos humanos da Relatoria Especial para a liberdade de expressão, A/HRC/29/32, 22 de maio de 2015.

67 CDH, Resolução sobre o Direito à Privacidade na Era Digital, UN Doc. A/HRC/RES/34/7, 23 de março de 2017, tradução nossa.

68 Ver: Conselho da Europa, Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data, 28 de janeiro de 1981, ETS 108.

69 Ver: Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção de pessoas naturais a respeito do processamento de dados pessoais e da livre circulação de tais dados, e revogação da Diretiva 95/46/EC (GDPR), Artigo 9.

70 Ver: Rede Ibero-americana de Proteção de Dados (RIPD), Padrões de Proteção de Dados Pessoais para os Estados Ibero-Americanos, Artigos 2.1(d) e 29.4.

71 Ver: Convenção da União Africana sobre Segurança Cibernética e Proteção de Dados Pessoais, cit. Artigo 10.4(d).

72 Ver: Alto Comissariado das Nações Unidas para os Direitos Humanos, The right to privacy in the digital age, A/HRC/39/29, 3 de agosto de 2018, para 14.

73 Ibid., parágrafo 61(c).

74 Ver: Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/HRC/41/41, 17 de maio de 2019, para 57.

75 Ver: Biometric Update, Biometric Update, UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition, 3 de julho de 2018.

76 Ver: ACNUDH, UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. 25 de junho de 2019.

77 Ver: Corte Europeia S. and Marper v. the UK [GC], App. Nos. 30562/04 and 30566/04, 4 de dezembro de 2008, paras 112 e 125.

78 Ver: Conselho de Segurança da ONU, Resolução 2396 (2017).

79 Ver: 2018 Addendum to the 2015 Madrid Guiding Principles, Anexo à carta datada de 28 de dezembro de 2018 do Presidente do Comitê do Conselho de Segurança estabelecido de acordo com a resolução 1373 (2001), relativa ao antiterrorismo, dirigida ao Presidente do Conselho de Segurança.

80 Ver: UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism, Ccompilado por CTED e UNOC (siglas em inglês), 18 de junho de 2018.

81 Ver: Guiding Principles on Business and Human Rights: Implementing the UN "Protect, Respect and Remedy" Framework, 2011. A publicação contém os Princípios Orientadores da ONU sobre Empresas e Direitos Humanos: Implementando os parâmetros "Proteger, Respeitar e Remediar", que foram desenvolvidos pelo Representante Especial da Secretaria-Geral sobre a questão de direitos humanos e corporações transnacionais e outras empresas comerciais. O Representante Especial anexou os Princípios Orientadores ao seu relatório final ao Conselho de Direitos Humanos (A/HRC/17/31), que também inclui uma apresentação sobre os Princípios Orientadores e um resumo do processo que levou ao seu desenvolvimento. O Conselho de Direitos Humanos da ONU endossou os princípios na Resolução 17/4 (A/HRC/RES/17/14), de 16 de junho de 2011.

82 Ibid.

83 Ibid., princípio 15.

84 Algumas empresas foram ainda mais longe e começaram a investir em assessores legislativos próprios para promulgá-los; Ver: Vox, Jeff Bezos says Amazon is writing its own facial recognition laws to pitch to lawmakers. 26 de setembro de 2019.

85 Ver: Relatoria Especial sobre Liberdade de Expressão, Report to the Human Rights Council on Freedom of expression, states and the private sector in the digital age, 2013, A/HRC/32/38, 11 de maio de 2016.

86 Ver: Google, Artificial Intelligence at Google: Our Principles.

87 Um banco de dados de impressões digitais de pedidos de asilo em toda a UE, o EURODAC, destina-se a armazenar impressões digitais de todas as pessoas que cruzam uma fronteira europeia. Entretanto, houve preocupações quando foi anunciado que as informações do banco de dados seriam disponibilizadas às autoridades e à Europol em suas investigações sobre terrorismo. A reformulação do banco de dados para fins de terrorismo, e não para fins de imigração, estigmatiza e estereotipa ainda mais uma população já vulnerável: os requerentes de asilo, que já estão fugindo de perseguições, estão sendo imediatamente associados a atos terroristas. Ver: Statewatch e PICUM, Data protection, Immigration Enforcement and fundamental Rights: What's the EU's Regulations on Interoperability Mean for People with Irregular Status.

