7 de junho de 2021

Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada.

Nós, abaixo assinados, pedimos pelo banimento total do uso de reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto que permitam a vigilância em massa e a vigilância discriminatória direcionada. Essas ferramentas são capazes de identificar, seguir, destacar individualmente e rastrear pessoas em todos os lugares que elas vão, minando nossos direitos humanos - incluindo os direitos à privacidade e à proteção de dados, o direito à liberdade de expressão, o direito à liberdade de reunião e associação (levando à criminalização de protestos e causando um efeito inibitório), e os direitos à igualdade e à não-discriminação.

Nós temos visto essas tecnologias serem usadas de modo a possibilitar uma série de abusos e violações a direitos humanos . Na China, nos Estados Unidos, Rússia, Inglaterra, Uganda, Quênia, Eslovênia, Myanmar, Emirados Árabes Unidos, Israel e Índia, a vigilância de manifestantes e civis tem prejudicado os direitos à privacidade e à liberdade de reunião e associação. A prisão equivocada de pessoas inocentes nos Estados Unidos, Argentina e Brasil tem minado o direito das pessoas à privacidade e seu direito ao devido processo e à liberdade de ir e vir. A vigilância de minorias étnicas e religiosas e outras comunidades marginalizadas e oprimidas na China, Tailândia e Itália tem violado o direito das pessoas à privacidade e seus direitos à igualdade e à não discriminação.

Essas tecnologias, desde seu design, ameaçam os direitos dos cidadãos e já causaram danos significativos. Nenhuma proteção técnica ou legal poderia eliminar totalmente a ameaça que representam e, portanto, acreditamos que nunca devem ser usadas em espaços públicos ou de acesso público, seja pelo governo ou pelo setor privado. O potencial de abuso é muito grande e as consequências muito graves.

Pedimos pelo banimento porque, embora uma moratória pudesse interromper temporariamente o desenvolvimento e uso dessas tecnologias, e ganhar tempo para reunir evidências e organizar a discussão democrática, já está claro que essas investigações e discussões só irão demonstrar ainda mais que **o uso dessas tecnologias em espaços acessíveis ao público é incompatível com nossos direitos humanos e liberdades civis e deve ser banido de vez**.

O escopo de nossa chamada

Os termos “reconhecimento facial” e “reconhecimento biométrico remoto” abrangem uma ampla gama de tecnologias, desde o sistema de autenticação facial que desbloqueia o telefone de uma pessoa, ou de outra forma autoriza o acesso a certos lugares, a tecnologias que identificam o jeito de

andar de alguém, até sistemas que buscam identificar a identidade de gênero ou o estado emocional de alguém .

Nosso pedido de banimento se concentra especificamente, mas não está limitado, ao uso dessas tecnologias para identificar ou distinguir uma pessoa de um conjunto maior de indivíduos, também conhecido como “identificação” facial ou biométrica (ou seja, correspondência um-para-muitos). Estamos preocupados com o uso dessas tecnologias para identificar, destacar individualmente ou rastrear indivíduos usando seu rosto, maneira de andar, voz, aparência ou qualquer outro identificador biométrico que permita a vigilância em massa ou vigilância direcionada discriminatória, ou seja, vigilância que impacta desproporcionalmente os direitos humanos de minorias religiosas, étnicas e raciais, dissidentes políticos e outros grupos marginalizados. Também reconhecemos que, em certos casos, sistemas faciais e outros sistemas de “autenticação” biométrica (ou seja, correspondência um a um) podem ser construídos e usados de uma maneira que igualmente permite formas problemáticas de vigilância, por exemplo, criando grandes bases de dados biométricos que podem ser reutilizados para outros fins.

Embora alguns aplicativos de reconhecimento facial e biométrico aleguem proteger a privacidade das pessoas ao não vincular os dados às identidades reais, eles podem, no entanto, ser usados para destacar indivíduos em espaços públicos ou para fazer inferências sobre suas características e comportamentos. Em todas essas situações, não importa se os dados são anonimizados para proteger informações de identificação pessoal ou apenas tratados localmente (ou seja, ‘no limite’); o dano aos nossos direitos ocorre independentemente, porque essas ferramentas são fundamentalmente projetadas para, e possibilitam, a vigilância de pessoas de uma forma que é incompatível com nossos direitos.