88 Ver: S. and Marper v. the UK, op.cit., para 103.

89 O exemplo de coleta de metadados em massa na UE mostra como os Estados coletam informações para uma determinada finalidade (por exemplo, encontrar terroristas), mas com o tempo aumenta o escopo para incluir crimes não violentos, tais como arrombamentos para realização de furtos.

90 Deve-se destacar que a utilização de reconhecimento facial para fins de segurança pública no Brasil depende de regulamentação de lei específica, a partir do determinado no art. 4º, III, da LGPD. Nesse caso, o consentimento a partir da LGPD não seria a base legal utilizada.

91 Ver: CNIL, Reconhecimento facial: para o debate das questões em jogo, 15 de novembro de 2019, p. 6.

92 Ver: Ada Lovelace Institute and DataKind UK, Examining the Black Box: Tools for Assessing Algorithmic Systems, 29 de abril de 2020.

93 Por exemplo, a empresa britânica Sthaler desenvolveu um sistema biométrico para autenticação de clientes e segurança para ser usado em festivais de música. O sistema também está sendo implementado para outros fins. Ver: From Sthaler to FinGo, S/D.

94 Ver: O Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal, Novembro de 2019.

95 Ver: German Data Ethics Commission, Parecer, Outubro de 2019.

96 Ver: Tribunal Administrativo de Marselha, 27 de fevereiro de 2020, req. n. 1901249.

97 Quando acompanhada de salvaguardas legais e processuais apropriadas, a interceptação direcionada das comunicações de uma pessoa é um ato legítimo de um governo democrático, que pode ser necessário para prevenir o crime e a desordem e proteger a segurança nacional. A vigilância direcionada só pode ser justificada quando prescrita por lei, for necessária para atingir um objetivo legítimo e proporcional ao objetivo perseguido. Ver: Tribunal Europeu, Klass e outros vs. Alemanha, App. No. 5029/71, 6 de setembro de 1978.

A Corte Europeia usou o conceito de "expectativa razoável de privacidade" – uma medida em que as pessoas podem esperar privacidade em espaços públicos sem serem submetidas a vigilância – como um dos fatores para decidir se há violação do direito ao respeito à vida privada nos termos da Convenção Europeia. Ver: Corte Europeia, Copland vs. Reino Unido, App. Nos. 62617/00, 3 de julho de 2007, para 42.

De forma semelhante, o Conselho Europeu de Proteção de Dados, em suas diretrizes sobre o processamento de dados pessoais através de dispositivos de vídeo, afirma que os indivíduos "podem também esperar estar livres de monitoramento dentro de áreas de acesso público, especialmente se essas áreas são tipicamente utilizadas para recuperação, regeneração e atividades de lazer, bem como em lugares onde os indivíduos ficam e/ou se comunicam, tais como áreas de repouso, mesas em restaurantes, parques, cinemas e instalações fitness". Aqui, os interesses ou direitos e liberdades da pessoa em questão muitas vezes prevalecerão sobre os interesses legítimos do/a controlador/a. Ver: EDPB, Guidelines 3/2019 on processing personal data through video devices, Versão 2.0, 29 de janeiro de 2020.

98 Ver: P. Fussey & D. Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology, University of Essex, Human Rights Centre, Julho de 2019, p. 36 e fn. 87. Ver: Rede de Justiça Internacional e Segurança Pública, Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, 30 de junho de 2011. O Documento p. 016632 afirma que "o uso do reconhecimento facial para fins de vigilância tem o potencial de fazer com que as pessoas se sintam extremamente desconfortáveis, que alterem seu comportamento e pode levar à autocensura e inibição". Ver: Relatório do Alto Comissariado das Nações Unidas para os Direitos Humanos, Impacto das novas tecnologias na promoção e proteção dos direitos humanos no contexto de reuniões, incluindo protestos pacíficos, A/ HRC/44/24, p. 34.

99 Ver: Corte Europeia, Szabó e Vissy v Hungary, App nos. 37138/14, 12 de janeiro de 2016, para 38. Ver: Human Rights Watch & Pen International, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy. Julho de 2014; e CNIL, 2019 report, op.cit. (a CNIL observou que a vigilância constante e o reconhecimento facial em espaços públicos podem fazer com que atitudes e comportamentos aparentemente normais pareçam suspeitos, tais como usar óculos escuros, ter o capuz levantado, ou olhar para o chão ou um telefone).

Relevante destacar que a preocupação quanto ao desencorajamento de ações da sociedade civil se torna ainda mais grave quando se leva em consideração que, desde o início do governo Bolsonaro, a participação da sociedade civil nos debates públicos vem sendo ameaçada. Esse contexto compreende inclusive ações de repressão direta a membros de determinadas organizações, como foi o caso de medidas de criminalização contra a ONG Projeto Saúde e Alegria, bem como às prisões de quatro integrantes da Brigada de Incêndios de Alter do Chão.

100 Ver: FRA 2020 report, op.cit., p. 20; ou London Policing Ethics Panel, Final Report on Live Facial Recognition, Maio de 2019.

101 Ver: Special Rapporteur on FoE, Vigilância e Direitos Humanos, A/HRC/41/35, 28 de maio de 2019

102 Ver: Indian Express – a Polícia de Délhi filma protestos, passa as imagens através de um software de reconhecimento facial para escanear a multidão, 28 de dezembro de 2019; India Today – Amit Shah sobre as provas dos protestos de Delhi: 1100 pessoas identificadas usando tecnologia de reconhecimento facial, 300 vieram da UP, 11 de março de 2020.

103 Apesar de não ter sido elaborada a partir de tecnologias biométricas, vale a pena citar a lista criada pelo Governo Federal brasileiro no final de 2020. Neste relatório, pessoas comunicadoras, jornalistas, influenciadores/as e defensoras de direitos humanos são categorizadas a partir de sua orientação política e tratadas como detratoras. Tecnologias biométricas facilitariam a categorização e fomentariam a perseguição destas pessoas. (cf. CRUZ, Isabela. A lista de 'detratores'. E o histórico de monitoramento do governo, Nexo, [s.l.], 2 dez. 2020.

104 Ver: Vigilância e Direitos Humanos, op.cit., p. 15.

105 Ver: o Comitê de Normas da Vida Pública, Artificial Intelligence and Public Standards, Seção 4.7: Avaliação de Impacto, fevereiro de 2020.

O Comitê observou que a responsabilização adequada depende dos órgãos públicos estarem cientes dos riscos de seus sistemas de IA, para que as autoridades possam ser avaliadas em relação a quaisquer medidas de mitigação que tomem.

106 Em dezembro de 2020, o Tribunal de Recursos da Nona Circunscrição dos EUA acolheu os argumentos do requerente de que o acesso a pedidos de informação que buscam acesso a dados agregados é essencial para equilibrar o interesse do público em compreender como o governo usa dados biométricos e outros dados pessoais que coleta sem revelar os dados subjacentes que são frequentemente privados ou de outra forma intrusivos. Ver: US Court of Appeals for the Ninth Circuit, The Center for Investigative Reporting v. United States Department of Justice, No.18-17356D.C. No. 3:17-cv-06557-JSC, 3 de dezembro de 2020. Ver: EPIC v. FBI- Next Generation Identification; and US Government Accountability Office, Face Recognition Technology Report and Recommendations, Maio de 2016.

107 PPor exemplo, no Reino Unido, o Escritório do Comissário para Retenção e Uso de Material Biométrico, cujo papel é fornecer supervisão independente do regime estabelecido pela Lei de Proteção de Liberdades de 2012 e governar a retenção e o uso de amostras de DNA, perfis e impressões digitais pela polícia na Inglaterra e no País de Gales, não está coberto pela Lei de Liberdade de Informação. O Reino Unido, portanto, não tem obrigação legal de responder a pedidos de acesso a informações. Para mais informações sobre o mandato e o poder do Comissariado, veja a página do *Office of Biometrics Commissioner* no site do governo britânico.