Além disso, muitas aplicações de classificação facial e biométrica, que fazem inferências e predições sobre aspectos como a identidade de gênero das pessoas, emoções ou outros atributos pessoais, possuem falhas graves e fundamentais em seus fundamentos científicos. Isso significa que as inferências que elas fazem sobre nós são frequentemente inválidas, em alguns casos até operacionalizando teorias eugenistas de frenologia e fisiognomia, perpetuando, assim, a discriminação, e adicionando uma camada adicional de dano à medida que somos tanto vigiados quanto descaracterizados.

Nosso apelo pelo banimento abrange o uso dessas tecnologias quando forem utilizadas para vigilância em espaços acessíveis ao público e em espaços que as pessoas não podem evitar. Embora o uso dessas tecnologias tenha atraído atenção e crítica, seu uso por atores privados pode representar a mesma ameaça aos nossos direitos, especialmente quando atores privados efetivamente se envolvem na vigilância em nome de governos e agências públicas em parcerias público-privadas, ou fornecem informações derivadas dessa vigilância às autoridades.

Também vimos um desenvolvimento preocupante com provedores privados de reconhecimento facial compilando e combinando bancos de dados de indivíduos "suspeitos" e compartilhando esses bancos de dados com vários clientes. Na prática, isso cria “bancos de dados de âmbito nacional” compartilhados entre empresas privadas, que são compilados a critério de funcionários não

treinados, sem qualquer supervisão e que podem levar à discriminação contra indivíduos que aparecem em listas de observação em todas as entidades que usam esses bancos de dados.

O uso dessas tecnologias para vigiar pessoas em parques municipais, escolas, bibliotecas, locais de trabalho, centros de transporte, estádios esportivos, conjuntos habitacionais e até mesmo em espaços online, como plataformas de mídia social, constitui uma ameaça existencial aos nossos direitos humanos e deve ser interrompido.

Por que banimento?

O reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto têm falhas técnicas significativas em suas formas atuais, incluindo, por exemplo, sistemas de reconhecimento facial que refletem vieses raciais e são menos acurados para pessoas com tons de pele mais escuros. Entretanto, as melhorias técnicas desses sistemas não evitarão a ameaça que representam aos nossos direitos humanos.

Embora dados de treinamento mais diversificados ou outras medidas para melhorar a precisão possam resolver alguns problemas atuais com esses sistemas, tais medidas apenas os aperfeiçoarão como instrumentos de vigilância e os tornarão mais eficazes em minar nossos direitos.

Essas tecnologias representam uma ameaça aos nossos direitos de duas formas principais:

Primeiro, os dados de treinamento - o banco de dados de rostos com o qual os dados de entrada são comparados e os dados biométricos tratados por esses sistemas - são geralmente obtidos sem o conhecimento, consentimento ou escolha genuinamente livre daqueles que estão incluídos neles, o que significa que essas tecnologias incentivam a vigilância em massa e discriminatória desde sua concepção.

Em segundo lugar, enquanto as pessoas em espaços acessíveis ao público puderem ser instantaneamente identificadas, destacadas ou rastreadas, seus direitos humanos serão minados. Até a ideia de que essas tecnologias poderiam estar em operação em espaços acessíveis ao público cria um efeito inibitório que mina a capacidade das pessoas de exercerem seus direitos.

Apesar de alegações questionáveis de que essas tecnologias aprimoram a segurança pública, quaisquer benefícios serão sempre ultrapassados pelas sistemáticas violações aos nossos direitos. Nós vemos cada vez mais provas de como essas tecnologias são usadas de modo abusivo e implementadas com pouca ou nenhuma transparência.

Qualquer pesquisa e análise de como o policiamento foi historicamente conduzido mostra que o uso experimental de tecnologias de vigilância comumente criminaliza comunidades marginalizadas e de baixa renda, incluindo comunidades racializadas, as mesmas comunidades que tradicionalmente enfrentam o racismo estrutural e a discriminação. O uso de reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto não é uma exceção a isso e, por esse motivo, deve

ser impedido antes que uma infraestrutura de vigilância ainda mais perigosa seja criada ou operacionalizada de modo permanente.

A mera existência dessas ferramentas, seja nas mãos das instituições policiais ou de empresas privadas (ou em parcerias público-privadas), sempre criará incentivos para que sejam utilizadas de modo a desvirtuar sua função e para aumentar a vigilância em espaços públicos, levando a um efeito inibidor na liberdade de expressão. Como sua própria existência mina nossos direitos e a supervisão efetiva dessas tecnologias não é possível de modo a impedir abusos, não há outra opção a não ser bani-las totalmente em seu uso em espaços publicamente acessíveis.

Como será um banimento?

Existem algumas tecnologias de vigilância que são simplesmente tão perigosas que inevitavelmente causam muito mais problemas do que resolvem. Quando se trata de reconhecimento facial e outras tecnologias biométricas remotas que permitem vigilância em massa e vigilância direcionada discriminatória, o potencial de abuso é muito grande e as consequências muito graves.

Não há margem para dúvidas: a proteção dos direitos humanos exige a proibição do uso dessas tecnologias em locais publicamente acessíveis pelos governos regionais, nacionais, estaduais, provinciais, municipais, locais e outros, incluindo todas as suas subdivisões e autoridades, e especialmente suas agências de aplicação da lei e controle de fronteiras, que já detêm recursos humanos e tecnológicos suficientes para manter a segurança sem o uso dessas tecnologias.

Como uma rede global de organizações da sociedade civil, reconhecemos que cada país tem maneiras diferentes de desenvolver soluções que priorizam os direitos humanos em cada sistema constitucional, convencional ou jurídico.

No entanto, quaisquer forem os meios, o resultado deve ser o banimento total do uso dessas tecnologias para vigiar, identificar, rastrear, discriminar e seguir pessoas em espaços acessíveis ao público.

Por todas essas razões, pedimos:

---

1. Aos **legisladores e gestores de políticas públicas** em todos os níveis de governo em todo o mundo para:

a. Cessar com todo o investimento público em usos de reconhecimento facial e outras tecnologias biométricas remotas que permitam a vigilância em massa e vigilância discriminatória direcionada;
b. Adotar leis, estatutos e/ou regulamentos abrangentes que:
    i. proíbam o uso dessas tecnologias para vigilância de espaços públicos e acessíveis ao público, incluindo transporte público, por ou em nome de governos nacionais, federais, estaduais, municipais, locais e/ou outras subdivisões políticas, incluindo suas agências, departamentos, secretarias, ministérios, escritórios executivos, conselhos, comissões,

escritórios ou seus contratantes e/ou outras subdivisões e autoridades; com especial ênfase em qualquer tipo de aplicação da lei, investigação criminal, controle de fronteira e agências de inteligência;

ii. proíbam o uso dessas tecnologias por entidades privadas em espaços públicos, espaços acessíveis ao público e locais de acomodação pública, onde tal uso possa permitir a vigilância em massa ou discriminatória, incluindo, mas não se limitando, ao seu uso em parques, escolas, bibliotecas, locais de trabalho, centros de transporte, estádios esportivos e conjuntos habitacionais;

iii. proíbam agências governamentais, especialmente agências de aplicação da lei, de usar e acessar dados e informações derivados do uso dessas tecnologias por empresas privadas e outros atores privados, exceto para fins de auditorias ou verificação de conformidade;

iv. protejam as pessoas contra o uso dessas tecnologias para tomar decisões relacionadas aos direitos econômicos, sociais e culturais, incluindo moradia, emprego, benefícios sociais e assistência de saúde;

v. excluam o uso dessas tecnologias e das informações delas derivadas como evidência para processar criminalmente ou acusar pessoas para prendê-las ou detê-las de outra forma; e

vi. restrinjam o acesso do governo a informações biométricas armazenadas por empresas privadas.

c. Estabelecer regras e regulamentos que proíbam a aquisição dessas tecnologias por agências governamentais e estatais para usos que permitem vigilância em massa e vigilância direcionada discriminatória;

d. Impedir o uso de reconhecimento facial e outras tecnologias biométricas remotas para vigilância em massa ou vigilância discriminatória de minorias religiosas, étnicas e raciais e de dissidentes políticos e outros grupos marginalizados;

e. Obrigar a divulgação do uso dessas tecnologias para aqueles indivíduos que, sem saber, foram submetidos a elas e que não tiveram a chance de exercer seus direitos ao devido processo para contestar o uso da tecnologia; e

f. Fornecer reparação adequada aos indivíduos que foram prejudicados pelo uso dessas tecnologias.