No Brasil, um grupo de entidades – incluindo a ARTIGO 19 – acionou o Judiciário em 2020 com a finalidade de obter informações a respeito de um projeto que, entre outras medidas, visava à implementação de câmeras de reconhecimento facial no metrô de São Paulo – no caso, informações obtidas previamente por vias extrajudiciais haviam sido insuficientes. Ver: T. Dias, As perguntas que o metrô de São Paulo não respondeu antes de vender seu rosto por R$ 58 milhões, 11 de fevereiro de 2020. No Paraguai, entidades ajuizaram uma ação judicial em 2019 para questionar negativas de acesso a informações relacionadas a câmeras de vigilância equipadas com tecnologia biométrica que estavam sendo implementadas pelo Ministério do Interior e pela Polícia Nacional do país. Ver: TEDIC, ¿Quién vigila al vigilante?, 16 de setembro de 2019. Os dois casos se relacionam com a cobrança de informações, feita pela sociedade civil e por outras instituições, a respeito desse tipo de projeto para analisá-lo à luz dos direitos humanos.

108 O acesso aos pedidos de informação tem permitido aos indivíduos obter informações cruciais da tecnologia de reconhecimento facial, tais como taxa de erro, acordos de licença entre órgãos públicos e empresas privadas ou divulgação de dados biométricos entre agências para um amplo conjunto de finalidades; veja, por exemplo, a experiência da EPIC nos EUA em desafiar o uso de tecnologias biométricas por várias agências públicas: EPIC FOIA: DHS Biometric Program. O acesso aos pedidos de informação também revelou a falha dos órgãos públicos em conduzir uma auditoria de privacidade sobre o uso do reconhecimento facial ou testar adequadamente a precisão da tecnologia. Ver: U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI should better ensure privacy and accuracy, 2016.

109 Ver: UK Biometrics and Forensics Ethics Group Principles, dezembro de 2020.

110 De fato, sistemas de verificação 1:1 também trazem desafios. Ver: A. Kak, The State of Play and Open Questions for the Future, Regulating Biometrics: Global Approaches and Urgent Questions, setembro de 2020.

111 Ver: FRA, relatório 2020, op.cit.

112 Ver: The Guardian, Met police deploy live facial recognition technology, 11 de fevereiro de 2020; EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 de dezembro de 2019; Human Rights Watch, Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights, 15 de novembro de 2019; or The Times of India, From protest to chai, facial recognition is creeping up on us, 5 de janeiro de 2020; The Ken, Watch this space: New Bill could unleash facial recognition free for all, 11 de fevereiro de 2020.

113 Por exemplo, no Brasil, os sistemas de reconhecimento facial têm sido aplicados desde pelo menos 2011, e seu uso para fins de segurança foi amplamente expandido em 2019, principalmente durante o Carnaval, através de parcerias com agentes privados. Hoje, mais de 40 cidades do País adotaram a tecnologia. Ver: Le Monde Diplomatique Brasil, Reconhecimento facial: a banalização de uma tecnologia controversa, 22 de abril de 2020. Ver: Instituto Igarapé, Infográfico: Reconhecimento facial no Brasil, 2021.

114 Ver: The Guardian, Facial recognition… coming to a supermarket near you, 4 de agosto de 2019. Big Brother Watch, Co-op Facial Recognition Supermarkets Revealed, 14 de janeiro de 2021.

115 Ver: Instituto Brasileiro de Defesa do Consumidor (Idec) Idec quer saber como Hering usa dados de reconhecimento facial de clientes, 6 de março de 2019.

116 Ver: Idec, Idec pede esclarecimento sobre coleta de dado facial em loja do Carrefour, 23 de abril de 2019

117 Ver: Idec, ViaQuatro é condenada por reconhecimento facial no Metrô de SP: Empresa vai pagar R$100 mil por captar gênero, idade e emoções de passageiros quando olhavam anúncio publicitário, 11 de maio de 2021.

118 Ver: The Telegraph, Uber faces racism claim over facial recognition software, 23 de abril de 2019.

119 No âmbito do transporte público, deve-se citar as diversas situações no Brasil em que o reconhecimento facial é utilizado (Cf. Riocard, Biometria Facial – Bilhete Único Intermunicipal).

120 Por exemplo, a Huawei colocou o reconhecimento facial no centro de seu projeto "Cidades Seguras", que a empresa está tentando desenvolver em várias cidades em todo o mundo, com foco especial nas regiões africanas e asiáticas. Ver: CSIS, Watching Huawei's "Safe Cities", 4 de novembro de 2019.

121 Por exemplo, em 2019, São Francisco proibiu o uso do reconhecimento facial pelos órgãos cujo papel é fazer cumprir a lei. Ver: EFF, Stop Secret Surveillance Ordinance, 05 de junho de 2019. Para a ordem de banimento, Ver: The Guardian, San Francisco was right to ban facial recognition. Surveillance is a real danger, 30 de maio de 2019.

Portland atualmente está discutindo um banimento que abarca agentes públicos e privados. Ver: Fast Company, Portland plans to propose the strictest facial recognition ban in the country, 12 de fevereiro de 2019.

No Reino Unido, a Polícia da Escócia revelou que eles não mais usariam tecnologias de reconhecimento facial já que não estavam "aptas para uso" por conta de, entre outros fatores, preocupações com privacidade e direitos humanos. Os planos para implementação, inicialmente para 2026, foram pausados para que possa haver uma consulta sobre o impacto do software. Ver: BBC, Facial recognition: 'No justification' for Police Scotland to use technology, 11 de fevereiro de 2020.

122 Por exemplo, a IBM, em uma carta ao Congresso dos EUA sobre a Reforma para Justiça Racial, anunciou que iria parar a venda de software de reconhecimento facial "para uso geral". Ver: IBM CEO's Letter to Congress on Racial Justice Reform, 8 de junho de 2020.

A Amazon anunciou uma moratória de um ano no uso policial de sua tecnologia Rekognition. Ver: Amazon, We are implementing a one-year moratorium on police use of Rekognition, 10 de junho de 2020.

A Microsoft comprometeu-se a não vender suas tecnologias de reconhecimento facial a agências de cumprimento das leis. Ver: The Washington Post, Microsoft won't sell police its facial recognition technology, following similar moves from Amazon and IBM, 11 de junho de 2020.

123 Ver: http://reconocimientofacial.info

124 No Brasil, deve-se destacar o trabalho realizado pelo InternetLab e pelo Idec em relatório acerca da utilização do reconhecimento facial pelo setor privado. Ver: Reconhecimento Facial e o Setor Privado, 2020.

125 Ver: New York Times, The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?, 28 de março de 2019.

126 Em Moscou, por exemplo, o governo está usando a tecnologia de reconhecimento facial para garantir que as pessoas obrigadas a permanecer em casa ou em hotéis por conta da quarentena do coronavírus o façam. Ver: Reuters, Moscow deploys facial recognition technology for coronavirus quarantine, 21 de fevereiro de 2020.

Empresas chinesas estão implementando a tecnologia de reconhecimento facial que pode detectar temperaturas elevadas em uma multidão ou sinalizar cidadãos e cidadãs que não usam máscara. Ver: The Guardian, 'The New Normal': China's excessive coronavirus public monitoring could be here to stay, 9 de março de 2020.

O Reino Unido está considerando o reconhecimento facial como fundamental para o estabelecimento de um sistema de passaporte de imunidade.

127 Ver: National Geographic, Reconhecimento facial com máscara já é uma realidade – gostemos ou não, 17 de setembro de 2020.

128 Ver: Facewatch, Facewatch launches facemask recognition upgrade, 11 de maio de 2020.

129 Preocupantemente, a Comissão Europeia parece apoiar esta abordagem, e recentemente concedeu seu "selo de excelência" à tecnologia Aware, desenvolvida pela empresa espanhola Herta Security, que fornece análise avançada de vídeo, incluindo reconhecimento facial em tempo real e análise de comportamento de multidões, para ser usada na luta do bloco contra outro surto potencial do coronavírus. Ver: Euractiv, Crowd monitoring facial recognition tech awarded seal of excellence, 19 de junho de 2020.

130 No início de 2019, o Ministro do Interior da Sérvia e o Diretor de Polícia anunciaram a colocação de 1000 câmeras em 800 locais em Belgrado. O público foi informado que essas câmeras de videomonitoramento terão software de reconhecimento facial e de placas de carro. Três organizações da sociedade civil do país publicaram uma análise detalhada do DPIA do Ministério do Interior sobre o uso de vigilância por vídeo inteligente, concluindo que não atendia às condições formais ou materiais exigidas pela Lei de Proteção de Dados Pessoais na Sérvia. O órgão sérvio de proteção de dados confirmou as conclusões. Ver: EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 de dezembro de 2019.