---

2. Os **tribunais e juízes** devem reconhecer as ameaças existenciais aos direitos humanos decorrentes do uso dessas tecnologias e agir para prevenir e, se necessário, reparar os danos causados por seu uso; e

---

3) As **agências administrativas**, incluindo as agências/autoridades de proteção de dados e de proteção ao consumidor, devem usar sua autoridade total para proteger a privacidade e os direitos do consumidor, incluindo instar as empresas a interromper o uso dessas tecnologias.

Finalmente, reconhecemos que a ameaça existencial representada pelas tecnologias de reconhecimento facial e reconhecimento biométrico remoto deve ser enfrentada não apenas por

países e governos de todos os tipos, mas também por outros atores importantes nos níveis internacional e nacional.

Por essa razão, nós pedimos para:

---

1. Organizações Internacionais, como o Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos (OHCHR), para intensificar e condenar o atual desenvolvimento e uso de reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto para vigiar comunidades em todo o mundo;

---

2. **Entidades privadas** que desenvolvem ou usem tecnologia de reconhecimento facial e reconhecimento biométrico remoto para:

a. assumir compromissos públicos para cessar a criação, desenvolvimento, venda e uso de reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto que permitem a vigilância em massa e a vigilância discriminatória direcionada;
b. cessar imediatamente a produção de tecnologias de reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto que permitem a vigilância em massa e a vigilância discriminatória direcionada, e excluir quaisquer dados biométricos adquiridos ilegitimamente usados para construir bancos de dados e quaisquer modelos ou produtos construídos com base em tais dados;
c. emitir relatórios de transparência que detalhem todos os seus contratos públicos (incluindo aqueles que estão suspensos, em andamento ou em fase de implementação) para o fornecimento dessas tecnologias; e
d. envolver-se de forma significativa e não retaliar os trabalhadores que se organizam em seus locais de trabalho para desafiar ou recusar o desenvolvimento de reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto que permitem a vigilância em massa e a vigilância discriminatória direcionada.

---

3. **Trabalhadores de empresas de tecnologia**, com o apoio de seus sindicatos, para se organizarem em seus locais de trabalho contra o desenvolvimento ou venda de reconhecimento facial e outras tecnologias de reconhecimento biométrico remoto, na medida do possível;

---

4. **Investidores e instituições financeiras** para:

a. conduzir a devida diligência em direitos humanos em seus investimentos atuais e futuros em empresas que desenvolvem e vendem reconhecimento facial e tecnologias de reconhecimento biométrico remoto, a fim de descobrir onde essas tecnologias são incompatíveis com os direitos humanos e permitem vigilância em massa e a vigilância direcionada discriminatória; e
b. fazer com que as empresas que investem parem de criar, desenvolver, vender ou de outra forma disponibilizar essas tecnologias que permitem a vigilância em massa e a vigilância direcionada discriminatória

---

5. **Organizações doadoras** para garantir financiamento para litígios e defesa por organizações não governamentais e organizações da sociedade civil que buscam reparação de danos nos tribunais e se

envolvem ativamente na formulação de políticas nos sistemas local, estadual, nacional, federal e internacional.

Conclusão

Pedimos à sociedade civil, ativistas, acadêmicos e outras partes interessadas de todo o mundo que assinem esta carta e se juntem à luta para garantir que o uso dessas tecnologias em espaços acessíveis ao público seja banido agora e para sempre para que nossos direitos humanos e liberdades civis sejam protegidos.

Contate **banBS@accessnow.org** para mais informações sobre como você pode apoiar esta iniciativa e confira **accessnow.org/ban-biometric-surveillance** para ver a lista completa de signatários e adicionar seu nome à lista.

Esta carta aberta foi elaborada por Access Now, Amnesty International, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF) e o Instituto Brasileiro de Defesa do Consumidor (IDEC).