131 Em fevereiro de 2020, o Facebook estabeleceu um acordo em uma ação coletiva em Illinois onde os usuários e usuárias alegaram que o sistema de *taggeamento* de fotos do site da empresa utilizava tecnologia de reconhecimento facial para analisar suas fotos e criar e armazenar 'modelos faciais' sem informá-los/as nem pedir seu consentimento em junho de 2011. Ver: New York Times, Facebook to Pay $550 Million to Settle Face Recognition Suit, 29 de janeiro de 2020.

Da mesma forma, o app para reconhecimento facial Clearview AI foi desenvolvido e amplamente comercializado para as agências de cumprimento da lei com base em um banco de dados de 3 bilhões de imagens ilegalmente tiradas do Facebook, do Google e do YouTube. A empresa enfrenta atualmente uma ação judicial movida em nome de vários cidadãos de Illinois por violação da Lei de Informações Biométricas do estado. Em março de 2020, o Procurador-geral de Vermont entrou com uma ação judicial contra a empresa definindo suas práticas comerciais como "inescrupulosas, antiéticas e contrárias às políticas públicas". Ver: Gizmodo, We Found Clearview AI's Shady Face Recognition App, 27 de fevereiro 2020; ou Vermont Attorney General Office,

Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law, 10 de março de 2020.

132 Ver: OneZero, Why you can't really consent to Facebook's Facial Recognition, 30 de setembro de 2019; E. Selinger & W. Hartzog, The Inconsentability of Face Surveillance, 66 Loyola Law Review 101 (2019).

133 Diversos estudos demonstram diferenças na taxa de acurácia de reconhecimento facial das pessoas a depender de características raciais, de gênero e de idade. Ver: B. F. Klar; M. J. Burge; J. C. Klontz; R. W. V. Bruegge; A. K. Jain, Face Recognition Performance: role of demographic information. IEEE Transactions On Information Forensics And Security, [s.l.], v. 7, n. 6, p. 1789-1801, dezembro de 2012.

134 Ver: National Institute of Standards and Technology, NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, 19 de dezembro de 2019; D. Leslie, Understanding bias in facial recognition technologies, The Alan Turing Institute, 2020; A. Najibi, Racial Discrimination in Face Recognition, 24 de outubro de 2020.

135 A organização Coding Rights, citada anteriormente, também lançou um documentário no qual discorre sobre as correlações entre o uso de reconhecimento facial e de gênero, raça e território. Ver: Coding Rights, Reconhecimento Facial: raça, gênero e território - From Devices To Bodies, 2021. Cabe destacar, ainda, uma linha do tempo elaborada por Tarcízio Silva acerca da temática de racismo algorítmico. Ver: T. Silva. Linha do Tempo do Racismo Algorítmico: casos, dados e reações, 2020.

136 Ver: J. Buolamwini & T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018. Além disso, o National Institute for Standards and Technology (NIST) realizou recentemente um estudo para avaliar a precisão com que os softwares de reconhecimento facial identificam pessoas de sexo, idade e origem racial variados. De acordo com suas descobertas, a resposta depende do algoritmo no coração do sistema, de sua aplicação e dos dados com os quais é alimentado. Entretanto, um estudo do NIST descobriu que a maioria dos algoritmos de reconhecimento de rostos exibe diferenciais demográficos. Um diferencial significa que a capacidade de um algoritmo de combinar duas imagens da mesma pessoa varia de um grupo demográfico para outro. As mulheres afro-americanas são o grupo demográfico com maior número de falsos positivos; no geral, os grupos asiáticos, afro-americanos e indígenas são os grupos mais sujeitos a resultados imprecisos. Ver: NIST, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 8280.

137 Ver: ACLU, Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, 26 de julho de 2018. (Que documentou que o sistema de reconhecimento facial desenvolvido pela Amazon reconheceu erroneamente 28 membros do Congresso dos EUA, dos 535 testados, como tendo cometido crimes. Entre eles, havia um número desproporcionalmente alto de negros). Ver: University of Essex, Human Rights Centre, Independent Report on the London Metropolitan Police Service's Trial of Live Recognition Technology, Julho 2019. (Que descobriu que aproximadamente 80% dos reconhecimentos do aplicativo estavam errados em seis testes em tempo real da Polícia Metropolitana do Reino Unido nas áreas de Londres do Soho, Romford e Stratford). Ver: Stark, Face Recognition is the Plutonium of AI, 17 de abril de 2019. (Que alertou que o viés racial é uma característica das tecnologias de reconhecimento facial, e não uma falha).

138 Ibid. ACLU. Além disso, há pelo menos três casos relatados de homens negros nos Estados Unidos que foram presos injustamente devido a um reconhecimento facial falho. Ver: NBCNews, Man wrongfully arrested due to facial recognition software talks about 'humiliating' experience, 26 de junho de 2020; The New York Times, Another

Arrest, and Jail Time, Due to a Bad Facial Recognition Match, 29 de dezembro de 2020; The New York Times, Wrongfully Accused by an Algorithm, 24 de junho de 2020.

139 O reconhecimento pessoal ocorre, de acordo com o artigo 226, do Código de Processo Penal brasileiro, quando pessoas são colocadas lado a lado para que a vítima possa reconhecer o suposto autor de um crime.

140 Ver: Interpol, Facial Recognition, S/D.

141 Ver: UK Information Commissioner's Office, ICO investigation into how the police use facial recognition technology in public places, 31 de outubro de 2019.

142 Ver: ARTIGO 19, Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence, Abril de 2019; ARTIGO 19 e Privacy International, Privacy and freedom of expression in the age of artificial intelligence, Abril de 2018.

143 Em 2019, a CNIL, o órgão francês de proteção de dados, condenou o uso de tecnologia de reconhecimento facial com o objetivo de controlar o acesso das crianças à escola, com o argumento de que o mesmo objetivo pode ser alcançado por meios menos invasivos dos direitos fundamentais das crianças. Ver CNIL, op.cit. Várias ONGs também denunciaram a implementação desta tecnologia de reconhecimento facial nas escolas. Ver: La Quadrature du Net, the League of Human Rights, CGT Educ'Action des Alpes-Maritimes and the Federation of Parents' Councils of Public Schools in the Alpes-Maritimes, Facial Recognition in High Schools: A recourse to block biometric surveillance, 19 de fevereiro de 2019.

Ver: Corte Administrativa de Marselha, julgamento de 27 de fevereiro de 2020.

A propósito, o juiz francês, envolvido em um caso relevante em Marselha, declarou durante a audiência que "a Região está usando um martelo para acertar uma formiga", o que explicita perfeitamente a falta de proporcionalidade entre a medida implementada (sistema de reconhecimento facial) e o objetivo a ser alcançado (controlar o acesso dos estudantes). De maneira semelhante, estudantes de várias escolas de várias cidades dos EUA protestaram contra o uso do reconhecimento facial e, em alguns casos, isso levou a administração da escola a abandonar o plano de implementação da tecnologia. Ver: The Guardian, 'Ban this technology': students protest US universities' use of facial recognition, 3 de março de 2020.

144 A sociedade civil em todo o mundo começou a levantar sua voz sobre o impacto da vigilância de reconhecimento facial no anonimato e sobre seu efeito inibidor na liberdade de expressão. Por exemplo, na Austrália, o diretor adjunto do Conselho das Liberdades Civis de New South Wales, no contexto do inquérito parlamentar sobre a implementação de sistemas de correspondência de imagens faciais, disse que "isto traz consigo uma ameaça real ao anonimato. Mas a dimensão mais preocupante é o efeito inibidor na liberdade de discussão política, no direito de protesto e no direito de dissidência. Pensamos que estas implicações potenciais devem ser motivo de preocupação para todos nós". Ver: The Guardian, Facial image matching system risks 'chilling effect' on freedoms, rights groups say', 7 de novembro de 2018.

145 Ver: E. Denham, Information Commissioner, Blog: Live facial recognition technology – police forces need to slow down and justify its use, S/D.

146 Para dar um exemplo, o Ministério do Interior na Índia, em fevereiro de 2020, prendeu 1100 pessoas que participaram de protestos pacíficos, identificando-as com o uso do reconhecimento facial. Ver: India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP, op. cit.

147 A liberdade religiosa é garantida pelo Artigo 18 da DUDH e garantida pelas disposições do Artigo 18 da ICCPR, assim como por outros instrumentos regionais e nacionais.

148 Ibid.

149 Ver o programa SPOT da US Transportation Security Authority ou iBorderCtrl da Europa (um sistema de IA cujas câmeras escaneavam os rostos dos viajantes em busca de sinais de engano enquanto eles respondiam às perguntas dos agentes de segurança de fronteira, testados na Hungria, Letônia e Grécia). As críticas ao conjunto de dados dos programas, os falsos positivos e o potencial discriminatório levaram à sua retração.

Ver: Government Accountability Office, Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities, 14 de novembro de 2013; Department of Homeland Security Office of Inspector General, TSA's Screening of Passengers by Observation Techniques, Maio de 2013; ACLU vs. TSA, 8 de fevereiro de 2017; Ars Technica, TSA's got 94 signs to ID terrorists, but they're unproven by science, 13 de novembro de 2013; The Intercept, Exclusive: TSA's Secret Behavior Checklist to Spot Terrorists, 27 de março de 2015; Ars Technica, The premature quest for AI-powered facial recognition to simplify screening, 2 de junho de 2017; J. Sánchez-Monederoa & L. Dencik, The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl, The Intercept, We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive, 26 de julho de 2019.

150 Exemplificando: o sistema de reconhecimento de emoções chinês Alpha Hawkeye é usado pelas autoridades da Estação Ferroviária Yiwu para prender "criminosos"; a empresa estatal Chang'an Automobiles comercializa carros com detectores de emoções e de fadiga; a Hikvision está colaborando com o Hangzhou Educational Technology Centre (que é responsável pelas aquisições edtech para escolas primárias e secundárias da cidade), supervisionado pelo Hangzhou Education Bureau.

151 Ver: P. Ekman, E. Richard Sorenson & W. V. Friesen, Pan-Cultural Elements in Facial Displays of Emotion, Science, 164(3875), 86-88, 1969; P. Ekman, Universal Facial Expressions of Emotions, California Mental Health Research Digest, 8(4), 151-158, 1973; P. Ekman, Universals and Cultural Differences in Facial Expressions of Emotions In Cole, J. (Ed.), Nebraska Symposium on Motivation, Lincoln, University of Nebraska Press, 207-282, 1973.

152 Ver: A. L. Hoffman & L. Stark, Hard Feelings – Inside Out, Silicon Valley, and Why Technologizing Emotion and Memory Is a Dangerous Idea, Los Angeles Review of Books, 11 de setembro de 2015.

153 APA e Vancouver. Ver: J. A. Russel, Is there universal recognition of emotion from facial expression? A review of the cross-cultural studies, Psychological Bulletin, 115(1), 102-141, 1994; L. Feldman Barrett et al, Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements, Psychological Science in the Public Interest, Vol. 20(1), 2019; Oxford Scholarship Online, Coherence between Emotions and Facial Expressions, The Science of Facial Expression, 2017; The New York Times, What Faces Can't Tell Us, 28 de fevereiro de 2014.

154 Ver: A. Daub, The Return of the Face, Longreads, Outubro de 2018.

155 Ver: L. Safra, C. Chevallier, J. Grezes & N. Baumard, Tracking historical changes in trustworthiness using machine learning analyses of facial cues in paintings, Nature Communications, 11, 4728, 2020; ou Coalition for Critical Technology, Abolish the #TechToPrisonTimeline, Medium, 23 de junho de 2020.

156 APA. Ver: C. Cun, C. Zhengdong & S. Beibei, Grasp the Truth in an Instant: Application of Micro-expressions Psychology in Customs Inspection of Passengers, Journal of Customs and Trade, 3, 31-33, 2018.

157 Ver: Comentário Geral nº 34, op.cit., que afirma que "qualquer forma de esforço para coagir a posse ou não de qualquer opinião é proibida. A liberdade de expressar a própria opinião inclui necessariamente a liberdade de não expressar a própria opinião", parágrafo 10.

158 Ver: Relatório do Alto Comissariado da ONU para os Direitos Humanos, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, 24 de junho de 2020, para 40.

159 Ver: Princípios Orientadores da ONU sobre Empresas e Direitos Humanos, op.cit., p. 15.

www.artigo19.org